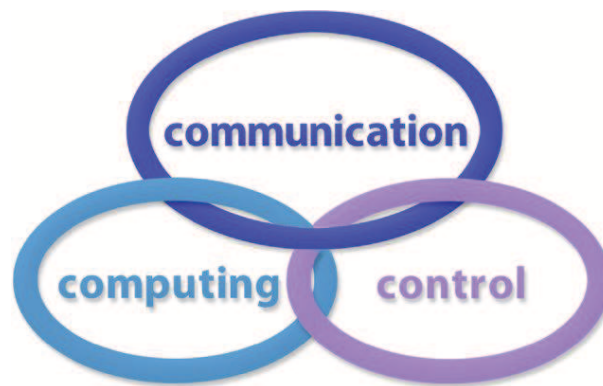


INTERNATIONAL JOURNAL
of
COMPUTERS COMMUNICATIONS & CONTROL

ISSN 1841-9836, e-ISSN 1841-9844



A Bimonthly Journal
With Emphasis on the Integration of Three Technologies

Year: 2019 Volume: 14 Issue: 6 Month: December

This journal is a member of, and subscribes to the principles of, the Committee on Publication Ethics (COPE).



<http://univagora.ro/jour/index.php/ijccc/>

CCC Publications

Copyright © 2006-2019 by Agora University & CC BY-NC

BRIEF DESCRIPTION OF JOURNAL

Publication Name: International Journal of Computers Communications & Control.

Acronym: IJCCC; **Starting year of IJCCC:** 2006.

ISO: Int. J. Comput. Commun. Control; **JCR Abbrev:** INT J COMPUT COMMUN.

International Standard Serial Number: ISSN 1841-9836, e-ISSN 1841-9844.

Publisher: CCC Publications - Agora University of Oradea.

Publication frequency: Bimonthly: Issue 1 (February); Issue 2 (April); Issue 3 (June); Issue 4 (August); Issue 5 (October); Issue 6 (December).

Founders of IJCCC: Ioan DZITAC, Florin Gheorghe FILIP and Misu-Jan MANOLESCU.

Indexing/Abstracting/Coverage:

- Since 2006, Vol. 1 (S), IJCCC is covered by Clarivate Analytics and is indexed in ISI Web of Science: Science Citation Index Expanded. Total number of abstracted papers until 2020: **1000**.

2019 Journal Citation Reports® Science Edition (Clarivate Analytics, 2018):

Subject Category: (1) Automation & Control Systems: Q4(2009, 2011, 2012, 2013, 2014, 2015), **Q3(2010, 2016, 2017, 2018)**; (2) Computer Science, Information Systems: Q4(2009, 2010, 2011, 2012, 2015), **Q3(2013, 2014, 2016, 2017, 2018)**.

Impact Factor/3 years in JCR: 0.373(2009), 0.650 (2010), 0.438(2011); 0.441(2012), 0.694(2013), 0.746(2014), 0.627(2015), 1.374(2016), 1.29 (2017), **1.585 (2018)**.

Impact Factor/5 years in JCR: 0.436(2012), 0.622(2013), 0.739(2014), 0.635(2015), 1.193(2016), 1.179(2017), **1.361(2018)**.

- Since 2008 IJCCC is indexed by Scopus: **CiteScore2018 = 1.56**.

Subject Category:

(1) Computational Theory and Mathematics: Q4(2009, 2010, 2012, 2015), **Q3(2011, 2013, 2014, 2016, 2017, 2018)**;

(2) Computer Networks and Communications: Q4(2009), Q3(2010, 2012, 2013, 2015), **Q2(2011, 2014, 2016, 2017, 2018)**;

(3) Computer Science Applications: Q4(2009), **Q3(2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018)**.

SJR: 0.178(2009), 0.339(2010), 0.369(2011), 0.292(2012), 0.378(2013), 0.420(2014), 0.263(2015), 0.319(2016), 0.326 (2017), 0.37 (2018).

- Since 2007, 2(1), IJCCC is indexed in EBSCO.

Focus & Scope: International Journal of Computers Communications & Control is directed to the international communities of scientific researchers in computers, communications and control, from the universities, research units and industry. To differentiate from other similar journals, the editorial policy of IJCCC encourages the submission of original scientific papers that focus on the integration of the 3 "C" (Computing, Communications, Control).

In particular, the following topics are expected to be addressed by authors:

(1) Integrated solutions in computer-based control and communications;

(2) Computational intelligence methods & Soft computing (with particular emphasis on fuzzy logic-based methods, computing with words, ANN, evolutionary computing, collective/swarm intelligence, membrane computing, quantum computing);

(3) Advanced decision support systems (with particular emphasis on the usage of combined solvers and/or web technologies).

EDITORIAL STAFF OF IJCCC

EDITORS-IN-CHIEF:

Ioan DZITAC

Aurel Vlaicu University of Arad, Romania
St. Elena Dragoi, 2, 310330 Arad
professor.ioan.dzitac@ieee.org

Florin Gheorghe FILIP

Romanian Academy, Romania
125, Calea Victoriei, 010071 Bucharest
fflip@acad.ro

MANAGING EDITOR:

Mișu-Jan MANOLESCU

Agora University of Oradea, Romania
Piata Tineretului, 8, 410526 Oradea
mmj@univagora.ro

EXECUTIVE EDITOR:

Răzvan ANDONIE

Central Washington University, USA
400 East University Way, Ellensburg, WA 98926
andonie@cwu.edu

PROOFREADING EDITOR:

Răzvan MEZEI

Lenoir-Rhyne University, USA
Madison, WI
proof.editor@univagora.ro

LAYOUT EDITOR:

Horea OROS

University of Oradea, Romania
St. Universitatii 1, 410087, Oradea
horos@uoradea.ro

TECHNICAL EDITOR:

Domnica Ioana DZITAC

New York University Abu Dhabi, UAE
Saadiyat Marina District, Abu Dhabi
domnica.dzitac@nyu.edu

EDITORIAL ADDRESS:

Agora University, Cercetare Dezvoltare Agora, Tineretului 8, 410526 Oradea, Bihor, Romania,
Tel./ Fax: +40 359101032, E-mail: ijccc@univagora.ro, rd.agora@univagora.ro
URL: <http://univagora.ro/jour/index.php/ijccc/>

EDITORIAL BOARD OF IJCCC (MEMBERS):

Vandana AHUJA

Amity University, INDIA
F3 Block, Amity University Campus
Sector - 125 Noida - 201 313
vahuja@amity.edu

Fuad ALESKEROV

Russian Academy of Sciences, RUSSIA
HSE, Shabolovka St, Moscow
alesk@hse.ru

Luiz F. AUTRAN GOMES

Ibmec, Rio de Janeiro, BRAZIL
Av. Presidente Wilson, 118
autran@ibmecrj.br

Barnabas BEDE

DigiPen Institute of Technology, USA
Redmond, Washington
bbede@digipen.edu

Dan BENTA

Agora University of Oradea, ROMANIA
Tineretului, 8, 410526 Oradea
dan.benta@univagora.ro

Pierre BORNE

Ecole Centrale de Lille, FRANCE
Villeneuve d'Ascq Cedex, F 59651
p.borne@ec-lille.fr

Alfred M. BRUCKSTEIN

Ollendorff Chair in Science, ISRAEL
Technion, Haifa 32000
freddy@cs.technion.ac.il

Ioan BUCIU

University of Oradea, ROMANIA
Universitatii, 1, Oradea
ibuciu@uoradea.ro

Amlan CHAKRABARTI

University of Calcutta, INDIA
87/1, College Street, College Square 700073
acakcs@caluniv.ac.in

Svetlana COJOCARU

IMMAS, Republic of MOLDOVA
Kishinev, 277028, Academiei 5
svetlana.cojocar@math.md

Felisa CORDOVA

University Finis Terrae, CHILE
Av. P. de Valdivia 1509, Providencia
fcordova@uft.cl

Petre DINI

Concordia University, CANADA
Montreal, Canada
pdini@cisco.com

Antonio Di NOLA

University of Salerno, ITALY
Via Ponte Don Melillo, 84084 Fisciano
dinola@cds.unina.it

Yezid DONOSO

Univ. de los Andes, COLOMBIA
Cra. 1 Este No. 19A-40, Bogota
ydonoso@uniandes.edu.co

Gintautas DZEMYDA

Vilnius University, LITHUANIA
4 Akademijos, Vilnius, LT-08663
gintautas.dzemyda@mii.vu.lt

Simona DZITAC

University of Oradea, ROMANIA
1 Universitatii, Oradea
simona@dzitac.ro

Ömer EGECIOGLU

University of California, USA
Santa Barbara, CA 93106-5110
omer@cs.ucsb.edu

Constantin GAINDRIC

IMMAS, Republic of MOLDOVA
Kishinev, 277028, Academiei 5
gaindric@math.md

Xiao-Shan GAO

Academia Sinica, CHINA
Beijing 100080, China
xgao@mmrc.iss.ac.cn

Enrique HERRERA-VIDEVA

University of Granada, SPAIN
Av. del Hospicio, s/n, 18010 Granada
viedma@decsai.ugr.es

Kaoru HIROTA

Tokyo Institute of Tech., JAPAN
G3-49,4259 Nagatsuta
hirota@hrt.dis.titech.ac.jp

Arturas KAKLAUSKAS

VGTU, LITHUANIA
Sauletekio al. 11, LT-10223 Vilnius
arturas.kaklauskas@vgtu.lt

Gang KOU

SWUFE, CHINA
Chengdu, 611130
kougang@swufe.edu.cn

Heeseok LEE

KAIST, SOUTH KOREA
85 Hoegiro, Seoul 02455
hsl@business.kaist.ac.kr

George METAKIDES

University of Patras, GREECE
Patra 265 04, Greece
george@metakides.net

Shimon Y. NOF

Purdue University, USA
610 Purdue Mall, West Lafayette
nof@purdue.edu

Stephan OLARIU

Old Dominion University, USA
Norfolk, VA 23529-0162
olariu@cs.odu.edu

Gheorghe PĂUN

Romanian Academy, ROMANIA
IMAR, Bucharest, PO Box 1-764
gpaun@us.es

Mario de J. PEREZ JIMENEZ

University of Seville, SPAIN
Avda. Reina Mercedes s/n, 41012
marper@us.es

Radu-Emil PRECUP

Pol. Univ. of Timisoara, ROMANIA
Bd. V. Parvan 2, 300223
radu.precup@aut.upt.ro

Radu POPESCU-ZELETIN

Technical University Berlin, GERMANY
Fraunhofer Institute for Open CS
rpz@cs.tu-berlin.de

Imre J. RUDAS

Obuda University, HUNGARY
Budapest, Becs ut 96b, 1034
rudas@bmf.hu

Yong SHI

Chinese Academy of Sciences, CHINA
Beijing 100190
yshi@gucas.ac.cn, yshi@unomaha.edu

Bogdana STANOJEVIC

Serbian Academy of SA, SERBIA
Kneza Mihaila 36, Beograd 11001
bgdnpop@mi.sanu.ac.rs

Athanasios D. STYLIADIS

University of Kavala, GREECE
65404 Kavala
styliadis@teikav.edu.gr

Mincong TANG

Beijing Jiatong University, CHINA
No.3 Shangyuancun, Haidian D., Beijing
mincong@bjtu.edu.cn

Gheorghe TECUCI

George Mason University, USA
University Drive 4440, Fairfax VA
tecuci@gmu.edu

Horia-Nicolai TEODORESCU

Romanian Academy, ROMANIA
Iasi Branch, Bd. Carol I 11, 700506
hteodor@etc.tuiasi.ro

Dan TUFIS

Romanian Academy, ROMANIA
13 Septembrie, 13, 050711 Bucharest
tufis@racai.ro

Edmundas K. ZAVADSKAS

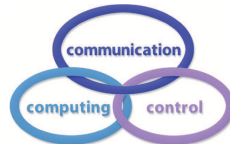
VGTU, LITHUANIA
Sauletekio ave. 11, LT-10223 Vilnius
edmundas.zavadskas@vgtu.lt

Contents

Parameter Estimation for PMSM based on a Back Propagation Neural Network Optimized by Chaotic Artificial Fish Swarm Algorithm J.W. Jiang, Z. Chen, Y.H. Wang, T. Peng, S.L. Zhu, L.M. Shi	615
Studies in Informatics and Control: A Bibliometric Analysis from 2008 to 2019 Y. Li, Z.S. Xu, X.X. Wang, F.G. Filip	633
Modeling of Characteristics on Artificial Intelligence IQ Test: a Fuzzy Cognitive Map-Based Dynamic Scenario Analysis F. Liu, Y. Peng, Z.X. Chen, Y. Shi	653
An Empirical Study of AML Approach for Credit Card Fraud Detection–Financial Transactions A. Singh, A. Jain	670
A Cluster–based Approach for Minimizing Energy Consumption by Reducing Travel Time of Mobile Element in WSN J. Siva Prashanth, S.V. Nandury	691
Hierarchical Decision-making using a New Mathematical Model based on the Best-worst Method M.H. Tabatabaei, M. Amiri, M. Ghahremanloo, M. Keshavarz-Ghorabae, E.K. Zavadskas, J. Antucheviciene	710
Wearable System for Daily Activity Recognition Using Inertial and Pressure Sensors of a Smart Band and Smart Shoes P.H. Truong, S. You, S.-H. Ji, G.-M. Jeong	726
Automated Expert System Knowledge Base Development Method for Information Security Risk Analysis D. Vitkus, Z. Steckeivicius, N. Goranin, D. Kalibatiene, A. Cenys	743
Identification of Opinion Spammers using Reviewer Reputation and Clustering Analysis M.J. Zhong, L.Tan, X.L. Qu	759

Parameter Estimation for PMSM based on a Back Propagation Neural Network Optimized by Chaotic Artificial Fish Swarm Algorithm

J.W. Jiang, Z. Chen, Y.H. Wang, T. Peng, S.L. Zhu, L.M. Shi



Jianwu Jiang

1. School of Computer Science and Technology, Soochow University, China
333 East GanJiang Way, SuShou, 225300, China
2. College of Information Engineering, Taizhou Polytechnic College, China
47955024@qq.com

Zhi Chen

College of Information Engineering, Taizhou Polytechnic College, China
17784068@qq.com

Yihuai Wang*

School of Computer Science and Technology, Soochow University, China
333 East GanJiang Way, SuShou, 225300, China
*Corresponding author: yihuaiw@suda.edu.cn

Tao Peng

School of Computer Science and Technology, Soochow University, China
sdpengtao401@gmail.com

Shilang Zhu

School of Computer Science and Technology, Soochow University, China
20154027006@stu.suda.edu.cn

Lianmin Shi

College of Information Engineering, Suzhou Institute of Trade & Commerce, China
20154027006@stu.suda.edu.cn

Abstract: Permanent Magnet Synchronous Motor(PMSM) control system with strong nonlinearity makes it difficult to accurately identify motor parameters such as stator winding, dq axis inductance, and rotor flux linkage. Aiming at the premature convergence of traditional Back Propagation Neural Network(BPNN) in PMSM motor parameter identification, a new method of PMSM motor parameter identification is proposed. It uses Chaotic Artificial Fish Swarm Algorithm(CAFSA) to optimize the initial weights and thresholds of BPNN, and then strengthens training by BPNN algorithm. Thus, the global optimal network parameters are obtained by using the global optimization of CAFSA and the local search ability of BPNN. The simulation results and experimental data show that the initial value sensitivity of the network model optimized by CAFS-BPNN Algorithm is weak, the parameter setting is robust, and the system stability is good under complex conditions. Compared with other intelligent algorithms, such as RSL and PSO, CAFS-BPNN has high identification accuracy and fast convergence speed for PMSM motor parameters.

Keywords: Permanent Magnet Synchronous Motor(PMSM), Back Propagation Neural Network(BPNN), Chaotic Artificial Fish Swarm Algorithm(CAFSA), parameter estimation, identification accuracy, convergence speed.

1 Introduction

Permanent magnet synchronous motor (PMSM) is widely used in industrial robots, servo drive control, electric vehicle speed regulation and other high-precision control fields due to its outstanding advantages in power and torque density, speed control performance and system robustness [10].

PMSM motor parameters include stator windings, dq axis inductance, rotor flux, etc. They can be used to reflect the performance of the motor system during operation, and can assist to complete motor condition monitoring [5] and fault diagnosis [12]. Therefore, accurate parameter identification ability is very important for motor control system.

However, motor parameters are very vulnerable to external factors such as temperature, flux saturation and skin effect [3], such as temperature change will affect the stator winding, permanent magnet demagnetization directly affects the dq axis inductance [22]. With the change of working condition and surrounding environment, there is a certain difference between actual parameters and nominal parameters [17].

Therefore, as a motor controller, it must have the function of self-tuning and identification of motor parameters. Considering the technical difficulty and cost, it is difficult to directly measure motor parameters through auxiliary sensors such as temperature and magnetism [5, 15].

PMSM control system has very strong non-linear and time-varying characteristics. It is very difficult to accurately identify the parameters of PMSM. The identification algorithm needs to comprehensively weigh the factors of complexity, convergence and computing time.

2 Related works

In traditional control theory, parameter identification methods of PMSM include least square method (RLS) [18, 23], extended Kalman filter identification (EKF) [1, 6, 20], model reference adaptive (MRAS) [2, 26] etc.

Because of the linear parameterization of RLS algorithm, RLS estimators are usually noise sensitive, which may lead to lower identification accuracy. When estimating the winding resistance and rotor flux by EKF, the estimator is noisy and unstable, so it can not accurately estimate the actual parameters.

MRAS estimator can not accurately estimate winding resistance, inductance and rotor flux simultaneously. It is often impossible to find the optimal solution of the estimated parameters accurately by using the above methods. With the development of swarm intelligence theory, many scholars have applied this kind of optimization algorithm to motor parameter identification, including ant colony algorithm [4], genetic algorithm [21], particle swarm optimization algorithm [14]. Ant colony algorithm and particle swarm optimization algorithm are easy to fall into local optimization convergence, and the optimization error is relatively large. Literature [11] uses genetic algorithm to identify dq axis inductance and rotor flux, because of the large space-time complexity, the convergence speed is slow. Literature [14] uses dynamic particle swarm optimization (DPSO-LS) algorithm and dynamic anti-learning strategy of Gauss distribution to enhance the global search ability, but the computational complexity becomes larger.

With the development of artificial intelligence technology, the artificial neural network is widely used in parameter identification of PMSM motor, and BPNN is the most widely used [21, 25].

BPNN is a multi-layer feedforward neural network trained by error back propagation algorithm. It has the advantages of clear model structure and simple calculation. It has been proved theoretically that its three-layer model can map any complex non-linear relationship model [16]. It is widely used in non-linear curve fitting in various signal processing and automatic control.

BPNN has excellent local optimization ability and can converge quickly and accurately in local areas. However, this advantage has also results in poor global search performance, local prematurity, poor global convergence, long iteration period and other problems, and its algorithm optimization is difficult to achieve the desired convergence accuracy and convergence speed. Therefore, it is necessary to combine the BPNN algorithm with the other intelligent algorithm with stronger global optimization ability. In the early stage of training, the cooperative algorithm is used to converge the network to the global extremum quickly, and then the local optimization characteristic of BPNN is used to converge quickly.

CAFSA is a swarm intelligence algorithm with excellent global searching ability. It simulates the behavior of fish swarm such as preying, swarming, following and moving to optimize the system. It has the characteristics of weak sensitivity to initial values, strong robustness to parameter setting, good global searching performance and fast convergence speed [19, 23].

CAFSA algorithm has large randomness and poor convergence in the later search period. It needs to improve the optimization performance by improving system step size, the field of view, adding congestion factor [8]. The combination of CAFSA and BPNN will make up for their respective optimization shortcomings, and improve the overall optimization performance in terms of convergence speed and accuracy.

This paper presents a PMSM motor parameter identification algorithm based on CAFS-BPNN, which combines BPNN with AFSA effectively. By injecting impulse current into the d-axis of PMSM motor control system, the sampling process data, including d-axis voltage, q-axis voltage, d-axis current, q-axis current and motor speed, are used as data sets for network training and testing. The parameters set $\{R_s, L_d, L_q, \psi_f\}$ to be identified are taken as network output. Combining the global search ability of CAFSA and the local fast convergence property of BPNN, the convergence accuracy and speed of PMSM motor parameter identification are effectively improved.

The outstanding contributions of this paper include:

(1) Using the forward propagation topology of BPNN, a nonlinear mapping identification model from sampled parameter set $\{u_d, u_q, i_d, i_q, \omega\}$ to identified parameter set $\{R_s, L_d, L_q, \psi_f\}$ of permanent magnet synchronous motor (PMSM) is constructed. The input data set of the mapping model is obtained by d-axis current injection method, and parameters of PMSM motor to be identified are obtained by simple and direct mapping model.

(2) The CAFS-BPNN algorithm of BPNN optimized by CAFSA is introduced into online identification of PMSM motor parameters. The connection weights and thresholds of BPNN network are taken as the optimization objects of CAFSA. The connection weights and thresholds of BPNN are optimized quickly by using CAFSA global search ability in the early stage of training, and then the optimization of BPNN is transferred to the global optimal extremum point in the later stage. By giving full play to their respective optimization characteristics and avoiding their own shortcomings, the convergence accuracy and speed of obtaining network parameters of PMSM motor parameter identification model are effectively improved.

(3) The population aggregation degree is embedded in CAFS-BPNN as the switching condition of the two intelligent algorithms. According to the optimization characteristics of the fish swarm algorithm, the aggregation degree of the population increases in the later stage of optimization. When it reaches the preset threshold, it means that it reaches the late stage of fast convergence optimization algorithm of CAFSA, and can be transferred to BPNN precision optimization algorithm, thus the time of turning into precision optimization algorithm is accelerated.

3 Theoretical analysis of group intelligence identification model for PMSM motor parameters

3.1 Mathematical model for PMSM motor identification

PMSM control system is a complex system with strong coupling and time-varying nonlinearity. It can establish mathematical models in static three-phase coordinate system, static $\alpha\beta$ coordinate system and synchronous rotating dq coordinate system. The mathematical models in three coordinate systems can be transformed each other. The mathematical model in the dq coordinate system is the most commonly used mathematical model [11].

Neglecting the magnetic saturation effect of PMSM and the eddy current and hysteresis loss of core are neglected, the voltage equation and flux linkage equation in the dq coordinate system are expressed as (1) and (2):

$$\begin{cases} u_d = R_s i_d + \frac{d\psi_d}{dt} - \omega \psi_q \\ u_q = R_s i_q + \frac{d\psi_q}{dt} + \omega \psi_d \end{cases} \quad (1)$$

$$\begin{cases} \psi_d = L_d i_d + \psi_f \\ \psi_q = L_q i_q \end{cases} \quad (2)$$

where u_d and u_q are the voltage component on the dq axis, i_d and i_q are the current component on the dq axis, R_s is the stator resistance, ψ_d and ψ_q are the flux linkage on the dq axis, L_d and L_q are the inductance on the dq axis, ψ_f is the flux chain generated by the permanent magnet, ω is the electrical angular speed.

In the synchronous rotating dq coordinate system, the mathematical model of PMSM can be expressed as:

$$\begin{cases} \frac{di_d}{dt} = \frac{R_s}{L_d} i_d + \frac{L_q}{L_d} \omega i_d + \frac{u_d}{L_d} \\ \frac{di_q}{dt} = \frac{R_s}{L_q} i_q + \frac{L_d}{L_q} \omega i_d + \frac{u_q}{L_q} - \frac{\psi_f}{L_q} \omega \end{cases} \quad (3)$$

$p = \{R_s, L_d, L_q, \psi_f\}$ is the set of parameters that need to be identified synchronously.

When $i_d = 0$, the dq axis current is decoupled so that the stator current has only the AC component of q axis. In the steady state, formula (2) is brought into formula (1) and discretized to express as follows:

$$\begin{cases} u_{d0} = -L_q \omega_0 \psi_{q0} \\ u_{q0} = R_s i_{q0} + \psi_{f0} \omega_0 \end{cases} \quad (4)$$

Formula (4) shows that the order of the motor equation is two, but the system needs to identify four parameters: $\{R_s, L_d, L_q, \psi_f\}$.

The equation of state is rank-deficit type. By injecting the d-axis current of instantaneous $i_d \neq 0$ into the steady state, the motor model is expressed as:

$$\begin{cases} u_{d1} = R_s i_{d1} - L_q \omega_1 i_{q1} \\ u_{q1} = R_s i_{q1} + L_d \omega_1 i_{d1} + \psi_f \omega_1 \end{cases} \quad (5)$$

It can be seen from literature [2] that the measurement error of rotor flux linkage ψ_{ferror} is caused by assuming $L_d = L_q$ and $\psi_f = \psi_{f0}$.

When ψ_{ferror} is negligible relative to ψ_{f0} , (12) shows that ψ_{fe} and ψ_{f0} are equal, and $|\psi_{ferror}|$ can be simplified as follows:

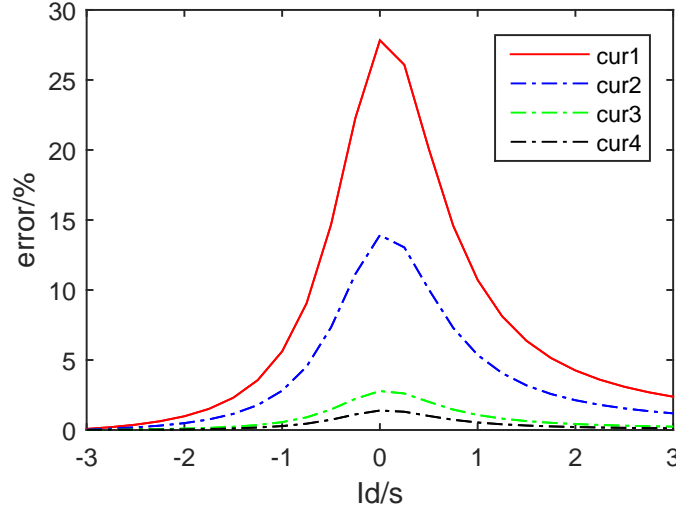


Figure 1: Estimation error of rotor flux relative to d-axis current

$i_q = 3.55A, i_{q0} = 3.35A, \psi_{m0} = 175Wb, L_d = 8.5mH$ Cure1: $\Delta\psi_m = 1\%\Delta\psi_{m0}, \Delta L = 10\%L_d$
Cure2: $\Delta\psi_m = 0.5\%\Delta\psi_{m0}, \Delta L = 5\%L_d$ Cure3: $\Delta\psi_m = 0.1\%\psi_{m0}, \Delta L = 1\%L_d$ Cure4: $\Delta\psi_m = 0.05\%\Delta\psi_{m0}, \Delta L = 0.5\%L_d$

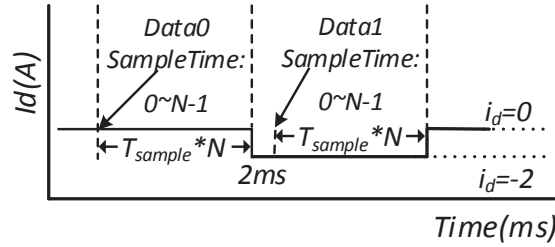


Figure 2: Time series model for data sampling

$$|\psi_{ferror}| \approx \left| \frac{\Delta\psi_f i_{q1}^2 + \Delta L i_{d1} i_{q1}^2}{i_{q1}^2 - i_{d1}^2 - i_{q1}^2} \right| = \left| \frac{\Delta\psi_f i_{q1}^2}{i_{d1}^2} + \frac{\Delta L i_{q1}^2}{i_{d1}} \right| \quad (6)$$

When i_{d1} is large enough, (13) shows that $|\psi_{ferror}| \rightarrow 0$ and $\psi_{fe} \approx \psi_{f0}$, see Fig. 1.

3.2 Data set acquisition method of PMSM motor identification model

Generally, PMSM motors can be controlled by constant torque angle (torque angle is 90°). Adjusting the d -axis current ($i_d = 0$) makes the q -axis get the maximum torque.

In order to obtain the information of motor speed, dq axis current and voltage needed to be sampled when evaluating motor parameters, Data0 and Data1 were obtained by alternately adjusting ($i_d = 0$) and ($i_d \neq 0$) injecting reverse d axis current ($i_d = -2A$) during sampling period.

The single sampling time is $T_{sample} (= 10^{-4}s)$, and the total sampling time is $T_{sample} * N$.

The time series model of data sampling is shown in Fig.2. Data1 data sampling start time is 2ms after current switching, which avoids the interference caused by current switching and ensures the stability of sampling data.

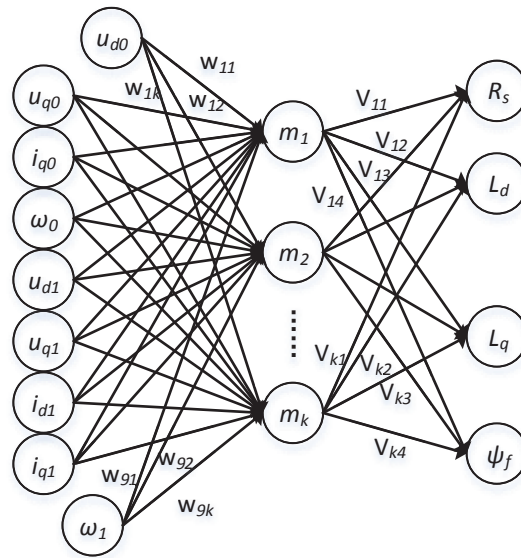


Figure 3: BPNN-PMSM motor parameter identification model

3.3 Parameter mapping model of PMSM motor identification based on BPNN

According to the principle of BPNN and the control strategy model of PMSM in Section 3.1, the set $\{R_s, L_d, L_q, \psi_f\}$ of PMSM parameters to be identified is taken as the output neuron set of BPNN, and the $data0 = \{u_{d0}, u_{q0}, i_{q0}, \omega_0\}$ ($i_d = 0$) and $data1 = \{u_{d1}, u_{q1}, i_{d1}, i_{q1}, \omega_1\}$ ($i_d \neq 0$) are used as the input neuron set.

The BPNN parameter identification model of PMSM motor as shown in Fig. 3 is constructed.

The three-layer neural network model consists of nine input neurons and four output neurons. The hidden layer uses Tansig function as the transfer function $f_1(\cdot)$, and the output layer uses linear purelin as the transfer function $f_2(\cdot)$.

The hidden layer neurons output $z_h = f_1(\sum_{i=0}^n \omega_{ih} x_i)$ ($h = 1, 2, \dots, 9$) and the output layer neurons output $y_j = f_2(\sum_{h=0}^m v_{hj} z_h)$ ($j = 1, 2, 3, 4$), thus the BPNN network completes the mapping from the input 9-dimensional space to the output 4-dimensional space.

After determining the input layer, output layer and data set of BPNN network, the key factors affecting the performance of BPNN network include the number of hidden layer layers, the number of hidden layer neurons, initial connection weights and thresholds, learning rate and learning algorithm. Increasing the hidden layer can reduce the network error and improve the accuracy, but the performance will also increase the network complexity and training time, and may appear the tendency of "over-fitting". According to Hornic's theory that three-layer BPNN can fit arbitrary non-linear curve, the identification model in this paper adopts a three-layer network structure with one hidden layer. The number of hidden layer neurons directly determines whether the network will appear "over-fitting" phenomenon, but there is no theory to accurately determine the number of hidden layer neurons in BPNN network. In this paper, empirical formula and experimental verification will be used to determine the optimal number.

The setting of initial connection weights and thresholds will have a great impact on the convergence speed of the model.

In this paper, the artificial fish swarm algorithm with strong initial robustness is introduced into the initial optimization of the model, so as to improve the convergence speed and speed up

the global optimization.

Through the study of BPNN network, the following empirical formulas for calculating hidden layer neuron data are formed:

Gagan pointed out the logarithmic relationship between the hidden layer neurons and the input neurons.

Formula 1: $m_1 = \log_2 n$ [20]. Kolmogorov's theorem shows that there exists a relationship between recessive neurons and input neurons.

Formula 2: $m_2 = 2n - 1$. D. Gao [7] used least square method to simplify the relationship between input and output and hidden layer neurons.

Formula 3: $m_3 = \sqrt{(0.43nl + 0.12l^2 + 2.54n + 0.77l + 0.35) + 0.51}$ [7]. The number of hidden layer neurons can be calculated by input neurons and output neurons.

Formula 4: $m_4 = \sqrt{nl}$. The number of neurons in the hidden layer was obtained by using input neurons and output neurons as well as by adjusting parameters.

Formula 5: $m_5 = \sqrt{n+l} + \alpha, \alpha = 1, 2, \dots, 10$. In the above formula, m is the number of neurons in the hidden layer, n is the number of neurons in the input layer, l is the number of neurons in the output layer.

Table 1: The number of neurons in the hidden layer of BPNN

No.	m ₁	m ₂	m ₃	m ₄	m ₅	m
n = 9, l = 4, α = 1, 2, ..., 10	4	17	8	6	5-14	4-17

The number of hidden layer neurons $m = m_1, m_2, m_3, m_4, m_5$ is obtained by combining the above empirical formulas. According to the BPNN-PMSM parameter identification model in Chapter 3.3, $n = 9, l = 4$ can be obtained. The number of hidden layer neurons m is shown in Tab.1.

Weight Mean Square Error (WMSE) is used to calculate the training errors.

The individual error of sample p can be expressed:

$$E_p = \frac{1}{2} \sum_{j=1}^l (\hat{y}_j^p - y_j^p)^2 w_j, \text{ and global error WMSE can be expressed: } WMSE = \sum_{i=1}^p E_p.$$

In the previous two formulas, l is the number of output nodes, p is the number of training samples, \hat{y}_j^p is the expected output value of network, y_j^p is the actual output value of network, and w_j is the error weight of output nodes.

According to the definition of net input value S_j of neuron node y_j , the hidden layer neuron output $z_h = f_1(S_h)$ and the output layer neuron output $y_j = f_2(S_j)$ described in chapter 3.3.

v_{hj} is the weights of output layer connection and w_{ih} is hidden layer connection. They can be adjusted by cumulative error algorithm.

The increments of connection weight Δv_{hj} and Δw_{ih} can be generated after each iteration.

They are expressed as follows:

$$\Delta v_{hj} = \sum_{i=1}^p \sum_{j=1}^l \eta (\hat{y}_j^p - y_j^p)^2 f_2'(S_j) z_j, \Delta w_{ih} = \sum_{i=1}^p \sum_{j=1}^l (\eta (\hat{y}_j^p - y_j^p)^2 f_2'(S_j) v_{hj} f_1'(S_h) x_i,$$

where η is learning rate and $\eta \in (0.01, 10)$.

In the process of learning, the weighted inertial momentum is used to reduce the learning oscillation and accelerate the convergence of the system.

The adjusted formula for calculating the actual weights can be expressed:

$$\Delta w(n) = -\eta_1 \Delta WMSE(n) + \alpha w(n-1), \text{ where } \eta_1 \text{ is learning rate and } \alpha \text{ is the inertial momentum.}$$

In order to adapt the BPNN network to the convergence speed in different periods, the system learning rate parameter η_1 is adjusted dynamically and adaptively.

The error ratio can be expressed:

$$\varphi = WMSE(n) / WMSE(n-1).$$

When φ is larger than the threshold value φ_{th} , the learning rate is increased, and vice versa, which ensures that the learning rate is earlier and faster in the early learning stage.

In the later stage of learning, the learning rate decreases, the vibration decreases and tends to be optimal.

Table 2: Relationships between hidden layer neurons and errors

Hidden layer neuron	Training error (%)	Testing error (%)	Hidden layer neuron	Training error (%)	Testing error (%)
4	12.6334	12.0542	11	8.2683	7.0547
5	10.4325	10.1453	12	7.5876	6.2482
6	10.0836	9.2695	13	7.0218	5.0624
7	9.5836	9.0521	14	6.6482	6.1486
8	9.0452	8.8485	15	5.8473	5.1862
9	8.6142	8.5858	16	5.8593	5.8864
10	8.056	8.1524	17	5.7324	5.3485

The data set is acquired by sampling model in section 3.2. The sampling times is 500. 400 sets of data are used as training set and the others are used as test set. The data of hidden layer neurons are set to 4-17. Because the parameters of four output neurons involved in this paper are equally important in motor performance evaluation, the training and testing results are shown in Tab.2 according to the average weight. The error data show that with the increase of the number of hidden layer neurons, the training error and test error decrease gradually, but the test error fluctuates when the number of hidden layer neurons exceeds 11. The number of hidden layer neurons can be set at 13-15 in the comprehensive comparison error data, which is selected as 15 in this paper.

3.4 Chaos artificial fish swarm algorithm

In this paper, the Chaos Artificial Fish Swarm Algorithms (CAFSA) algorithm is used to optimize BPNN, and a PMSM motor parameter identification model based on CAFSBPNN algorithm is proposed.

Relevant definitions of CAFSBPNN algorithms

The state of individual AF fish in artificial fish swarm at time t is defined as: $X_S(t) = (x_1^S(t), x_2^S(t), \dots, x_D^S(t))$, ($S = 1, 2, \dots, AF_Num$).

where AF_Num is the size of artificial fish, D is the state dimension of $X_S(t)$ (the sum of connection weights and thresholds of BPNN), $x_i^S(t)$ ($i = 1, 2, \dots, D$) are variables waiting for optimization. $E_S(t) = \frac{1}{e_S(t)}$ is the current food concentration of S th artificial fish.

$Visual$ is the visual range of artificial fish (perceived distance), $Step$ is moving step of artificial fish, Δ is crowding factor.

CAFSBPNN is a three-layer BPNN network with one hidden layer, in which the number of neurons in the input layer (L_{in}) is $n = 9$, the number of neurons in the hidden layer (L_h) is $m = 15$, and the number of neurons in the output layer (L_o) is $l = 4$.

The dimension D of $X_S(t)$ of artificial fish can be calculated as: $D = m(n + 1) + l(m + 1) = 15 * 10 + 4 * 16 = 216$.

The connection weights of $L_{in} \rightarrow L_h$ and $L_h \rightarrow L_o$ in BPNN are assigned to the front part of $X_S(t)$, and the thresholds of neurons in L_h and L_o are stored in the back part of $X_S(t)$.

Individual fish $X_S(t)$ contains the connection weights and thresholds needed to construct BPNN network, which can represent a BPNN.

When AF is initialized, AF_Num of the artificial fish are put in the range of [-1,1] by chaotic random mode.

Initial fish food concentration $E_S(t) = \frac{1}{e_S(t)}$, where $e_S(t) = \frac{WMSE}{N}$, $WMSE$ is the global weighted mean square error, and N is the dimension of training sample set.

The smaller the error $e_S(t)$ between the expected output value and the actual output value of the network, the higher the food concentration $E_S(t)$ of the artificial fish, and the better the performance of the neural network constructed by the artificial fish.

The distance d_{PQ} between any two artificial fish $X_P(t)$ and $X_Q(t)$ in AF is calculated as follows:

$d_{PQ} = \frac{\sum_{i=1}^D |X_i^P(t) - X_i^Q(t)|}{D}$, $X_i^P(t)$, $X_i^Q(t)$ is the corresponding state value of two artificial fish.

When $d_{PQ} < Visual$, $X_P(t)$ and $X_Q(t)$ are the corresponding state values of two artificial fish.

Behavior description of artificial fish swarm algorithms

(a) *Prey behavior*: Fish tend to move towards high food concentration in water through their sensory organs.

Artificial fish $X_i(t)$ traverses all the partner fish in the search field, and the number of partners Frd_Num was calculated.

At first, the target fish $X_{target}(t)$ is assigned $X_i(t)$, and the food concentration is compared with that of partner fish $X_j(t)$ in each traverse. If $E_{target}(t) < E_j(t)$, the target fish to be searched is recorded as partner fish $X_j(t)$.

After searching all the partner fish, if the target fish $X_{target}(t)$ is found, then the artificial fish $X_i(t)$ moves one step to the $X_{target}(t)$ according to: $X_i(t+1) = X_i(t) + rounds() \cdot step \cdot \frac{X_{target}(t) - X_i(t)}{d_{targeti}}$; otherwise, the artificial fish $X_i(t)$ moves one step to the cluster center.

(b) *Swarm behavior*: Fish like to gather, forage collectively and avoid risks. Assuming that the current state of artificial fish is artificial fish $X_i(t)$, the number of companion fish Frd_Num and the central position $X_c(t)$ are obtained by traversing the search field.

If $\frac{E_c(t)}{Frd_Num} > \Delta E_i(t)$, it means that the food concentration in the partner center is high but not too crowded.

It can move forward to the center according to: $X_i(t+1) = X_i(t) + rounds() \cdot step \cdot \frac{X_c(t) - X_i(t)}{d_{ci}}$, otherwise preying behavior will be carried out.

(c) *Fellow behavior*: Some individuals in the fish swarm find the food and share the location, and others follow and arrive at the food point to eat together.

Assuming that the current state of artificial fish is $X_b(t)$, the number of partners in the field of vision is Frd_Num and the highest concentration of food is $X_b(t)$.

If $\frac{E_b(t)}{Frd_Num} > \Delta E_i(t)$, it shows that the partner with the highest food concentration is not too crowded at $X_b(t)$.

At this time, $X_i(t)$ can move towards partner $X_b(t)$ according to: $X_i(t+1) = X_i(t) + rounds() \cdot step \cdot \frac{X_b(t) - X_i(t)}{d_{bi}}$; otherwise, preying behavior will be carried out.

(d) *Moving behavior*: When the individual fish $X_i(t)$ in the fish swarm finds that there is no other partner around them, it can move randomly to the next position within its field of vision according to:

$X_i(t+1) = X_i(t) + \text{rounds}() \cdot \text{step}$, thus widening the range of swarming, and further exploring for obtaining global optimum.

(e) *Bulletin board*: Update and preserve the highest food concentration and the corresponding individual fish status. In the iteration traversal process, when the individual fish food concentration is higher than the bulletin board record, the bulletin board is updated.

Chaotic search

Chaotic phenomena refer to irregular and unpredictable behaviors in non-linear systems, which are ergodic and random. When chaotic search is introduced into AFSA algorithm, its ergodicity can make the fish swarm search range include the whole target area, and its randomness is conducive to the search process breaking away from local extremum and tending to global optimum, which improves the search efficiency of AFSA algorithm and shortens the convergence time of global optimization.

Typical chaotic systems include Logistic mapping, Lorenz system and Henon map. In this paper, one-dimensional logistic chaotic system is used as the random motion behavior required in the search process of AFSA.

Definitions are as follows: $y_{k+1} = f(\mu, y_k) = \mu y_k(1 - y_k)$, where, $y_k \in (0, 1)$ and it is the value of y after k th iterations, and μ is the control parameter of the system.

When $\mu = 4$, the system is in a completely chaotic state, at which time y_k can not repeat all the values between $(0, 1)$.

Logistic chaotic system optimizes the activities of artificial fish swarm.

It means that the generation of all random numbers includes the initialization of artificial fish and the activities of fish swarm. Therefore, the following provisions are made for artificial fish swarm:

(a) The chaotic system generates the initial artificial fish. There are 216 initial connection weights and thresholds to be optimized in the parameter identification model of permanent magnet synchronous motor based on CAFSNNA.

For the i -th Artificial Fish $X_i(t)$, the chaotic variable $y_{ik}(k = 1, 2, \dots, 216)$ is generated by using the logistic system, and the initial value $X_i(0)$ is set accordingly.

If the range of parameters to be identified is (a, b) , the initial state of artificial fish $X_i(0)$ is: $X_i(0) = (x_1^i(0), x_2^i(0), \dots, x_{216}^i(0))$, where $x_k^i(0) = a_i + (b_i + a_i)y_{ik}$.

Similarly, AF_Num artificial fish can be produced.

(b) The random number function $\text{rounds}()$ used in formula (14-17) is generated by logistic chaotic system when calculating the preying, swarming, following and moving behavior of artificial fish swarm.

4 Process analysis of PMSM motor parameter identification network algorithm based on CAFSPNNA

4.1 Network optimization algorithm for PMSM motor parameter identification based on CAFSBPNN

CAFSPNN includes two parts for PMSM motor parameter identification. In the early stage, the superior global optimization ability of chaotic artificial fish swarm is used to quickly approach the global optimal point. In the later stage, the fast local convergence of BPNN neural

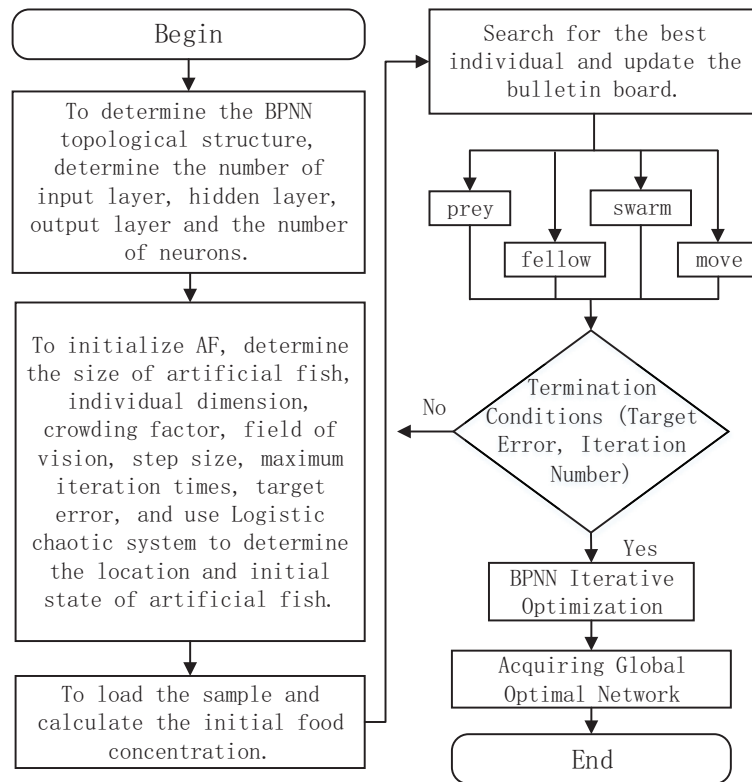


Figure 4: Procedure of PMSM motor parameter identification based on CAFSBPNN

network is used to complete the final global optimal point. The specific steps are as follows (see Fig. 4).

(1) Initialize BPNN: According to the PMSM motor parameter evaluation model, the BPNN network topology structure is determined: the number of input layer, hidden layer, output layer and the number of their respective neurons.

(2) Initialize CAFS: According to the topological structure of BPNN network, the connection weights and thresholds are determined. Set the initial state value of artificial fish: fish size(AF_Num), individual fish state dimension(D), visual range($Visual$), moving step($step$), crowding factor(Δ), maximum iteration number(i_{max}), target error($WMSE_{max}$).

Logistic chaotic system is used to determine the position and initial state of artificial fish. The initial position of individual fish $X_i(0)$ and corresponding food concentration $E_i(0)$ were calculated by loading samples data.

(3) Update bulletin board: The highest food concentration of individual fish was selected by traversing comparison, and the Bulletin Board was judged and updated.

(4) Behavior selection of AF: Fish swarm chooses and executes four kinds of activities: preying, following, swarming and moving. Logistic chaotic system is used to enter the next optimal position.

(5) CAFS termination condition judgment: According to the Bulletin Board, the optimal food concentration and the number of iterations, it is judged whether the CAFS termination condition of CAFSNNA optimization is satisfied, and then it is transferred to the later BPNN optimization, otherwise the next step (3) is to continue the fish optimization.

(6) BPNN optimization: Transfer to the BPNN iterative optimization process, using the aforementioned BPNN back propagation iteration weight updating method until the final opti-

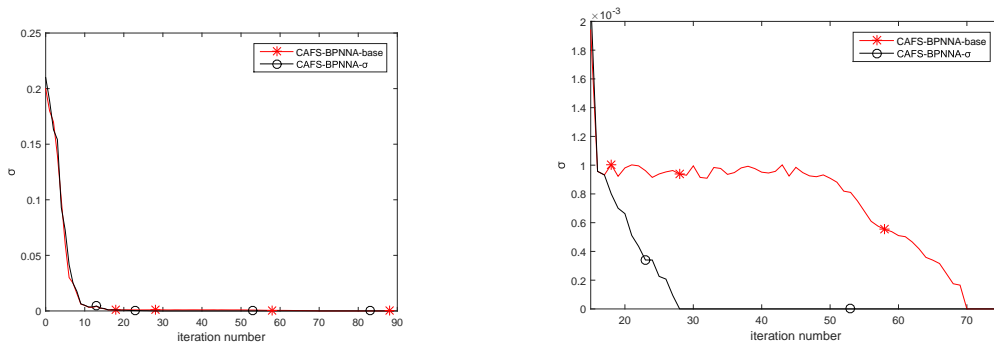


Figure 5: Aggregation degree σ of optimized iterative population based on CAFSBPNNa

mization conditions are satisfied to obtain the global optimal network.

4.2 Selection of switching opportunity for two swarm intelligence algorithms in CAFSBPNNa network optimization

In the identification model, the optimization process of BPNN network parameters is completed by CAFS and BPNN algorithms in two stages. If the switching point is too late, the CAFS algorithm will produce blind search when it approaches the global extremum point in the later stage, which will affect the convergence speed. On the contrary, if the switching point is too early and enters the BPNN search process too early, it will lead to premature convergence to the local extremum point, which will affect the convergence accuracy.

Therefore, accurately grasping the switching time of the two algorithms is very important for the whole optimization. In the traditional CAFS algorithm, the termination conditions are mainly determined by the number of iterations and the target error, but in the optimization process of CAFSNNA fusion algorithm, it is difficult to accurately judge whether it has entered the optimal terminal of CAFS fast convergence by only a single system target error.

In the later stage of CAFS algorithm, the individual fish in the population are clustered near the global extremum because of their preferential characteristics, so the individual aggregation degree of the population is obviously increased, and the individual fitness value of each individual fish will also approach the average fitness value of the system.

For this reason, the aggregation degree defined by formula (7) is introduced to judge the aggregation of individual fish [9].

$$\sigma = \frac{1}{D} \sum_{j=1}^D \left(\frac{f_j - f_{avg}}{f} \right)^2 \quad (7)$$

In the formula, f_j is the fitness function value of individual fish $X_j(t)$, f_{avg} is the average fitness value of population, and f is the normalized parameter. In the early stage of identification, the individual fish in the fish swarm have great difference, including loose distribution, low clustering degree and large value.

In the later stage of optimization, the fish flock clustering degree increases and aggregation degree σ is higher. When σ is less than the threshold value, aggregation degree of the fish swarm is very high. The fusion algorithm has entered the later stage of rapid convergence of CAFS, and then it can be turned into BPNN for precision optimization.

Fig.5 is the change curve of aggregation degree σ in the iteration process of CAFSBPNNa, and CAFS-BPNNa-base is the original curve of iteration optimization. CAFS-BPNNa- σ is an

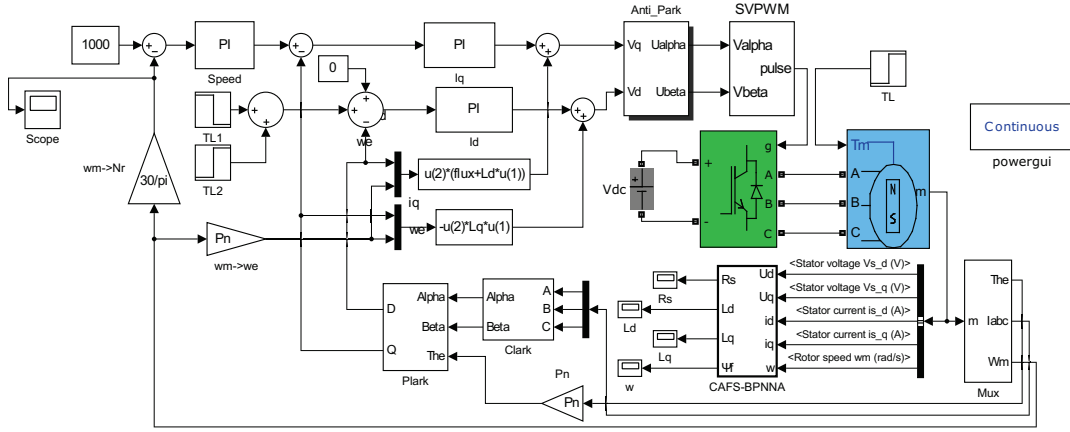


Figure 6: The block diagram of PMSM speed control system based on CAFS-BPNN

iterative curve with the judgment of population aggregation degree σ . After the first curve is below 0.0001, the CAFS fish swarm optimization enters the disordered state until it reaches the preset iteration number of 50 and then turns to BPNN to search for the global extremum quickly.

The latter iteration curve adds the optimum iteration of judging the degree of population aggregation σ to switch directly to another BPNN optimization algorithm after σ drops below 0.0001, and reaches the extremum point after fast convergence.

The comparison results show that the iteration optimization which combines the judgment of population aggregation degree σ can effectively avoid the disordered swimming in the later optimization stage of the fish swarm algorithm and improve the convergence speed of the fusion algorithm.

5 Result and analysis

5.1 Experimental setting of PMSM motor parameter identification

Table 3: Nominal parameters of PMSM motors

Parameter	Value	Parameter	Value	Parameter	Value
P/W	2600	$\omega/r \cdot \text{min}^{-1}$	2000	R_s/Ω	2.875
ψ_f/Wb	0.175	I/A	4	$T/N \cdot m$	5
L_d/mH	8.5	$J/kg \cdot m^2$	$0.48e^{-5}$	U/V	380
$\omega_{max}/r \cdot \text{min}^{-1}$	2500	L_q/mH	8.5	P_p/p	4

The PMSM speed control system based on speed closed-loop control regulation is constructed on the motor control platform, as shown in Fig.6. The parameters of PMSM motor are as shown in Tab.3.

The range of parameters to be determined is $R_s \in (0, 5)$, $L_d \in (0, 015)$, $L_q \in (0, 015)$, $\psi_f \in (0, 3)$.

The motor adopts SVPWM control strategy and the pulse current(-2A) injected into the d-axis at 0.1s lasts 5 ms. Fig.7 shows the speed tracking curve of the motor when the current pulse is injected at $\omega = 2000r/min$.

The data show that the speed fluctuation of the motor after the instantaneous pulse input is less than 0.5%, and the influence on the system can be neglected. Data0 and Data1 are generated

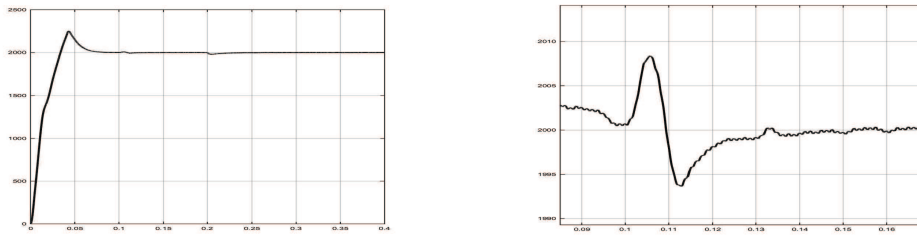


Figure 7: PMSM motor speed ω at pulse current $I_d=-2A$

by sampling $\{u_d, u_q, i_d, i_q \text{ and } \omega\}$ before and after pulse current injection, and 500 groups are sampled as training and testing sets of CAFSBPNN.

5.2 Experimental setting of PMSM motor parameter identification

The parameters of CAFSNN algorithm are as follows: the input neuron number $n = 9$; the hidden neuron number $m = 15$, and Tansig taken as transfer function; output neuron number $l = 4$, and linear purelin taken as transfer function. The training error is calculated by $WMSE$.

Connection weight updating is calculated by cumulative error method of adaptive inertial momentum. Intelligent fish swarm settings include: the fish swarm number $AF_Num = 30$, individual fish size dimension $D = 216$, visual field range $Visual = 1$, maximum step size $Step = 0.5$, crowding factor $\Delta = 14$, maximum iteration number $imax = 400$, training sample 400 groups, minimum allowable training error is 0.001.

In order to compare the performance of PMSM motor parameter identification based on CAFSBPNN algorithm, RLS and PSO are introduced for analogy identification. RLS parameter configuration: learning factor $C_1 = C_2 = 2$, inertia weight $W = 0.5$, the maximum number of iterations is 400. PSO parameter configuration: estimate $\hat{\Theta}(0) = 1 \frac{n}{P_0}$, covariance $P_0 = p_0 I, p_0 = 10^6$, the maximum number of iterations is 400.

5.3 Training error analysis based on motor speed and torque

The speed and torque of PMSM motor are the two main indexes that affect the performance of the motor. Therefore, in the experiment, the motor is set in different conditions of speed and torque to compare the identification ability of various intelligent algorithms for motor parameters. Fig.8 is PMSM motor speed $\omega = 2000r/m$ and load torque is $2N \cdot m$. The three intelligent algorithms in this paper track and compare the waveforms of motor parameter identification effect and iteration times. Tab.4 gives the identification error data of three algorithms for motor under normal speed of $2000r/m$ and maximum speed of $2500r/m$, as well as Torque is $2N \cdot m$ and $3N \cdot m$.

Fig.8 shows that RLS has the worst convergence performance. It usually needs 150 iterations to reach the convergence point of all identification parameters. PSO has better convergence effect, but its convergence accuracy is not high compared with other two algorithms. Compared with RLS and PSO, the proposed CAFSBPNN algorithm has better convergence time and accuracy.

When the torque value is fixed to $2N \cdot m$ and the speed is adjusted to the maximum speed, the total training error of the three algorithms decreases, among which the RLS decreases the most, the CAFSBPNN algorithm changes the least and the identification accuracy is the highest. When the speed is fixed at $2000r/m$ and the torque is increased by $1N \cdot m$, the single error of PSO arithmetic fluctuates, the errors of R_s and L_d become larger, the errors of L_q and ψ_f become smaller, and the total error increases. The ψ_f of RLS and CAFSBPNN is basically constant,

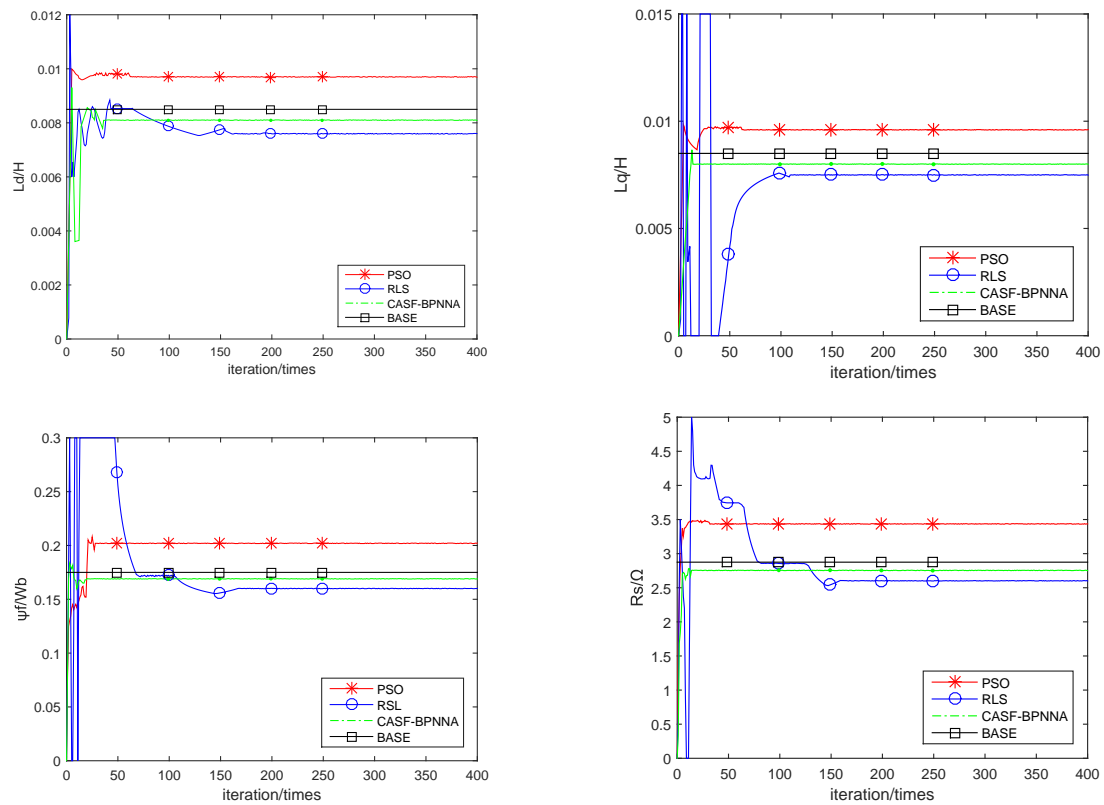


Figure 8: PMSM motor parameter identification results ($\omega = 2000r/min, T = 2N \cdot m$)

and the total training error decreases with the decrease of R_s, L_d and L_q . CAFSBPNN has the smallest change and the highest accuracy.

In summary, compared with RSL and PSO, CAFSBPNN is superior to the other two reference algorithms in parameter identification under uniform working conditions and error fluctuation under changing working conditions, and it always shows good convergence and identification accuracy.

Table 4: PMSM motor parameter identification error

Working condition	Algorithm	R_s/Ω	L_d/mH	L_q/mH	ψ_f/Wb	Error
$T = 2N \cdot m$ $\omega = 2000r/min$	PSO	0.554/19.3%	1.185/13.9%	1.113/13.1%	0.009/5.2%	12.8%
	RSL	0.741/25.8%	1.343/15.8%	1.181/13.9%	0.078/44.8%	25.1%
	CAFBNNA	0.132/4.6%	0.365/4.3%	0.467/5.5%	0.007/4.5%	4.7%
$T = 2N \cdot m$ $\omega = 2500r/min$	PSO	0.477/16.6%	0.552/6.5%	1.147/13.5%	0.012/7.1%	10.9%
	RSL	0.293/10.2%	1.011/11.9%	0.629/7.4%	0.072/41.3%	17.7%
	CAFBNNA	0.129/4.5%	0.229/2.7%	0.382/4.5%	0.006/3.8%	3.8%
$T = 3N \cdot m$ $\omega = 2000r/min$	PSO	0.684/23.8%	1.198/14.1%	0.824/9.7%	0.008/4.9%	13.1%
	RSL	0.514/17.9%	1.037/12.2%	0.663/7.8%	0.081/46.8%	21.1%
	CAFBNNA	0.117/4.1%	0.365/4.3%	0.314/3.7%	0.007/4.4%	4.1%

6 Conclusion

Aiming at the identification of PMSM motor parameters R_s, L_d, L_q and ψ_f , the full rank identification model of motor parameters is derived based on PMSM motor voltage equation and flux equation. The feasibility of motor parameters identification by d-axis current injection in steady state and the sampling method of sample data set are analyzed. A method of parameter identification of PMSM motor by optimizing BPNN with CAFS is proposed. Compared with PSO and RLS, experiments show that the proposed CAFSBPNN algorithm has high accuracy and short convergence time for motor parameter identification, and has the stability of identification when working conditions are changed.

The specific advantages are as follows:

(1) The CAFSBPNN algorithm fully coordinates the local and global search performance advantages of BPNN and CAFS, speeds up the convergence speed and improves the convergence of motor parameter identification.

(2) The application of chaotic search reduces the sensitivity of initial value of parameter identification and enhances the robustness of parameter setting in the learning process.

(3) The CAFSBPNN algorithm has good stability, and can maintain good identification effect under different speed and torque conditions.

CAFSBPNN algorithm has good versatility. It can be used not only for parameter identification of PMSM motor, but also for parameter identification and on-line tracking of other motors such as stepping motor, induction motor and precision motor. CAFSBPNN algorithm proposed in this paper is more computational than on-chip system resources. The system adopts online sampling and periodic uploading of motor operation data. The parameters of identification network are optimized and updated by off-line optimization and remote download. Later on-chip system is implemented. In the future, the online optimization and updating methods of network parameters are further studied on the basis of improving the performance of on-chip system and optimizing the time and space complexity of algorithm.

Acknowledgment

Financial supports from the Priority Academic Program Development of Jiangsu Higher Education Institutions.

Bibliography

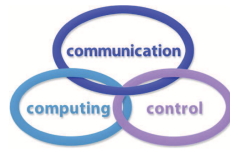
- [1] Babak, N.M.; Meibody-Tabar, F.; Sargos F.M.(2004). Mechanical sensorless control of PMSM with online estimation of stator resistance, *IEEE Transactions on Industry Applications*, 40(2), 457-471, 2004.
- [2] Boileau, T.; Leboeuf, N.; Nahid-Mobarakeh, B. et al.(2011). Online Identification of PMSM Parameters: Parameter Identifiability and Estimator Comparative Study, *IEEE Transactions on Industry Applications*, 47(4), 1944-1957, 2011.
- [3] Bose, B. K.(2009). Power Electronics and Motor Drives Recent Progress and Perspective, *IEEE Transactions on Industrial Electronics*, 56(2), 581-588, 2009.
- [4] Chen, Z.; Zhong, Y.; Li J.(2011). Parameter identification of induction motors using Ant Colony Optimization, *IEEE World Congress on Computational Intelligence*, IEEE.2011.

- [5] Da, Y.; Shi, X.; Krishnamurthy, M.(2013). A New Approach to Fault Diagnostics for Permanent Magnet Synchronous Machines Using Electromagnetic Signature Analysis, *IEEE Transactions on Power Electronics*, 28(8), 4104-4112, 2013.
- [6] Donoso, Y.; Montoya, G. A.; Solano F. (2015). An Energy-Efficient and Routing Approach for Position Estimation using Kalman Filter Techniques in Mobile WSNs, *International Journal of Computers Communications & Control*, 10(4), 500-507, 2015.
- [7] Gao, D.Q.(1998). On Structures of Supervised Linear Basis Function Feedforward Three-Layered Neural Networks, *Chinese Journal of Computers*, 21(1), 81-86, 1998.
- [8] Hajisalem, V.; Babaie, S.(2018). A Hybrid Intrusion Detection System Based on ABC-AFS Algorithm for Misuse and Anomaly Detection. *Computer Network*, 136, 37-50, 2018.
- [9] He, S.; Wu, Q. H.; Saunders, J. R.(2009). Group Search Optimizer - An Optimization Algorithm Inspired by Animal Searching Behavior, *IEEE Transactions on Evolutionary Computation*, 13(5), 973-990, 2009.
- [10] Kim, J.; Jeong, I.; Lee, K.(2014). Fluctuating Current Control Method for a PMSM Along Constant Torque Contours, *IEEE Transactions on Power Electronics*, 29(11), 6064-6073, 2014.
- [11] Liu K.; Zhang Q.; Chen J.; et al.(2011). Online Multiparameter Estimation of Nonsalient-Pole PM Synchronous Machines with Temperature Variation Tracking, *IEEE Transactions on Industrial Electronics*, 58(5), 1776-1788, 2011.
- [12] Liu, K.; Zhu, Z.Q.; Stone, D.A.(2013). Parameter Estimation for Condition Monitoring of PMSM Stator Winding and Rotor Permanent Magnets, *IEEE Transactions on Industrial Electronics*, 60(12), 5902-5913, 2013.
- [13] Liu, Q.; Hameyer, K.(2015). A fast online full parameter estimation of a PMSM with sinusoidal signal injection, *Energy Conversion Congress & Exposition*, IEEE, 2015.
- [14] Liu, Z.H.; Wei, H.L.; Zhong, Q.C.; et al.(2017). Parameter Estimation for VSI-Fed PMSM based on a Dynamic PSO with Learning Strategies. *IEEE Transactions on Power Electronics*, 32(4), 3154-3165, 2017.
- [15] Lu, K.; Vetuschi, M.; Rasmussen, P.O. et al.(2010). Determination of High-Frequency d- and q- axis Inductances for Surface-Mounted Permanent-Magnet Synchronous Machines, *IEEE Transactions on Instrumentation & Measurement*, 59(9), 2376-2382, 2010.
- [16] Mirchandani, G.; Cao, W.(1989). On hidden nodes for neural nets, *IEEE Transactions on Circuits and Systems*, 36(5), 661-664, 1989.
- [17] Omar, S.H.; Roberto, M.R.; Jose, R.M.; Hayde, P.B.(2015). Parameter Identification of PMSMs Using Experimental Measurements and a PSO Algorithm, *IEEE Transactions on Instrumentation & Measurement*, 64(8), 2146-2154, 2015.
- [18] Pellegrino, G.; Vagati, A.; Guglielmi, P. et al.(2011). Performance Comparison Between Surface-Mounted and Interior PM Motor Drives for Electric Vehicle Application, *IEEE Transactions on Industrial Electronics*, 59(2), 803-811, 2011.
- [19] Sengottuvelan, P.; Rasath, N.(2016). BAFSA: Breeding Artificial Fish Swarm Algorithm for Optimal Cluster Head Selection in Wireless Sensor Networks, *Wireless Personal Communications*, 94(4), 1-13, 2016.

- [20] Shi, Y.; Sun, K.; Huang, L. et al.(2012). Online Identification of Permanent Magnet Flux Based on Extended Kalman Filter for IPMSM Drive With Position Sensorless Control, *IEEE Transactions on Industrial Electronics*, 59(11), 4169-4178, 2012.
- [21] Wei, C.; Xin, L.; Mei, C.(2009). Suboptimal Nonlinear Model Predictive Control Based on Genetic Algorithm, *International Symposium on Intelligent Information Technology Application Workshops*, IEEE, 2009.
- [22] Xiao, X.; Chen, C.; Zhang, M.(2010). Dynamic Permanent Magnet Flux Estimation of Permanent Magnet Synchronous Machines, *IEEE Transactions on Applied Superconductivity*, 20(3), 1085-1088, 2010.
- [23] Yan, H.; Wang, Y. R.; Shi, H. X.; Li, Q.; Zeng, Y. S.; Jaini, R.(2019). Solid-Liquid Flow of Axial Flow Pump in Loop Reactor and Operating Control with Single Invert, *International Journal of Simulation Modelling*, 18(3), 464-475, 2019.
- [24] Zhang, D.(2017). High-speed Train Control System Big Data Analysis Based on Fuzzy RDF Model and Uncertain Reasoning, *International Journal of Computers Communications & Control*, 12(4), 577-591, 2017.
- [25] Zhang, D.; Sui, J.; Gong, Y.(2017). Large scale software test data generation based on collective constraint and weighted combination method, *Tehnicki Vjesnik*, 24(4), 1041-1050, 2017.
- [26] Zhang, H.P.; Ye, J.H.; Yang, X. P.; Muruve, N.W.; Wang, J.T.(2018). Modified Binary Particle Swarm Optimization Algorithm in Lot-Splitting Scheduling Involving Multiple Techniques, *International Journal of Simulation Modelling*, 17(3), 534-542, 2018.

Studies in Informatics and Control: A Bibliometric Analysis from 2008 to 2019

Y. Li, Z.S. Xu, X.X. Wang, F.G. Filip



Yang Li

Business School
Sichuan University, China
No. 24, South section 1 of the first ring road, Chengdu, 610064, China
liyang_ly18@163.com

Zeshui Xu*

Business School
Sichuan University, China
No. 24, South section 1 of the first ring road, Chengdu, 610064, China
*Corresponding author: xuzeshui@263.net

Xinxin Wang

Business School
Sichuan University, China
No. 24, South section 1 of the first ring road, Chengdu, 610064, China
wangxinxin_cd@163.com

Florin Gheorghe Filip

Romanian Academy
125 Calea Victoriei, Bucharest, 010071, Romania
ffilip@acad.ro

Abstract: As an international scientific journal, *Studies in Informatics and Control (SIC)* covers the field of Information Technology (IT) and topics related to research areas, as well as important applications in IT, with particular emphasis on Advanced Automatic Control, Modeling and Optimization. *SIC* has greatly contributed to the areas where it involves since its first online publication way back in 1992. This paper sets out to analyze the structure and the underlying trend of the journal by making use of bibliometric methods. Firstly, the classical indicators are provided to illustrate the performance of the journal. This current study performs an in-depth analysis of the most productive and the most influential authors, institutions, and countries/regions, as well as the most cited research works published in *SIC*. Secondly, the visualization tools VoS viewer and CiteSpace are used to create scientific maps that may explain the structure of the journal in an intuitionistic way. In the science mapping, the co-citation maps, and the co-authorship networks of various items (such as authors, institutions, and countries/regions) are conducted. Also, the bursts detection of these items are derived. The co-occurrence of keywords and their bursts detection and timeline review are shown, respectively. Finally, some conclusions are given. This paper provides a comprehensive and visual understanding of this well-regarded scientific journal.

Keywords: *Studies in Informatics and Control*, bibliometric analysis, science mapping analysis, Web of Science, information technology.

1 Introduction

As an international scientific journal, *Studies in Informatics and Control (SIC)* is one of the leading journals in the field of Information and Communication Technologies (I&CT) in Romania. It provides important perspectives on topics relevant to Information Technology (IT), with an emphasis on useful applications in the most important areas of IT such as Automatic Control, System Modeling and Optimization. The journal was first published in 1989 under the name "Studies in Computers and Informatics" as a publication of the Institute for Computer Technique and Informatics (ITCI). It was renamed as the current name *SIC* in 1990. In 1992, the journal became an international one with an Editorial Board of scientists from 17 countries and prof. Theodore Williams of Purdue University played a major role in shaping journal profile. Since 1992, *SIC* has been published both in print and online by the Romanian Institute for R&D in Informatics, ICI Burcharest under the auspices of the Romanian Academy [12]. According to the current homepage of the journal (<https://sic.ici.ro/about-sic/>), this quarterly journal has been included within the coverage of Inspec database (since 1993), DOAJ (since 1996), Google Scholar (since 2006) and Philadelphia-based Institute of Scientific Information (ISI Thomson-Reuters) / Clarivate Analytics - Science Citation Index Expanded (SCIE) (since 2008), Scopus (since 2010) and other relevant academic databases and search engines listings. The journal impact factor in 2018 was 1.347 according to the Journal Citation Reports (JCR) published in Web of Science (WoS). The ranking of the journal in the research field of automation & control system was 45 out of 62 while in the field of operations research & management science it was 53 out of 84. Prof. F.G. Filip, a member of the Romanian Academy, is the founder and editor-in-chief of the journal.

Bibliometrics analyze patterns that appear in the publication and communication of documents by using mathematical and statistical methods [11]. It provides a systematic, transparent, and reproducible review to a large body of information by providing a structural analysis [1]. Bibliometric methods are used in various fields for the purpose of research evaluation [19]. Because bibliometrics is effective in revealing the evaluation of a research direction, it has been applied in many fields, such as economy [10], management [21], innovation [5,13], decision support [14] and entrepreneurship [16,17]. In addition, it also has been widely used to evaluate a certain journal, including *European Journal of Operational Research* [15], *Information Sciences* [29], *IEEE Transaction on Fuzzy Systems* [28], *International Journal of Intelligent Systems* [18], *Knowledge-Based System* [8], *Technological and Economic Development of Economy* [27], *International Journal of Strategic Property Management* [31], *International Journal of Computers Communications & Control* [25], etc.

The bibliometric evaluation comprises two procedures [20]: performance analysis and science mapping. The performance analysis evaluates the performance of different scientific actors based on the number of publications and citations [8] and it is illustrated by a series of bibliometric indicators. The science mapping mostly aims at displaying the structure, evaluation and dynamic aspects of scientific research [2,3]. In fact, many visualization tools or softwares are created to make science mapping analysis, and Cobo et.al [7] made a comparison of them. Two of the most common science mapping softwares, VoS viewer and CiteSpace are applied in this paper. VoS viewer represents the bibliometric map in an easy-to-interpret way [24] and can construct the maps of co-citation, co-authorship, co-occurrence, citation and bibliographic coupling. Besides, burst-detection provided by CiteSpace helps scholars to identify emergent terms regardless of how many times their host documents are cited [6]. The hot topics and research trends can be detected from the time-line view of CiteSpace.

The main contribution of this paper consists in performing a bibliometric analysis of the research works published in *SIC*. The bibliometric indicators are applied to various levels such

as authors, institutions, and countries/regions. The analysis of co-citation, co-authorship and co-occurrence concerning various items, as well as the burst detection and time-line view are presented in science mapping. The rest of this paper is structured as follows: Section 2 describes the source of data used in this paper, and the performance analysis of *SIC* is illustrated in Section 3. In Section 4, scientific maps and relative evaluation are presented. Furthermore, some conclusions are given in Section 5.

2 Data description

According to the website of *SIC* (<https://sic.ici.ro/>), the journal has been included within the coverage of Clarivate Analytics - SCIE (since 2008). Clarivate Analytics is a company with an entrepreneurial mission to help customers reduce the time from new ideas to life-changing innovations. SCIE created as *SCI* in 1964 indexes more than 9,200 of the world's most impactful journals across 178 scientific disciplines. And it contains more than 53 million records and 1.18 billion cited references way back from 1900 to 2019. Since the SCIE is included in the WoS Core Collection, relative data have been downloaded from WoS Core Collection SCIE (<https://apps.webofknowledge.com/>) to analyze the performance of research works published in the journal from 2008 to November 1, 2019. With the database set at WoS Core Collection, the citation indexes set at SCIE and the timespan set at 2008-2019, full records and cited references of documents in *SIC* are searched and exported in plain text form in November 1, 2019. The performance analysis and science mapping analysis of the journal are based on 527 papers that have been searched and their relative information derived from WoS.

3 Performance analysis of *SIC*

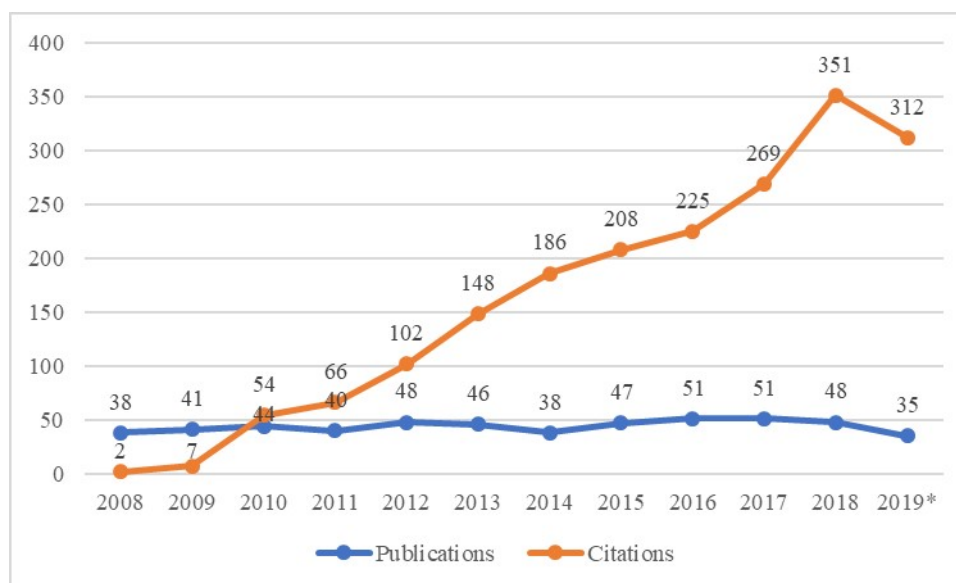
In this section, the annual publications and citations of the journal are described. Depending on the bibliometric indicators, the most productive and influential authors, countries/regions, and institutions are exhibited, as well as the most cited documents.

3.1 Annual publications and citations

Since 2008, 527 research works have been published in *SIC*, among which 517 documents are articles, which accounts for 98.102% of the total number of research works. The other four types of the documents are editorial materials (6; 1.139%), proceeding papers (6; 1.139%), reviews (3; 0.569%) and biographical items (1; 0.19%).

It can be seen from Figure 1 that, the annual publications in *SIC* are constant. The minimum number of publications was 38 in 2008 and 2014, and the maximum number of publications was 51 in 2016 and 2017. Since *SIC* was included within the coverage of Clarivate Analytics - SCIE in 2008, the number of annual citations of this scientific journal keeps to increase rapidly and exceeded 50 in 2010 and 100 in 2012 for the first time. A great augment of citations appeared in 2018. The number of citations is 351 in 2018, which is 82 higher than that in 2017 (269 citations). During the past 10 months of 2019, the research works in *SIC* has been cited 312 times, which is higher than the number of citations in 2017.

In order to illustrate the citation structure of the publications in *SIC*, the relative information is listed in Table 1. The number of publications (P), the number of citations (C), the number of cumulative publications and citations (CP and CC), the number of document whose number of citations is more than 50 (≥ 50), 30 (≥ 30), 20 (≥ 20), 10 (≥ 10), 5 (≥ 5) and 1 (≥ 1), H-index (the abbreviation of Hirsch-index) [9] and the total citations of annual publications (TC) are listed by year to evaluate performance.



* As of November 1, 2019.

Figure 1: Annual publications and citations from 2008 to 2019*.

The number of C became greater than that of P in 2010 for the first time and the number of CC is higher than the number of CP since 2012. It means that all the publications in *SIC* have been cited at least once on average. During the 12-year period, only 2 documents published in 2012 and 2015 are cited not less than 50 times. 6 of 527 documents are cited not less than 30 times, and 2 of the 6 documents published in 2013. 14 of 527 documents are cited not less than 20 times, and 4 of the 14 documents published in *SIC* in 2010. The 44 documents published in 2010 gained much attention and made much influence with the highest number of citations (254). 4 of the 44 documents are cited not less than 20 times, 8 of the 44 documents are cited not less than 10 times, and the H-index of the 44 documents is 9. These 3 indicators are the highest compared with them of other 11 years. The highest numbers of documents with number of citations not less than 30 and not less than 5 are in 2013. In the year of 2016, 44 of the 51 documents are cited at least once, which is the highest compared with other 11 years. Based on the above analysis, it can be found that the documents in 2010, 2012, 2013, 2015 and 2016 have greatly contributed to *SIC*.

3.2 The most productive and influential authors and documents

In this subsection, some bibliometric indicators concerning the publications and the citations are utilized to evaluate authors and documents.

The most productive and the most influential authors

Table 2 lists the top 8 productive authors who published not less than 10 articles in *SIC* since 2008. Some indicators such as P, the year of first publication (YFP), the year of latest publication (YLP), average publications (AP) and type of their research works, are shown in Table 2.

Benrejeb, M. is the most productive author who has published 13 documents in the journal since 2008. Thorsteinsson, G. from Iceland published 12 articles in this journal from 2008 to 2016 and the AP of him is 1.33. Niculescu, A. from Romania published 11 articles and 1 editorial

Table 1: Characteristics of annual publications from 2008 to 2019*.

Year	P	C	CP	CC	≥50	≥30	≥20	≥10	≥5	≥1	H-index	TC
2008	38	2	38	2	0	0	0	4	7	30	6	113
2009	41	7	79	9	0	0	1	3	10	35	6	147
2010	44	54	123	63	0	0	4	8	16	37	9	254
2011	40	66	163	129	0	1	1	2	11	37	6	162
2012	48	102	211	231	1	1	1	6	14	41	8	239
2013	46	148	257	379	0	2	2	7	17	39	8	247
2014	38	186	295	565	0	0	2	2	8	32	6	131
2015	47	208	342	773	1	1	1	4	10	39	5	192
2016	51	225	393	998	0	0	0	2	10	44	5	141
2017	51	269	444	1267	0	1	2	4	16	38	8	217
2018	48	351	492	1618	0	0	0	3	4	22	4	82
2019*	35	312	527	1897	0	0	0	0	0	5	1	5

* As of November 1, 2019.

Table 2: The top 8 productive authors in *SIC* from 2008 to 2019*.

Rank	Authors	Countries	P	YFP	YLP	AP	Type
1	Benrejeb, M	Tunisia	13	2008	2018	1.18	Article (13)
2	Thorsteinsson, G	Iceland	12	2008	2016	1.33	Article (12)
3	Niculescu, A	Romania	12	2008	2019	1.00	Article (11), Editorial material (1)
4	Page, T	England	11	2008	2013	1.83	Article (11)
5	Wang, H. P	China	11	2010	2019	1.10	Article (11)
6	Tian, Y	China	11	2014	2019	1.83	Article (11)
7	Borne, P	France	10	2008	2019	0.83	Article (10)
8	Radulescu, C. Z	Romania	10	2009	2019	0.91	Article (10)

* As of November 1, 2019.

material in *SIC* since 2008 and he published 1 document in the journal per year on average. The 2 authors with highest number of AP (1.83) is Page, T. from England and Tian, Y. from China. Page, T published his 11 articles in *SIC* during the period from 2008 to 2013, while Tian, Y. published 11 articles in the journal in the last 6 years. In terms of YFP, 5 of the top 8 productive authors started to publish in the journal since 2008. 5 of the top 8 productive authors continue to publish in the journal until 2019. 2 of the top 8 productive authors come from Romania, and another 2 of the 8 authors are from China. The other 4 authors come from Tunisia, Iceland, England and France, respectively. The research areas of all these 8 authors are operations research & management science and automation & control systems, according to the classification of WoS.

According to some common indicators about citations, Table 3 lists the top 3 influential authors with the number of citations higher than 100.

Table 3: The top 3 influential authors in *SIC* from 2008 to 2019*.

Rank	Authors	Country	P	C	AC	≥50	≥30	≥20	≥10	≥5	≥1	H-index
1	Zavadskas, E. K	Lithuania	8	170	21.25	1	2	3	5	7	7	7
2	Turskis, Z	Lithuania	5	128	25.6	1	2	3	4	4	4	4
3	Tuba, M	Serbia	7	115	16.43	1	2	3	4	4	6	4

* As of November 1, 2019.

In Table 3, P and C are the publications and citations of the authors respectively, and

AC represents the average citations of an author. Zavadskas, E. K. from Lithuania published 8 articles in *SIC* and obtained 170 citations in total. The H-index of him is 7, which means that there are 7 of his articles published in the journal cited at least 7 times. The AC of Turskis, Z. from Lithuania (25.6) is the highest, for he published only 5 articles in the journal and obtained 128 citations. All of the 3 authors have 1 article cited not less than 50 times and have 1 article has not been cited until November 1, 2019. There is some interesting information observed on the website of WoS. Only 2 articles in *SIC* are cited not less than 50 times, and 1 of them is a cooperative article published in June 2015 by Zavadskas, E.K, Turskis, Z. and Antucheviciene, J., while another one is the work of Bacanin, N and Tuba, M. The 2 articles written by the 3 authors with on citations are published in September 2019. 1 of the 2 articles is "A Novel Extended EDAS in Minkowski Space (EDAS-M) Method for Evaluating Autonomous Vehicles" [30] written by Zavadskas, E.K, Stevic, Z, Turskis, Z and Tomasevic, M. The another one is written by Tuba, M together with Tuba, E, namely article "Generative Adversarial Optimization (GOA) for Acute Lymphocytic Leukemia Detection" [23].

The most cited documents

To analyze the influence of the documents published in the journal during the period from 2008 to November 1, 2019, the top 6 cited publications which have been cited not less than 30 times, are listed in Table 4. The relative information, namely C, AC, the number of authors (NA), the type of document, the publication year, and research area (RA) of these publications are also listed.

Table 4: The top 6 influential documents in *SIC* from 2008 to 2019*.

Rank	Title	Authors	C	AC	NA	Type	Year	RA
1	Selecting a contractor by using a novel method for multiple attribute analysis: weighted aggregated sum product assessment with grey values (WASPAS-G). Artificial bee colony (ABC) algorithm for constrained optimization improved with genetic operators.	Zavadskas, E. K; Turskis, Z; Antucheviciene, J.	54	10.8	3	Article	2015	Automation & Control Systems; Operations Research & Management Science.
2	Multi-criteria assessment model of technologies.	Bacanin, N; Tuba, M.	50	6.25	2	Article	2012	Automation & Control Systems; Operations Research & Management Science.
3	A state of the art on supply planning and inventory control under lead time uncertainty. Simulation-based optimization using genetic algorithms for multi-objective flexible JSSP.	Zavadskas, E. K; Turskis, Z; Volvaciovas, R; Kildiene, S.	42	6.00	4	Article	2013	Automation & Control Systems; Operations Research & Management Science.
4	Adjusted fireworks algorithm applied to retinal image registration.	Dolgui, A; Ben A. O; Hnaien, F; Louly, M. A. O.	35	5.00	4	Article	2013	Automation & Control Systems; Operations Research & Management Science.
5		Nicoara, E. S; Filip, F. G; Paraschiv, N.	33	3.67	3	Article	2011	Automation & Control Systems; Operations Research & Management Science.
6		Tuba, E; Tuba, M; Dolicanin, E.	31	10.33	3	Article	2017	Automation & Control Systems; Operations Research & Management Science.

* As of November 1, 2019.

All of the 6 most influential documents are articles and their research areas cover Automation & Control Systems and Operations Research & Management Science. The 6 articles are results of cooperation among authors, and only 1 of them was written by 2 authors while the other 5 of

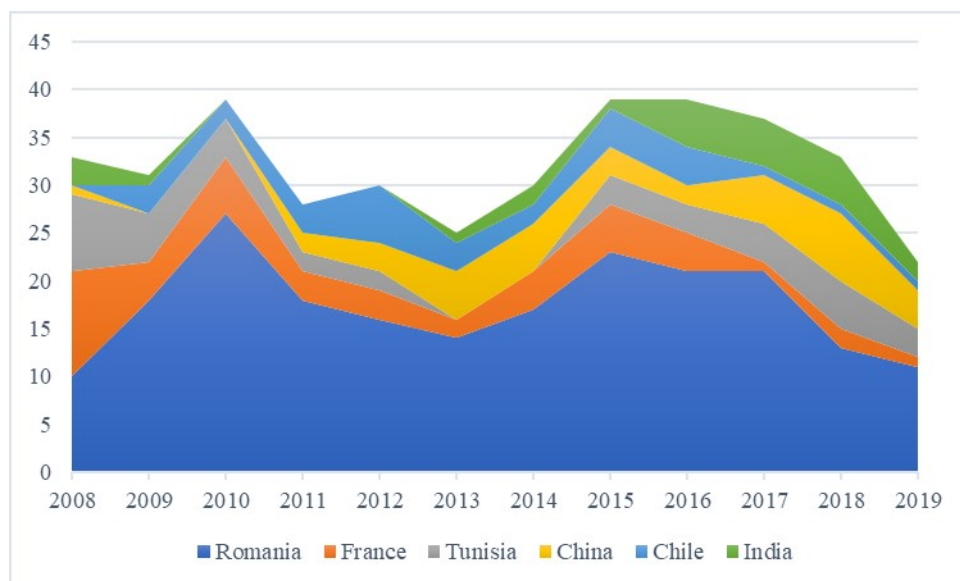
the 6 articles were written by 3 or 4 authors.

3.3 The productive and influential countries/regions and institutions

In this subsection, the countries/regions and institutions that mostly contribute to the journal from the perspective of productivity and influence respectively are analyzed. The indicators such as P, C, AC and H-index are exhibited.

The most productive and the most influential countries/regions

To analyze the productivity of countries/regions, the top 6 most productive countries/regions with publications not less than 20 and their annual publications are shown in Figure 2.



* As of November 1, 2019.

Figure 2: The annual publications of top 10 productive countries/regions from 2008 to 2019*.

The top 6 productive countries/regions are Romania (209), France (46), Tunisia (39), China (37), Chile (30) and India (25) in a strict order. The number of the total publications of the 6 countries/regions reached the highest value (39) in 2010, 2015 and 2016. Romania published more than 20 documents in the journal in 2010, 2015, 2016, and 2017 and it is the most productive country among the 6 countries/regions per year except for in 2008. In this year, France published 11 documents in the journal while the publication of Romania is 10. As the second productive country, the publication of France is more than 10 documents only in 2008, and it published just 1 to 6 documents in the journal per year from 2009 to 2019. Chile had its first 3 publications in the journal way back in 2009, and has continued to publish at least one document in the journal until 2019. Some countries/regions published no documents in the journal only occasionally. The third productive country Tunisia published no documents in *SIC* in 2013 and 2014, and published at least 2 documents in the journal in other years. China published only 1 article in the journal in the first 3 years, while it published frequently in *SIC* in the last 10 years. India published nothing in the journal during the period from 2010 to 2012.

To analyze the influence of countries/regions, the indicators are used to describe the citation structures of top 7 most cited publications which are cited not less than 100 times, as listed in Table 5.

Table 5: The top 7 influential countries/regions in *SIC* from 2008 to 2019*.

Rank	Country/Regions	P	C	AC	≥ 50	≥ 30	≥ 20	≥ 10	≥ 5	≥ 1	H-index
1	Romania	209	682	3.26	0	1	3	15	45	163	10
2	France	46	209	4.54	0	1	2	6	14	38	8
3	Lithuania	14	198	14.14	1	2	3	6	10	11	8
4	Serbia	17	183	10.76	1	2	4	7	7	14	7
5	Chile	30	133	4.43	0	0	2	3	8	26	5
6	Tunisia	39	112	2.87	0	0	0	3	9	27	7
7	China	37	107	2.89	0	0	0	3	8	25	5

* As of November 1, 2019.

The most productive country Romania is also the most influential one with 682 citations and the highest value of H-index 10. Lithuania and Serbia are the only two countries with the value of AC over 10, which means their publications in the journal are cited more than 10 on average. They are also the only 2 countries with 1 of their publications in the journal cited not less than 50 times, and the 2 countries published less than 20 documents in the journal while obtained more than 180 citations. Although Lithuania published just 14 documents in *SIC*, it is the third influential country with the highest value of AC 14.14. As 1 of the top 6 productive country, India was not included for its publications in the journal are cited just 39 times in total. It is reasonable to infer that the number of citations have no any direct connection with the number of publications. In other words, a high number of publications does not always involve a high citation score.

The most productive and the most influential institutions

Table 6 lists the top 10 productive institutions whose number of publications exceeds 15. The relative indicators are also listed in order to illustrate their productivity and influence.

Table 6: The top 10 productive institutions from 2008 to 2019*.

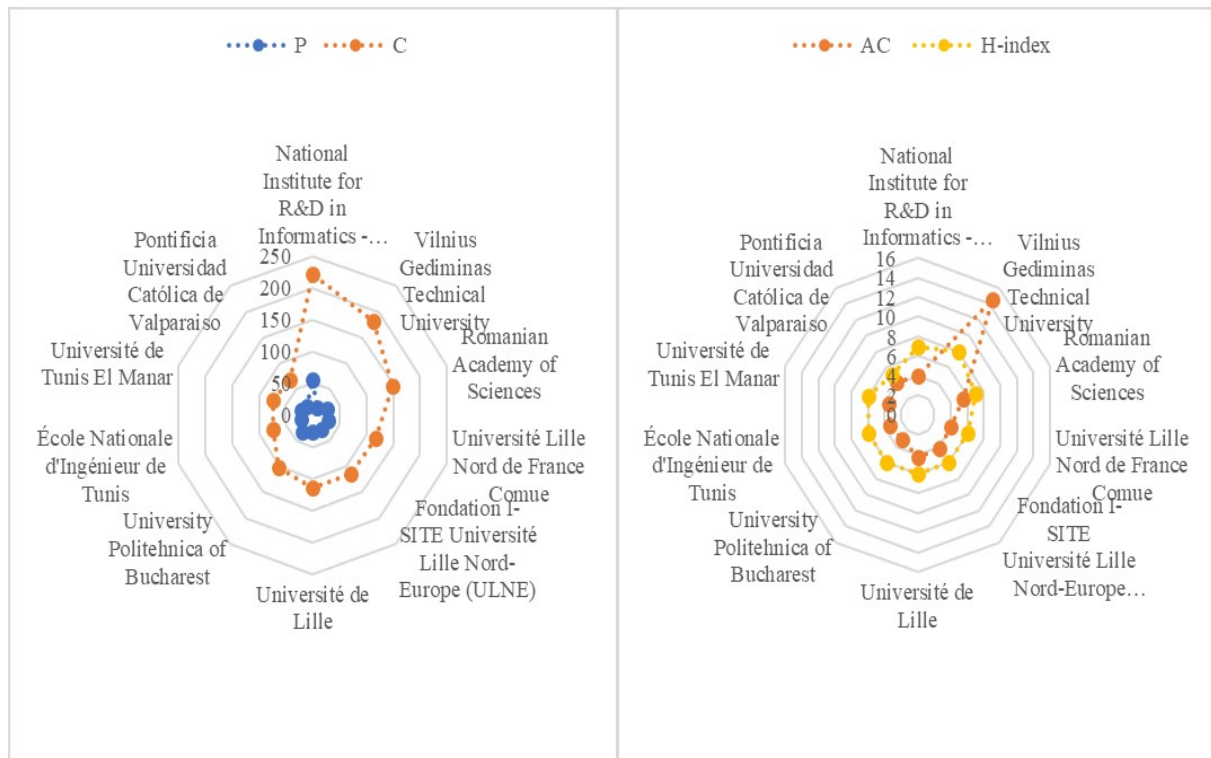
Rank	Institutions	Countries/Regions	P	C	C/P	H-index
1	National Institute for R&D in Informatics - ICI	Romania	56	222	3.96	7
2	University Politehnica of Bucharest	Romania	33	102	3.09	6
3	Université Lille Nord de France (ComUE)	France	29	117	4.03	6
4	Romanian Academy of Sciences	Romania	27	148	5.48	7
5	Fondation I-SITE Université Lille Nord-Europe (ULNE)	France	27	115	4.26	6
6	Université de Lille	France	27	115	4.26	6
7	École Nationale d'Ingénieur de Tunis	Tunisia	22	74	3.36	6
8	Université de Tunis El Manar	Tunisia	21	71	3.52	6
9	École Centrale Lille	France	19	62	3.26	5
10	Pontificia Universidad Católica de Valparaiso	Chile	17	69	4.06	5

* As of November 1, 2019.

From Table 6, it can be figured out that the National Institute for R&D in Informatics - ICI Bucharest is the leading productive institution, with a number of publications almost twice higher than that of the second productive institution - University Politehnica of Bucharest. 4 of 10 institutions are in France, 3 of 10 institutions are in Romania, and other 2 are in Tunisia. Pontificia Universidad Católica de Valparaiso is the only institution from Chile. The publications of the top 6 institutions are more than 25, while the publications of other 4 are around 20.

In fact, there is no significant difference in the list of top 10 productive and cited institutions. Vilnius Gediminas Technical University (Lithuania) takes the place of École Centrale Lille

(France) and is the top 2 cited institutions with 13 P, 183 C, 14.54 AC and the value of H-index 8. The relative indicators: P, C, AC and H-index, are used to illustrate the influence of the top 10 influential institutions in Figure 3.



* As of November 1, 2019.

Figure 3: The radar map of top 10 productive institutions in terms of P, C, AC and H-index from 2008 to 2019*.

The number of publications of the National Institute for R&D in Informatics - ICI Bucharest (Romania) is distinctly higher than these of other institutions, while there are no obvious differences among other institutions. The number of citations is higher than the number of their publications, and the citations of the National Institute for R&D in Informatics - ICI Bucharest (Romania) and Vilnius Gediminas Technical University (Lithuania) are one or half more than those of other institutions. There are no evident differences among the H-indices of these 10 institutions. The AC of Vilnius Gediminas Technical University (Lithuania) is 14.54, while the AC of other institutions are less than 6.

4 Science mapping analysis of *SIC*

In order to intuitively display the structure of publications in *SIC*, science network maps have been developed by using the VoS viewer and CiteSpace regarding three different aspects: co-citation analysis, co-authorship analysis, and co-occurrence analysis. Parts of burst information are detected by CiteSpace and listed in Tables. The co-citation analysis of authors, references and journals, the co-authorship of authors, institutions, and countries/regions, co-occurrence of keywords and the corresponding burst detection of the 527 documents published in *SIC* are presented, respectively.

4.1 Co-citation analysis

Co-citation was defined as the frequency with which two documents are cited together in the very beginning [22]. It was expanded into the co-citation analysis of journals and authors [26]. In the network of co-citation analysis, different nodes represent different references/journals/authors, and they are clustered by similarity and presented by a color. The size of the node represents the total number of citations with which the reference/journal/author is cited. The link between two nodes means that they are co-cited, and the size of the link represents the strength of their co-citation relationship. In the following, three types of co-citation analysis: references co-citation analysis, journals co-citation analysis, and authors co-citation analysis, are made, and all the network maps are established using VoS viewer.

Depending on the visualization tool VoS viewer, 8,335 cited authors are derived. In order to show them clearly, the minimum number of an author's citations is set at 10, and 52 authors meet the threshold. The cluster resolution is set at 0.5. The largest set of connected items consists of 49 authors, as shown in Figure 4.

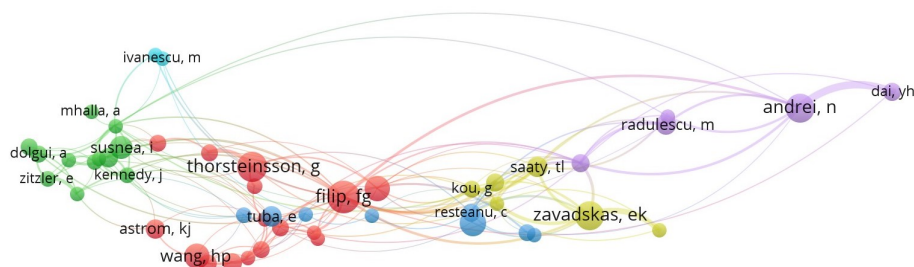


Figure 4: Authors co-citation network.

As Figure 4 illustrates, all of the 49 authors are classified into six clusters, which are represented by six different colors. The bigger the node is, the more the author is cited by documents published in *SIC* from 2008 to November 1, 2019. The most-cited author is Filip, F.G with 51 citations of his publications. The link shows the co-citation relationship between two authors. The width of the link is positively related to the strength of the relationship. The link between Andrei, N and Dai, Y. H is the widest, and the link strength is 93. This means that Andrei, N and Dai, Y. H are co-cited 93 times. Furthermore, the top 10 cited authors with the strongest citation bursts are listed in Table 7.

The cited author with the strongest citation bursts is Banciu, D from Romania. The strength of bursts is 3.9566 and the period of citation bursts is 2010-2014. The citation of Liouane, N from Tunisia burst in 2008 and 2009, and the citation bursts of other 9 authors occurred later than 2009. From 2010 to 2014, the citations of authors successively burst, and the citations of 3 authors burst in 2010. Only the citation of Zadeh, L. A from USA and Wang, H. P from China burst in last 3 and 4 years respectively, which means that the works of Zadeh, L. A and Wang, H. P have been taken into consideration and cited by many scholars in the last 3 or 5 years.

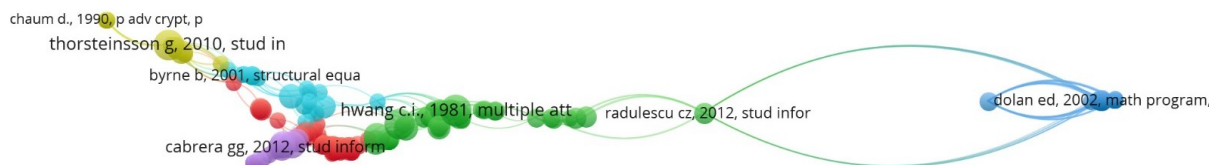


Figure 5: The references co-citation networks.

Table 7: The top 10 cited authors with the strongest citation bursts from 2008 to 2019*.

Rank	Cited Authors	Strength	Begin	End	2008-2019
1	Banciu, D	3.9566	2010	2014	
2	Suduc, A. M	3.4812	2011	2013	
3	Zadeh, L. A	3.4076	2017	2019	
4	Gabrera, G. G	3.1207	2014	2015	
5	Susnea, I	3.0751	2011	2014	
6	Thorsteinsson, G	3.0739	2010	2013	
7	Liouane, N	2.8432	2008	2009	
8	Peng, Y	2.7815	2012	2013	
9	Page, T	2.6353	2010	2012	
10	Wang, H. P	2.5943	2016	2019	

* As of November 1, 2019.

To visualize the references co-citation networks, the minimum number of citations of a reference is set at 3, and 209 of 10,810 references have met the threshold. Figure 5 illustrates the largest set of connected items which consists of 204 references. With the cluster resolutions set as 0.5, there are six clusters differentiated by six colors. Two linked items are cited together at least once. Table 8 lists the top 1 reference with the strongest citation bursts from 2008 to 2019. The reference was published by Cabrera, G.G in 2012, and the citation of the reference bursts in 2014 and 2015. This means that the citations of this article in these 2 years are more numerous than those of the other years. Cabrera G.G et al. [4] proposed a hybrid algorithm which combines the Particle Swarm Optimization (PSO) algorithm and the Simulated Annealing (SA) algorithms to solve the Probabilistic Traveling Salesman Problem (PTSP).

Table 8: The top 1 reference with the strongest citation bursts from 2008 to 2019*.

Rank	Reference	Year	Strength	Begin	End	2008-2019
1	Cabrera, G.G, 2012, STUD INFORM CONTROL, V21, P49	2012	2.7439	2014	2015	

* As of November 1, 2019.

By setting the minimum number of citations of a journal at 20 and the resolution at 1.0, the journals co-citation network can be visualized in Figure 6. 46 of 6,286 journals are selected and *SIC* is the most cited journal (651 citations) followed by European Journal of Operational Research with 115 citations. Figure 6(a) shows the co-citation relationship between the 46 journals. The thicker the link is, the more the linked 2 journals are cited together. To make it clearer, the minimum strength of the link is set at 150 and the result can be seen in Figure 6(b). The existing links from Figure 6(b) show that the linked journals are co-cited not less than 150 times. Only 6 links meet the threshold, and the linked journals by the 6 links are illustrated in Table 9.

For further studying of the cited journals, the CiteSpace has been applied in order to detect the citation bursts of them. The top 10 cited journals with the strongest citation bursts and the related information are listed in Table 10.

International Journal of Computers, Communications & Control (IJCCC) is the journal with the strongest citation bursts 11.578, which is at least twice than those of others. Compared

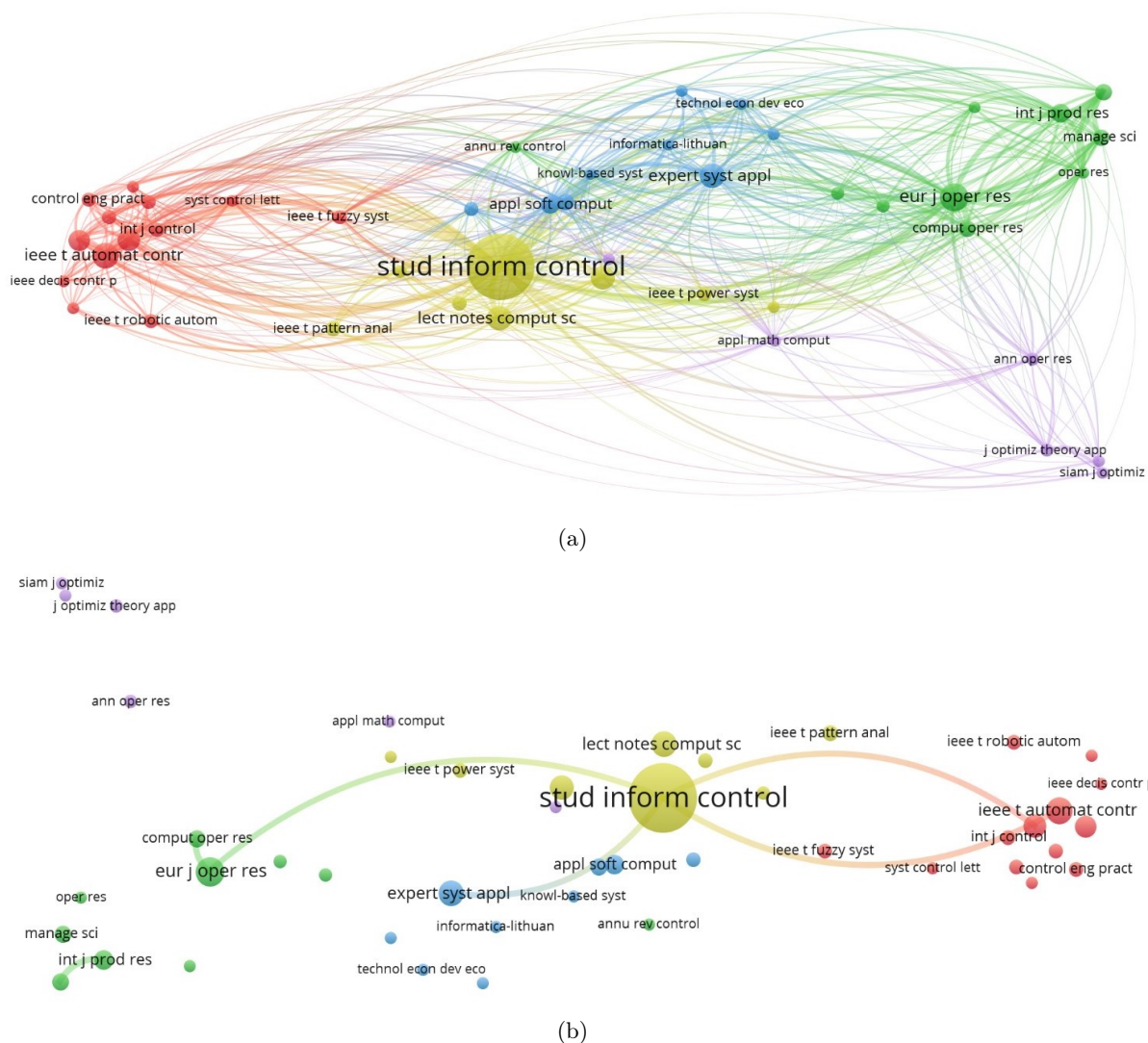


Figure 6: The journals co-citation network.

to other 2 journals whose bursts lasted for four years from 2009 to 2012, *IJCCC* is cited more than them. The citation bursts of most journals began in 2009, 2011 or 2013 and lasted for 2-4 years. The journals *ISA Transactions* is more cited than before, because its citation bursts occurred in the last 4 years.

4.2 Co-authorship network

Co-authorship reflects the collaborative relationship between authors/institutions/countries/regions that have published documents in the journal. In the following, the cooperation relationship is analyzed from the perspective of authors (microcosmic scale), institutions (middle scale) and countries/regions (macroscopic scale). The VoS viewer is applied in order to create the network maps and the CiteSpace in order to detect the citation bursts information.

It can be found that 1,147 authors published at least 1 document in *SIC*. In Figure 7, the largest set of connected items consists of 76 authors and their co-authorship networks are shown. With the clustering resolution set at 0.5, 11 clusters are derived and represented by 11 colors. The size of the node reflects the number of publications of the author, and the strength of the

Table 9: The 6 couples of journals with strongest co-citation strength from 2008 to 2019*.

Rank	Link strength	Journal 1	Journal 2
1	172	<i>International Journal of Production Research</i>	<i>International Journal of Production Economics</i>
2	165	<i>Computers & Operations Research</i>	<i>European Journal of Operational Research</i>
3	160	<i>Studies in Informatics and Control</i>	<i>IEEE Transactions on Automatic Control</i>
4	155	<i>Studies in Informatics and Control</i>	<i>Expert System with Applications</i>
5	153	<i>Studies in Informatics and Control</i>	<i>Automatica</i>
6	150	<i>Studies in Informatics and Control</i>	<i>European Journal of Operational Research</i>

* As of November 1, 2019.

Table 10: The top 10 cited journals with the strongest citation bursts from 2008 to 2019*.

Rank	Cited Journals	Strength	Begin	End	2008-2019
1	<i>International Journal of Computers Communications & Control</i>	11.578	2009	2012	
2	<i>European Journal of Operational Research</i>	4.6737	2011	2015	
3	<i>Operations Research</i>	4.4687	2013	2016	
4	<i>Computers in Industry</i>	4.2578	2011	2014	
5	<i>Mathematical Programming</i>	3.9211	2008	2009	
6	<i>Communications of the ACM</i>	3.9011	2009	2012	
7	<i>IEEE Transactions on Neural Networks</i>	3.8133	2009	2012	
8	<i>Journal of the Operational Research Society</i>	3.7977	2013	2015	
9	<i>Journal of Intelligent Manufacturing</i>	3.7971	2011	2013	
10	<i>ISA Transactions</i>	3.7841	2016	2019	

* As of November 1, 2019.

link represents the frequency of cooperation. The linked authors are cooperators and they finish at least 1 document with each other. In each cluster, almost every author has cooperated with the most productive author. By setting the minimum strength of link at 4, the Figure 7(b) is derived. The strongest cooperation relationship is between Wang, H. P and Tian, Y, they have written 10 documents in cooperation. Wang, H. P and Christov, N have published 4 documents together, and they represent the second strongest cooperative relationship.

To analyze the co-authorship of the institutions, the VoS viewer has been employed to map the co-authorship networks. The minimum number of documents of an institution is set at 5, and 32 of 457 institutions meet the threshold. Among all the 32 institutions, 17 are part of the largest connected network as shown in Figure 8 (with the clustering resolution set at 0.5).

17 institutions are grouped into 4 clusters which are marked in red, yellow, green and blue, and Figure 8 shows the cooperation relationship between them. The National Institute for R&D in Informatics, ICI Bucharest and the University Politehnica of Bucharest are the two most productive institutions of them. The top 6 groups with the strongest cooperation are listed in Table 11. The National Institute for R&D in Informatics maintains a strong cooperation with many other institutions.

The co-authorship network of countries/regions is shown in Figure 9. It is the largest linked network consisting of 54 countries/regions (there are 60 countries/regions in total) obtained by applying the VoS viewer.

International cooperation relationships among 54 countries/regions are exhibited in Figure 9. Romania, France, China and Tunisia are the four most productive countries. Table 12 lists

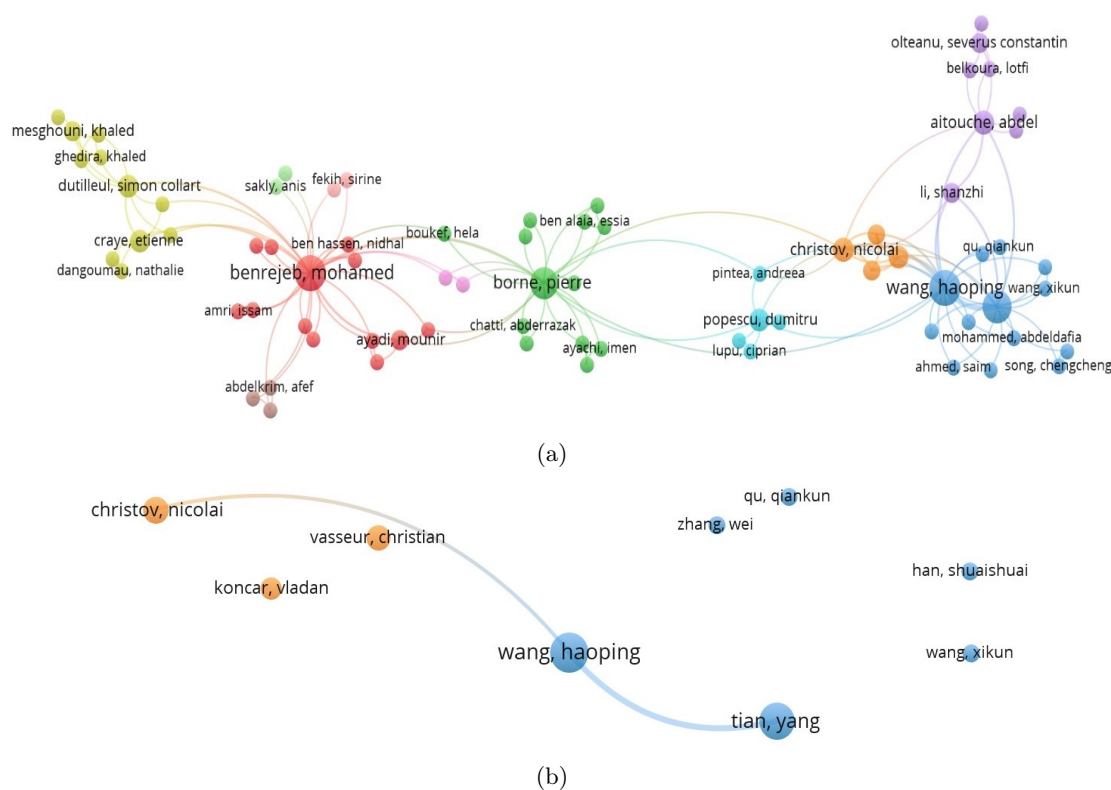


Figure 7: Co-authorship networks of authors.



Figure 8: Co-authorship network of institutions.

the main international cooperation information of the top 6 most productive countries/regions.

The links represent the number of cooperators, and total link strength represents the number of international cooperative publications. Cooperation strength is the percentage of total link strength from the number of documents. The main cooperators of the 6 countries/regions and their link strength are listed, and the link strength represents the number of cooperative documents. Romania is the most productive (209 documents) country in the past 12 years and owns the most collaborative countries/regions. However, the total link strength of Romania (31) is not the highest, and the cooperation strength (14.83%) is the lowest. France has published 46 documents in *SIC* since 2008, and 76.09% of these research works were written with authors from other 10 countries/regions. As the country with the highest cooperation strength (76.09%), France establishes a strong international collaborative relationship. The collaborative strength between France and Tunisia is the strongest, and they have cooperated for 17 times. In the last 12 years, the authors from Tunisia have written documents with authors from France, Lithuania and Saudi Arabia. Indian authors prefer to cooperate with the authors who come from Romania, England, France and Oman.

Table 11: The top 6 groups with the strongest cooperation from 2008 to 2019*.

Rank	Link strength	Institutions 1	Institutions 2
1	7	Spiru Haret University	University of Iceland
2	6	École Centrale Lille	Ecole Nationale d'Ingénieur de Tunis
3	5	Bucharest University of Economic Studies	National Institute for R&D in Informatics - ICI
4	5	CASA ACAD Romane	National Institute for R&D in Informatics - ICI
5	4	University Politehnica of Bucharest	National Institute for R&D in Informatics - ICI
6	4	Loughborough University	University of Iceland

* As of November 1, 2019.

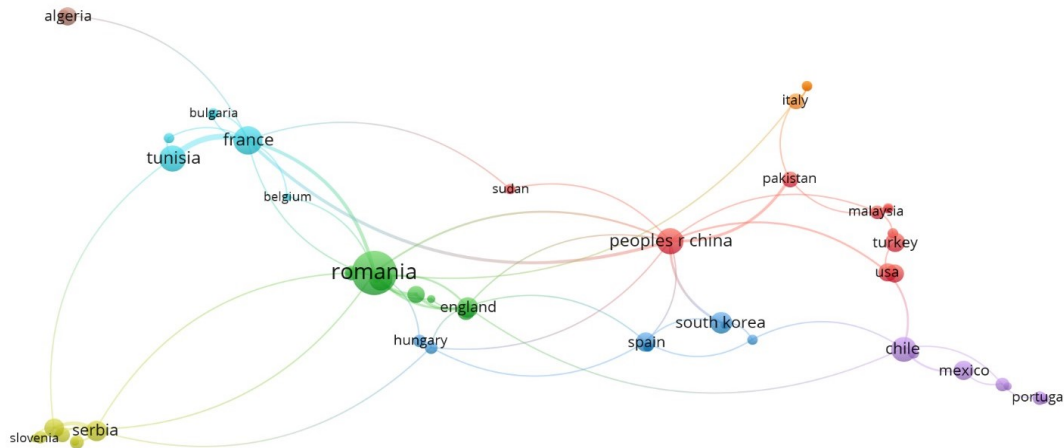


Figure 9: Co-authorship networks of countries/regions.

Next, CiteSpace is used to detect the citation bursts of authors, institutions, and countries/regions. Table 13 lists the top 1 author, the top 4 institutions and the top 5 countries/regions with the strongest citation burst from 2008 to 2019.

Tian, Y is the only one author with citation bursts over the past 12 years, and the citation bursts began in 2014 and lasted until 2019. The documents published by Tian Y in *SIC* have been cited more often in the last 6 years than in the first 6 years starting 2008. The documents of École Centrale de Lille has been cited more often in the preceding 4 years, while the documents of Vilnius Gediminas Technical University have gained a lot of attentions recently. University Politehnica of Bucharest has the highest strength of citation bursts (6.2612) from 2014 to 2017. The citation bursts of Tunisia and England occurred in 2008, and lasted for 2 or 3 years respectively. From 2011 to 2014, Spain had the highest strength of citation bursts (4.8054). The citation bursts of documents from Turkey have continued to 2019 from 2017.

4.3 Co-occurrence analysis

As a quantitative analysis method, co-occurrence analysis is useful to support the knowledge services and knowledge mining. The keywords show the research fields and the underlying trends of the publications. Thus, the keyword co-occurrence analysis is a good way to reveal the hot topics and research trends of the journal. The following research is based on 2,988 keywords detected by employing the CiteSpace.

Figure 10 shows the largest connected co-occurrence network and classification map of the keywords. The two linked keywords appear together in not less than 1 document. The top 7 most frequently used keywords are labeled. The bigger the node is, the higher the occurrence is. The network is divided into 6 clusters and the smaller the cluster ID is, the more components

Table 12: The international cooperation of the top 6 most productive countries/regions from 2008 to 2019*.

Rank	Countries/Regions	Documents	Links	Total link strength	Cooperation strength	Main cooperators	
						Countries/Regions	Link strength
1	Romania	209	14	31	14.83%	Iceland	7
						France	6
						India	3
						England	3
2	France	46	10	35	76.09%	Tunisia	17
						Romania	6
						China	5
3	Tunisia	39	3	19	48.72%	France	17
						Lithuania	1
						Saudi Arabia	1
4	China	37	10	21	56.76%	France	5
						Pakistan	4
						South Korea	3
5	Chile	30	6	9	30.00%	USA	2
						Peru	2
						Mexico	2
6	India	25	4	7	28.00%	Romania	3
						England	2
						France	1
						Oman	1

* As of November 1, 2019.

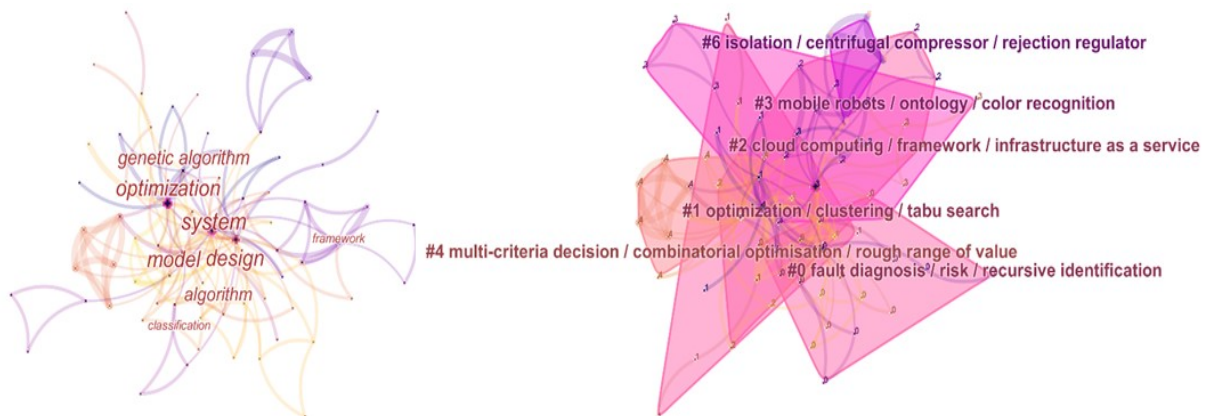


Figure 10: The keyword co-occurrence network and classification map.

the cluster has. The cluster is labeled with indexing terms and three algorithms: latent semantic index (LSI), log-likelihood ratio (LLR) and mutual information (MI) in sequence.

To analyze the hotspots and the underlying trends of the journal, the CiteSpace is applied in order to detect the top 5 keywords with the strongest citation bursts and to map the timeline view of keywords.

The main attention is paid to the keywords 'system', 'model', and 'design' which have frequently appeared in the journal during 2010-2011, 2012-2015, and 2012-2013 respectively, and 'model' is the keyword with the strongest citation bursts. In the last 4 years, the keyword 'algorithm' has gained much attention, and the research concerning this keyword has been prevalent. The keyword 'mobile robot' was paid much attention during 2012-2014. From Figure 11, it can be observed that most keywords of the publications are a combination of these three words. *SIC* not only focuses on the research of algorithms, models and system designs, but also pays attention to the application of these technologies and combination with other theories. Especially, they are combined with decision-making techniques, Internet, supply chain and energy.

Table 13: The top 1 author, 4 institutions and 5 countries/regions with the strongest citation bursts from 2008 to 2019*.

Rank	Authors	Strength	Begin	End	2008-2019
1	Tian, Y	4.0459	2014	2019	
Rank	Institutions	Strength	Begin	End	2008-2019
1	University Politehnica of Bucharest	6.2612	2014	2017	
2	École Centrale de Lille	4.4988	2008	2011	
3	Petroleum-Gas University	3.0844	2014	2016	
4	Vilnius Gediminas Technical University	3.0109	2015	2019	
Rank	Countries	Strength	Begin	End	2008-2019
1	Spain	4.8054	2011	2014	
2	England	4.0777	2008	2010	
3	Turkey	3.5189	2017	2019	
4	Tunisia	3.4792	2008	2009	
5	USA	2.9427	2009	2012	

* As of November 1, 2019.

Table 14: The top 5 keywords with the strongest citation bursts from 2008 to 2019*.

Rank	Keywords	Strength	Begin	End	2008-2019
1	Model	4.5285	2012	2015	
2	Design	3.3160	2012	2013	
3	System	3.0302	2010	2011	
4	Algorithm	2.9440	2016	2019	
5	Mobile Robot	2.6314	2012	2014	

* As of November 1, 2019.

5 Conclusions

The bibliometric analysis of the journal *SIC* is illustrated in this paper. The productivity and influence of authors, countries/regions, and institutions that have published documents in *SIC*, and the citations of the most cited documents is analyzed. The productivity and influence are reflected in terms of publications and citations, but also the H-index and other statistic information are used. A comprehensive performance analysis of the documents published in *SIC* between 2008-2019 is presented and illustrated. For an intuitionistic exhibition of the publications in *SIC*, science maps of the documents published in *SIC* from 2008 to 2019 have been developed, by using the visualization tools VoS viewer and CiteSpace. Co-citation analysis, co-authorship network and co-occurrence analysis are represented in visualization. Based on the above analysis, some conclusions are summarized as follows.

(1) *SIC* has had a more important influence in the area of IT in the last 10 years, and has gained more consideration and attention. Authors and institutions from Romania contribute most publications to the journal and gain most citations, while the average influence of their publications is not the highest. There is no doubt that Romania is one of the most productive and influential country in *SIC*, followed by France, Tunisia, China, Chile and India, respectively.

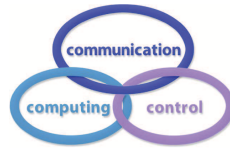
(2) The source of the references is extensive, as there are 8,335 cited authors and 6,286

-
- [4] Cabrera, G.; Roncagliolo, S.; Riquelme, J.P.; Cubillos, C.; Soto, R. (2012). A hybrid particle swarm optimization-simulated annealing algorithm for the probabilistic travelling salesman problem, *Studies in Informatics and Control*, DOI: 10.24846/v21i1y201206, 21(1), 49-58, 2012.
- [5] Cancino, C.A.; Merigó, J.M.; Coronado, F.C. (2017). A bibliometric analysis of leading universities in innovation research, *Journal of Innovation & Knowledge*, 2(2), 106–124, 2017.
- [6] Chen, C. (2006). CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature, *Journal of the American Society for information Science and Technology*, 57(3), 359–377, 2006.
- [7] Cobo, M.J.; López-Herrera, A.G.; Herrera-Viedma, E.; Herrera, F. (2011). Science mapping software tools: Review, analysis, and cooperative study among tools *Journal of the American Society for Information Science and Technology*, 62(7), 1382–1402, 2011.
- [8] Cobo, M.J.; Martínez, M.A.; Gutiérrez-Salcedo, M.; Fujita, H.; Herrera-Viedma, E. (2015). 25 years at Knowledge-Based Systems: A bibliometric analysis, *Knowledge-Based Systems*, 80, 3–13, 2015.
- [9] Costas, R.; Bordons, M. (2007). The h-index: Advantages, limitations and its relation with other bibliometric indicators at the micro level, *Journal of informetrics*, 1(3), 193-203, 2007.
- [10] Coupé, T. (2003). Revealed performances: Worldwide rankings of economists and economics departments, 1990-2000, *Journal of the European Economic Association*, 1(6), 1309-1345, 2003.
- [11] Diodato, V.P.; Gellatly, P. (2013). Dictionary of bibliometrics, Routledge, 2013.
- [12] Dumitrache, I. (2018). The contribution of the Romanian automation to the development of civilization, In *Filip F. G (ed.), Information Science and Technology in Romania* (in Romanian), Editura Academiei Romane, Bucharest, 294-351, 2018. 294–351, 2018.
- [13] Fagerberg, J.; Fosaas, M.; Sapprasert, K. (2012). Innovation: Exploring the knowledge base, *Research Policy*, 41(7), 1132–1153, 2012.
- [14] Filip, F.G.; Suduc, A.M.; Bizoi, M. (2014). DSS in numbers, *Technological and Economic Development of Economy*, 20(1), 154–164, 2014.
- [15] Laengle, S.; Merigó, J.M.; Miranda, J.; Słowiński, R.; Bomze, I.; Borgonovo, E.; Dyson, R.G.; Oliveira, J.F.; Teunter, R. (2017). Forty years of the European Journal of Operational Research: A bibliometric overview, *European Journal of Operational Research*, 262(3), 803–816, 2017.
- [16] Landström, H.; Harirchi, G.; Aström, F. (2012). Entrepreneurship: Exploring the knowledge base, *Research Policy*, 41(7), 1154–1181, 2012.
- [17] Luor, T.; Lu, H.P.; Yu, H.; Chang, K. (2014). Trends in and contributions to entrepreneurship research: A broad review of literature from 1996 to June 2012, *Scientometrics*, 99(2), 353–369, 2014.
- [18] Merigó, J.M.; Blanco-Mesa, F.; Gil-Lafuente, A.M.; Yager, R.R. (2017). Thirty years of the International Journal of Intelligent Systems: A bibliometric review, *International Journal of Intelligent Systems*, 32(5), 526–554, 2017.

-
- [19] Mongeon, P.; Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: a comparative analysis, *Scientometrics*, 106(1), 213–228, 2016.
- [20] Noyons, E.C.; Moed, H.F.; Luwel, M. (1999). Combining mapping and citation analysis for evaluative bibliometric purposes: A bibliometric study, *Journal of the American society for Information Science*, 50(2), 115–131, 1999.
- [21] Podsakoff, P.M.; MacKenzie, S.B.; Podsakoff, N.P.; Bachrach, D.G. (2008). Scholarly influence in the field of management: A bibliometric analysis of the determinants of university and author impact in the management literature in the past quarter century, *Journal of Management*, 34(4), 641–720, 2008.
- [22] Small, H. (1973). Co-citation in the scientific literature: A new measure of the relationship between two documents, *Journal of the American Society for information Science*, 24(4), 265–269, 1973.
- [23] Tuba, M.; Tuba, E. (2019). Generative Adversarial Optimization (GOA) for acute lymphocytic leukemia detection, *Studies in Informatics and Control*, 28(3), 245–254, 2019.
- [24] Van Eck, N.; Waltman, L. (2009). Software survey: VOSviewer, a computer program for bibliometric mapping, *Scientometrics*, 84(2), 523–538, 2009.
- [25] Wang, X.X.; Xu, Z.S.; Dzitac, I. (2019). Bibliometric Analysis on Research Trends of International Journal of Computers Communications & Control, *International Journal of Computers Communications & Control*, 14(5), 711–732, 2019.
- [26] White, H.D.; Griffith, B.C. (1981). Author cocitation: A literature measure of intellectual structure, *Journal of the American Society for information Science*, 32(3), 163–171, 1981.
- [27] Yu, D.J.; Xu Z.S.; Saparauskas J. (2019). The evolution of Technological and Economic Development of Economy: A bibliometric analysis, *Technological and Economic Development of Economy*, 25(3), 369–385, 2019.
- [28] Yu, D.J.; Xu, Z.S.; Kao, Y.S.; Lin, C.T. (2018). The structure and citation landscape of IEEE Transactions on Fuzzy Systems (1994-2015), *IEEE Transactions on Fuzzy Systems*, 26(2), 430–442, 2018.
- [29] Yu, D.J.; Xu, Z.S.; Pedrycz, W.; Wang, W.R. (2017). Information sciences 1968-2016: A retrospective analysis with text mining and bibliometric, *Information Sciences*, 418, 619–634, 2017.
- [30] Zavadskas, E.K.; Stević, R.; Turskis, Z.; Tomašević, M. (2019). A novel extended EDAS in Minkowski Space (EDAS-M) method for evaluating autonomous vehicles, *Studies in Informatics and Control*, 28(3), 255–264, 2019.
- [31] Zhou, W.; Xu Z.S.; Zavadskas, E.K. (2019). A bibliometric overview of International Journal of Strategic Property Management between 2008 and 2019, *International Journal of Strategic Property Management*, 23(6), 366–377, 2019.

Modeling of Characteristics on Artificial Intelligence IQ Test: a Fuzzy Cognitive Map-Based Dynamic Scenario Analysis

F. Liu, Y. Peng, Z.X. Chen, Y. Shi



Fangyao Liu*

Department of Information Systems and Quantitative Analysis
University of Nebraska at Omaha, Omaha, NE, 68182, USA

*Corresponding author: fangyaoliu@unomaha.edu

Yayu Peng

Department of Electrical and Computer Engineering
University of Nebraska-Lincoln, Lincoln, NE, 68588, USA
yayu.peng@huskers.unl.edu

Zhengxin Chen

Department of Computer Science
University of Nebraska at Omaha, Omaha, NE, 68182, USA
zchen@unomaha.edu

Yong Shi

1. Department of Information Systems and Quantitative Analysis
University of Nebraska at Omaha, Omaha, NE, 68182, USA
2. Key Lab of Big Data Mining and Knowledge Management, China Academy of Sciences, Beijing,
100190, China
yshi@unomaha.edu

Abstract: This research article uses a Fuzzy Cognitive Map (FCM) approach to improve an earlier proposed IQ test characteristics of Artificial Intelligence (AI) systems. The defuzzification process makes use of fuzzy logic and the triangular membership function along with linguistic term analyses. Each edge of the proposed FCM is assigned to a positive or negative influence type associated with a quantitative weight. All the weights are based on the defuzzified value in the defuzzification results. This research also leverages a dynamic scenario analysis to investigate the interrelationships between driver concepts and other concepts. Worst and best-case scenarios have been conducted on the correlation among concepts. We also use an inference simulation to examine the concepts importance order and the FCM convergence status. The analysis results not only examine the FCM complexity, but also draws insightful conclusions.

Keywords: fuzzy cognitive Map (FCM), inference simulation, artificial intelligent system, dynamic scenario analysis, IQ Test, linguistic analysis.

1 Introduction

In the academic field, artificial intelligence (AI) is a popular topic. And, many scholar papers and projects focused on this topic [7,33,36]. Also, in industry field, AI-based products are trying to make our lives more convenient and efficient [7]. However, there is a warm debate about

whether the emerging AI systems have the potential of helping or doing something devastating to human. To evaluate the smartness of AI systems, Liu et al. paper presents a method to measure the AI system through an IQ test [23]. Based on its measurement framework, a list of 100 AI-based search engines received an IQ score. For example, based on the IQ test result, Google search engine got the highest IQ score of 47.28 [23]. Which means Google's IQ score is almost the same as a six-year-old child's IQ score. These IQ results illustrate that AI-based system still has a long way to go to replace human, at least in industry world.

For the purpose of successfully conducting the IQ test for all the top 100 search engines, such as Google, Bing, Baidu, etc. In 2015, Liu et al. [23] proposed a measurement framework. This framework includes a test bank, which has hundreds of questions. Like a human IQ test, each search engine need to answer several questions that are selected from the developed test bank by random. For each question, they will receive a score between 0 and 100. This framework divides all the questions into four main indicator groups and further into 15 characteristics. Also, a few adult volunteers had the IQ test for the purpose of standardizing the IQ score, and mapping with the human being's IQ score.

Table 1 lists all the 15 IQ characteristics along with their corresponding weights for testing AI systems. After gathering expert opinions (Delphi method), all the 15 weights are calculated and presented in the Table 1.

- C1m (m=1,2...m) = ability to acquire knowledge.
- C2n (n=1,2...n) = ability to master knowledge.
- C3p (p=1,2...p) = ability to innovate knowledge.
- C4q (q=1,2...q) = ability of knowledge feedback.

Table 1: 15 IQ Characteristics for AI system and their corresponding Delphi weights

C1m	C2n	C3p	C4q
C11: Ability to identify word (3%)	C21: Ability to master general knowledge (6%)	C31: Ability to innovate by association (12%)	C41: Word feedback ability (3%)
C12: Ability to identify sound (3%)	C22: Ability to master translation (3%)	C32: Ability to innovate by creation (12%)	C42: Sound feedback ability (3%)
C13: Ability to identify image (4%)	C23: Ability to master calculation (6%)	C33: Ability to innovate by speculation (12%)	C43: Image feedback ability (4%)
	C24: Ability to master arrangement(5%)	C34: Ability to innovate by selection (12%)	
		C35: Ability to innovate by discover laws (12%)	

The proposed IQ test question bank is arranged according to all the 15 IQ characteristics (concepts). To illustrate, an example of testing question: "Please translate 'Technology's impact' into Spanish" should belong to characteristic C22 (Ability to master translation).

The results of Delphi weights are very subjective. Because they are coming from expert's own judgment, which means the results may be biased. Take advantage of linguistic terms from literature sources can be treated as a better method because all the literature publication sources are considered as an objective approach. One of the article's goals is to assign new weights though the fuzzy logic method (an objective approach). Based on the new weights, the interrelations among characteristics also should be investigated. There are some significant relationships among some characteristics. For example, "C21: Ability to master general knowledge" literally has a positive impact on "C24: Ability to master arrangement".

The main method of this research article is a fuzzy logic mathematics method, more specifically, called "fuzzy cognitive mapping" or "fuzzy cognitive map" (FCM). The core idea behind

fuzzy logic is that it aims to model the more imprecise reasoning used by humans when they make rational decisions, especially in an uncertain and imprecise environment [14, 37]. By providing a mathematical means of representing vagueness, fuzzy logic models, or sets, are able to recognize, represent, manipulate interdependence between characteristics (concepts).

2 Research method

2.1 Methodology

Fuzzy Cognitive Mapping (FCM) is the most important method of this research article. For the purpose of constructing FCM, the number of edges should be clarified. Theoretically, all the combination of two concepts should have an edge (relationship). However, the literature resources only support the meaningful edges, for example, the edge between one IQ characteristic and the AI system, or the edges of the interrelations among the 15 IQ characteristics. According to the literature resources, it is easy to assign the influence type (negative, positive, or null) of the edge.

Keyword extraction plays a significant role in the relationship between concepts capturing. For instance, one reference paper said concept C22 heavily impacts concept C31, then, keyword "heavily impacts" will be extracted here. Each keyword will be assigned with one of the linguistic terms ("VERY LOW", "LOW", "MEDIUM", "HIGH", and "VERY HIGH"). At least three linguistic terms will be assigned to each edge.

The linguistic terms are fuzzy set problems. The membership function plays a significant role in quantifying the membership grade of the element in X to the fuzzy set [45].

$$\mu_A : X \rightarrow [0, 1]$$

Where X represents the universe of discourse while the fuzzy set is A , and μ_A is the membership function [8].

A triangular function will be used in the FCM constructing process. Where a is the lower limit, b is the upper limit, and m is a value between a and b . Figure 1 illustrates the membership function as a graph.

$$\mu_A = \begin{cases} 0, & x \leq a \\ \frac{x-a}{m-a}, & a < x \leq m \\ \frac{b-x}{b-m}, & m < x \leq b \\ 0, & x > b \end{cases}$$

2.2 Linguistic term analyses

The literature resources, support the linguistic term assigning as references. Table 2 summarizes all the possible relationships between each IQ characteristic and the AI system, and the interrelationship among the 15 IQ characteristics. In particular, Barwise's paper mentioned IQ characteristics' ability to identify word is a "most common view" of AI system [24]. Then, the keyword "most common view" will be extracted here, while a linguistic term "HIGH" will be assigned to this edge. Table 2 gives an outline of the linguistic terms, influence type, keywords, and their corresponding reference papers.

In Table 2, "C" represents the "AI system IQ".

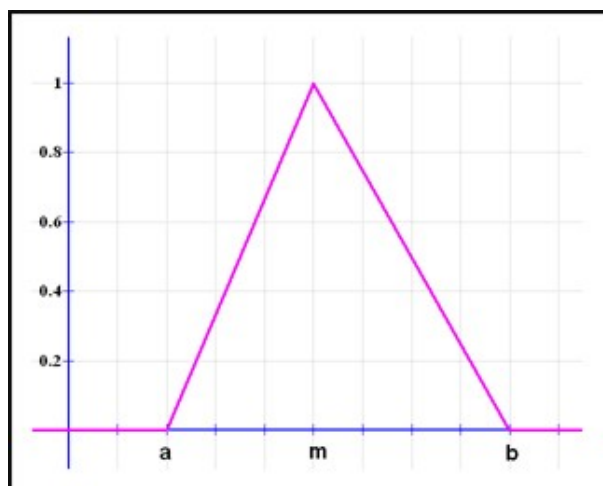


Figure 1: Membership function graph [19]

Table 2: Linguistic terms and their associated references

EDGE OF FCM	KEYWORD	LINGUISTIC TERM	REFERENCE
C11-C	an aspect of	LOW	Lynn et al (2001) [24]
	an aspect of	LOW	Lynn et al (2001) [24]
	an aspect of	LOW	Lynn et al (2001) [24]
C12-C	a key strategic	HIGH	Francisco (2015) [24]
	core capabilities	HIGH	Bernard (2018) [24]
	obvious	LOW	Adam (2016) [24]
C13-C	core capabilities	HIGH	Bernard (2018) [24]
	enable	MEDIUM	Flatworld (2017) [24]
C21-C	important component	HIGH	Bates et al (2003) [24]
	correlated	MEDIUM	Chamorro-Premuzic et al (2006) [24]
	partly represented	LOW	Cattell (1987) [24]
	related to	MEDIUM	Ackerman (2001) [24]
C22-C	no significant correlation	VERY LOW	Moghimi et al (2013) [24]
	weak relationship	LOW	Nasimi (2009) [24]
	no interrelationship	VERY LOW	Shangarffam (2009) [24]
C23-C	intersection	LOW	Greenberg (2000) [24]
	accelerate	MEDIUM	Greenberg (2000) [24]
	interleave	MEDIUM	Greenberg (2000) [24]
C24-C	a significant	MEDIUM	Wechsler, D. (1949) [24]
	common view	MEDIUM	APA (1995) [24]
C31-C	interpreted to	MEDIUM	Singh-Manoux et al (2005) [24]
	display	MEDIUM	Schutte et al (2011) [24]
	measures of	HIGH	Ferguson et al (2010) [24]
C32-C	demonstrates	HIGH	Kim et al (2010) [24]
	must entail	VERY HIGH	Gardner et al (1996) [24]
	referred to	HIGH	Sternberg (1985) [24]
C33-C	been central to	VERY HIGH	James (1950) [24]

	fundamental to	VERY HIGH	Leighton et al (2004) [24]
	can be important	HIGH	Bruner (1957) [24]
C34-C	directly	MEDIUM	Sternberg (1981) [24]
	commonly used	MEDIUM	Mayer et al (2007) [24]
	connects to	MEDIUM	Brackett et al (2006) [24]
C35-C	related to	MEDIUM	Teuber et al (1956) [24]
	may affect	LOW	Carroll (1993) [24]
C41-C	are as likely to	LOW	Argyris (1991) [24]
	important element	MEDIUM	Abisamra (2000) [24]
	a key for	HIGH	Jorfi et al (2014) [24]
C42-C	linked to	LOW	Luwel (2013) [24]
	taken into consideration	MEDIUM	Fernández-Martínez (2012) [24]
	is important to	HIGH	Bohland (2010) [24]
C43-C	dominated by	HIGH	Barry (1997) [24]
	driven by	MEDIUM	Messaris (1994) [24]
	result in	HIGH	Roth et al (2005) [24]
C11-C12	statistically significant	MEDIUM	Stanovich et al (1978) [39]
	foundational	VERY HIGH	Stanovich (1991) [40]
	strong connected	VERY HIGH	Nation et al (1998) [30]
C11-C13	improve	MEDIUM	Hull (1994) [17]
	dependent	MEDIUM	Zhu et al (2001) [44]
	benefit	MEDIUM	Wang et al (2001) [43]
C21-C22	important	MEDIUM	Collombat (2006) [9]
	widely identified as	LOW	Collombat (2006) [9]
	never an empty mind of	MEDIUM	Delisle (2003) [13]
C21-C23	result from	HIGH	Baroody (1999) [5]
	partially predicted by	LOW	Cowan (2011) [10]
	as the basis	MEDIUM	Askew (1998) [4]
C21-C24	commonly used	MEDIUM	Rugg et al (1997) [35]
	spontaneously	MEDIUM	Mandler et al (1988) [28]
	related to	MEDIUM	Gopnik et al (1984) [16]
C21-C31	able to	MEDIUM	Feigenson et al (2004) [15]
	a key precursor of	VERY HIGH	De Smedt et al (2009) [11]
	access to	HIGH	De Smedt et al (2011) [12]
C21-C32	according to	MEDIUM	Afuah et al (2003) [1]
	used to	MEDIUM	Afuah et al (2003) [1]
	embodied in	HIGH	Talaya et al (2008) [41]
C21-C33	found to be	HIGH	Scardamalia et al (1992) [38]
	directive effect	MEDIUM	Miyake et al (1979) [29]
	prompted by	HIGH	Bereiter (1989) [6]
C21-C34	facilitate	HIGH	Alexander et al (1995) [3]
	related to	MEDIUM	Qian et al (1995) [34]
	as a basic	MEDIUM	Linnenbrink-Garcia et al (2012) [22]
C21-C35	needed for	MEDIUM	Njoo et al (1993) [31]
	lies in	HIGH	Klahr et al (1988) [18]
	support	HIGH	Van (1988) [42]
C41-C42	statistically significant	MEDIUM	Stanovich (1978) [39]
	foundational	VERY HIGH	Stanovich (1991) [40]

	strong connected	VERY HIGH	Nation et al (1998) [30]
C41-C43	improve	MEDIUM	Hull (1994) [17]
	dependent	MEDIUM	Zhu et al (2001) [44]
	benefit	MEDIUM	Wang et al (2011) [43]
C31-C35	valuable for	MEDIUM	Agrawal et al (1996) [2]
	led to	HIGH	Piatetsky-Shapiro (1996) [32]
	indicate	HIGH	Koperski (1995) [20]
C31-C32	representative	HIGH	Luhn (1958) [25]
	based on	MEDIUM	Luhn (1958) [25]
	significance	MEDIUM	Luhn (1958) [25]

Based on the extracted keyword results, Table 3 is a more advanced tabulation is used to summary keyword information into a table according to their linguistic terms.

Table 3: Categorization of keywords based on linguistic terms

LINGUISTIC TERM	KEYWORD		
VERY LOW	no significant correlation	no interrelationship	
LOW	an aspect of obvious partly represented partially predicted by	weak relationship intersection widely identified as	are as likely to linked to may affect
MEDIUM	a field of enable taken into consideration according to needed for connects to directly commonly used directive effect related to as a basic improve	accelerate important never an empty mind of as the basis spontaneously able to used to correlated a significant common view interpreted to	important element display statistically significant dependent benefit valuable for based on significance interleave driven by
HIGH	prompted by most common view facilitate lies in support led to important result in	a key for dominated by result from referred to access to core capabilities embodied in representative	demonstrates can be important a key strategic component measures of indicate found to be
VERY HIGH	must entail been central to	strong connected a key precursor of	foundational

2.3 Defuzzification method

Table 2 and Table 3, present a tabulation of the defined five linguistic terms in the fuzzy set we will use later. The Triangular Membership Function [19] which is shown in Figure 2 means different linguistic terms have different output values.

For the purpose of converting a fuzzified output values into a traditional single crisp value, defuzzification process will be used here [27]. Among the existing defuzzification approaches (COG, COA, BOA, etc.), in this research article, we use the Center of Sums (COS) approach, which is one very useful approach for the defuzzification process [14,27]. This equation of COS is below:

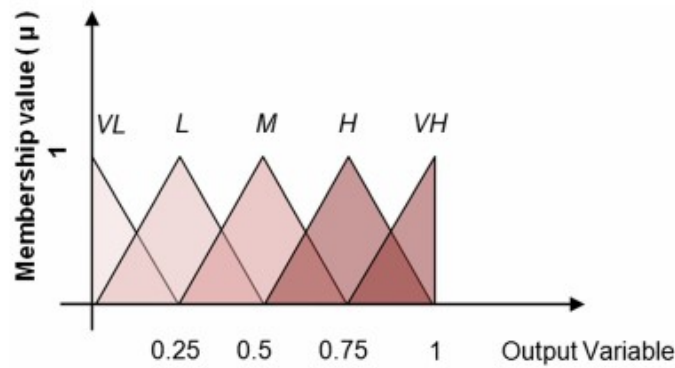


Figure 2: Triangular membership function [19]

$$x^* = \frac{\sum_{i=1}^N x_i * \sum_{k=1}^N \mu_{A_k}(x_i)}{\sum_{i=1}^N \sum_{k=1}^n \mu_{A_k}(x_i)}$$

Where n stands for the sum total of fuzzy sets, N is the sum total of fuzzy variables, and, $\mu_{A_k}(x_i)$ is the membership function for the k -th fuzzy set.

3 Data analysis

3.1 Fuzzy cognitive map results

As stated before, each edge, at least three linguistic terms are assigned to, even, for a few edges, four linguistic terms are assigned to.

A standard fuzzy set operation will be used, which is a standard union. Where,

$$\mu_{A \cup B}(u) = \max \{ \mu_A(u), \mu_B(u) \}$$

To illustrate, there are the three linguistic terms assigned to the edge of C22-C, they are: "LOW", "VERY LOW", and "VERY LOW".

$$A1 = \frac{1}{2} * [(0.25 - 0) + (0 - 0)] * 1 = 0.125$$

$$A2 = \frac{1}{2} * [(0.5 - 0) + (0.25 - 0.25)] * 1 = 0.25$$

$$A3 = \frac{1}{2} * [(0.25 - 0) + (0 - 0)] * 1 = 0.125$$

The center of area of the fuzzy set C1 is $\bar{x}_1 = (0.25 + 0)/2 = 0.125$, similarly, $\bar{x}_2 = 0.25$, $\bar{x}_3 = 0.125$. Now, the calculated defuzzified value $x^* = \frac{(A1\bar{x}_1 + A2\bar{x}_2 + A3\bar{x}_3)}{A1 + A2 + A3} = 0.1875$.

A final version of the calculated fuzzy cognitive map is presented in Figure. 3. This FCM is drawn with software "Mental Modeler".

The following FCM weights are calculated based on the defuzzified values of the FCM. A summary of the calculation results is presented in Table 4. And, Table 5 provides the corresponding adjacency matrix of the FCM. This matrix can be used to describe the interrelations between the concept.

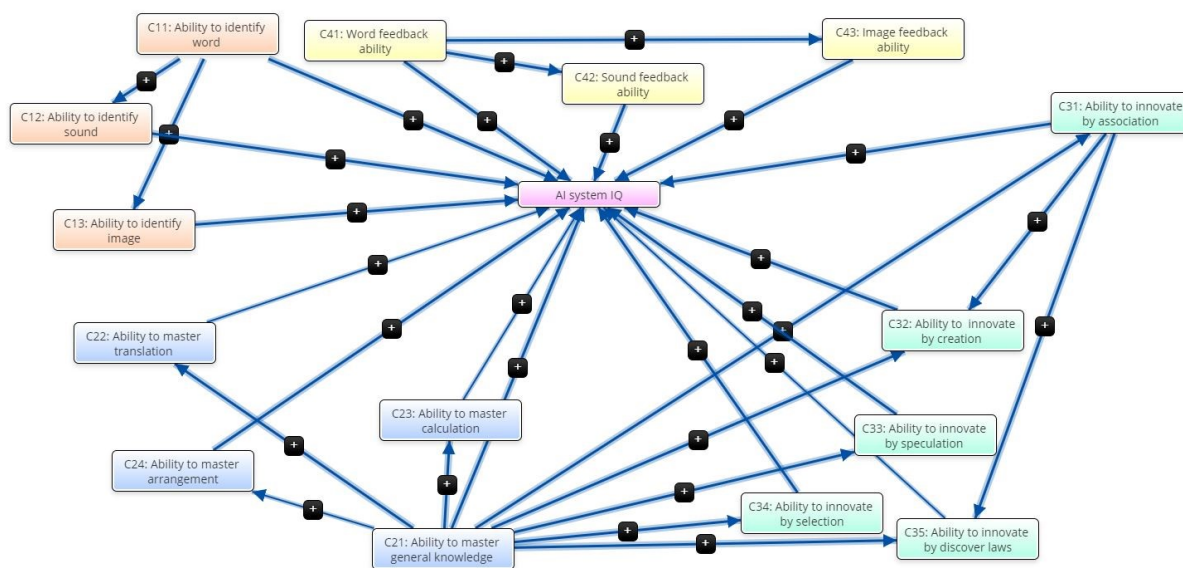


Figure 3: Fuzzy Cognitive Map with positive/negative sign to edges.

Table 4: Edge with its calculated weights

EDGE OF FCM	DEFUZZIFIED VALUE	FCM WEIGHT	DELPHI WEIGHT
C11-C	0.5	6.0373%	3%
C12-C	0.6786	8.1939%	3%
C13-C	0.5833	7.0432%	4%
C21-C	0.5625	6.792%	6%
C22-C	0.1875	2.264%	3%
C23-C	0.45	5.4336%	6%
C24-C	0.5	6.0373%	5%
C31-C	0.6071	7.3305%	12%
C32-C	0.7961	9.6126%	12%
C33-C	0.8125	9.8107%	12%
C34-C	0.5	6.0373%	12%
C35-C	0.4167	5.0315%	12%
C41-C	0.5	6.0373%	3%
C42-C	0.5	6.0373%	3%
C43-C	0.6875	7.3305%	12%
C11-C12	0.6525	N/A	0%
C11-C13	0.5	N/A	0%
C21-C22	0.5625	N/A	0%
C21-C23	0.5	N/A	0%
C21-C24	0.4	N/A	0%
C21-C31	0.7015	N/A	0%
C21-C32	0.6071	N/A	0%
C21-C33	0.6875	N/A	0%
C21-C34	0.6071	N/A	0%
C21-C35	0.6875	N/A	0%

C41-C42	0.6525	N/A	0%
C41-C43	0.5	N/A	0%
C31-C35	0.6875	N/A	0%
C31-C32	0.6071	N/A	0%

Table 5: Adjacency matrix collected from the Fuzzy Cognitive Map

	C11	C12	C13	C21	C22	C23	C24	C31	C32	C33	C34	C35	C41	C42	C43	AI system IQ
C11	0	0.65	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0.5
C12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.68
C13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.58
C21	0	0	0	0	0.56	0.5	0.4	0.7	0.61	0.69	0.61	0.69	0	0	0	0.56
C22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.19
C23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.45
C24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5
C31	0	0	0	0	0	0	0	0	0.61	0	0	0.69	0	0	0	0.61
C32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.8
C33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.81
C34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5
C35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.42
C41	0	0	0	0	0	0	0	0	0	0	0	0	0	0.65	0.5	0.5
C42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5
C43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.69
AI system IQ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

3.2 FCM steady-state analysis

A general descriptive summary about this FCM is shown in Table 6. The connection and component number is not extremely high. All the components can be categorized into the four groups. All the connections are supported by literature references. There are some interdependencies between the components in the same group. Also, there are some interconnections between components of different groups.

Figure. 3, which is the merged FCM, shows the density changed to 0.121 while the average connections per component increased to 1.8125. Hierarchy Index is another complexity measurement of FCM. Hierarchy Index is answerable to all the concepts' out-degree in an FCM of N components [26]. Below is the equation of Hierarchy Index.

$$h = \frac{12}{(N-1)N(N+1)} \sum_1^N \left[\frac{od(vi) - (\sum od(vi))}{N} \right]^2$$

Where N is the total number of components. And, $od(vi)$ is the row sum of absolute values

Table 6: General FCM statistics

FCM PROPERTIES	VALUE
Total components	16
Total connections	29
Density	0.121
Connections per Component	1.8125
No. of driver components	3
No. of receiver components	1
No. of ordinary components	12
Complexity score	0.3333

of a variable in the FCM adjacency matrix.

If h is close to 1, the FCM is supposed to be completely dominant (hierarchical). If h is close to 0, the FCM is supposed to be completely adapted eco-strategies (democratic) [24]. This FCM's hierarchy index is 0.326, which means, the FCM is much more adaptable to component changes because of its high level of integration and dependence. Also, the in-degree and out-degree of these nodes makes the FCM more democratic, and its system's steady-state more resistant to the alterations of individual components.

The component with the highest centrality was the "AI SYSTEM IQ" with a high score of 8.29. Also, the top three central components directly affecting the "AI SYSTEM IQ" component was the following, in ascending order of their complexity: Ability to innovate by discover laws 1.799, Ability to innovate by association 2.609, and, Ability to master general knowledge 5.319. A higher value means greater importance of an individual concept or several concepts in the overall model.

Table 7: Characteristic, type of concepts, in degree, out degree, centrality and in the FCM

CHARACTERISTIC	INDEGREE	OUTDEGREE	CENTRALITY	TYPE
AI system IQ	8.29	0	8.29	receiver
C11	0	1.65	1.65	driver
C12	0.65	0.68	1.33	ordinary
C13	0.5	0.58	1.08	ordinary
C21	0	5.319	5.319	driver
C22	0.56	0.19	0.75	ordinary
C23	0.5	0.45	0.95	ordinary
C24	0.4	0.5	0.9	ordinary
C31	0.7	1.909	2.609	ordinary
C32	1.22	0.8	2.02	ordinary
C33	0.69	0.81	1.5	ordinary
C34	0.61	0.5	1.109	ordinary
C35	1.38	0.42	1.799	ordinary
C41	0	1.65	1.65	driver
C42	0.65	0.5	1.15	ordinary
C43	0.5	0.69	1.19	ordinary

3.3 Dynamic scenario analysis of the AI system IQ

Worst and best-case scenario

The above AI system IQ FCM (Figure 3) shows its complexity. This research also conducted dynamic case scenario analyses along with inference simulation.

To start the analysis, we initially apply the current FCM. Both the worst and best scenario will be examined. After that, some insightful results and conclusions can be made. Based on our knowledge, the worst scenario means all the driver concepts are equal to 0.1. And, the best scenario means all the driver concepts are equal to 1.

From figure 4, we observe that there is approximately 58% increase in the "AI system IQ" in the worst scenario while compared to the initial steady-state scenario as the benchmark. Respectively, the "Ability to innovate by discover laws" has an increase of 13%, the "Ability of innovate by creation" has an increase of 11%. All the other concepts have an increase between 4% and 8%. The results also show that all concepts have a positive causality. Furthermore, all of the slight increases for all the ordinary concepts are related to the small increase of driver concepts.

Alternatively, all the driver concepts can be set as primarily affecting the FCM's ordinary concepts if all the values are set up with 1. From figure 5, we found that the "AI system IQ" in the best scenario while compared to the initial steady-state scenario as the benchmark, has a 100% increase. Similarly, the "Ability of innovate by creation" has an increase of 80%, and the "Ability to innovate by discover laws" has an increase of 75%. All the other concepts have an increase between 38% and 60%. This result also supports the conclusion of positive causality. Based on the results, the "Ability of innovate by creation" and "Ability to innovate by discover laws" has the most significant relevance impact.

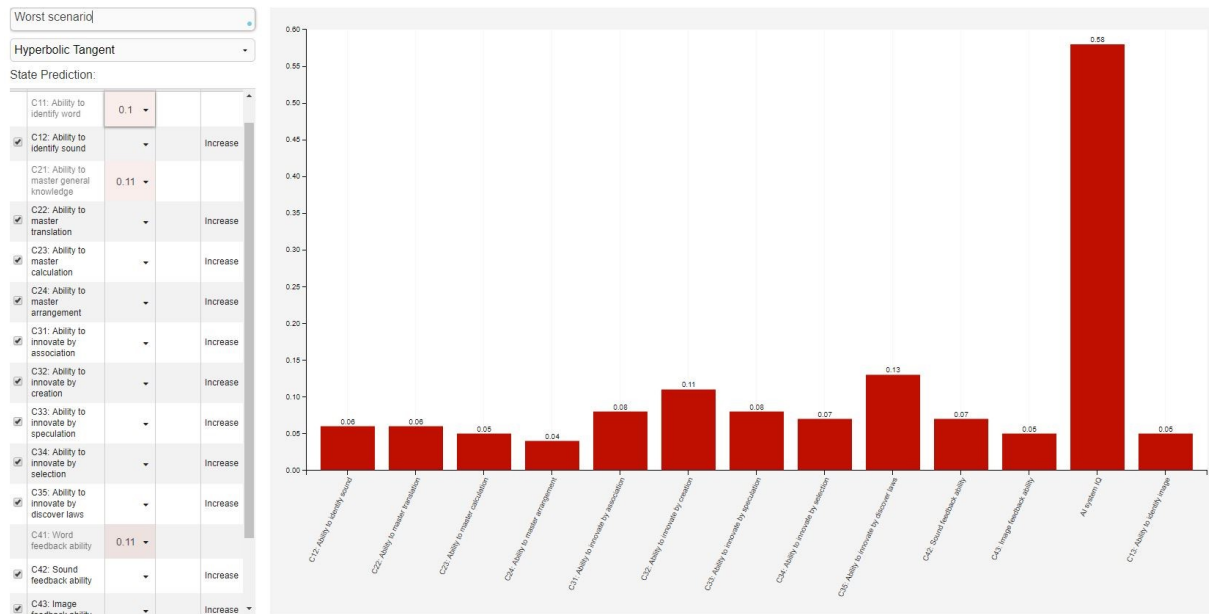


Figure 4: The driver concept effects for the worst scenario

FCM inference simulation

Based on the corresponding adjacency matrix (Table 5), there are some interrelations between concepts of this FCM. The value A_i of C_i is computed at each simulation step and it

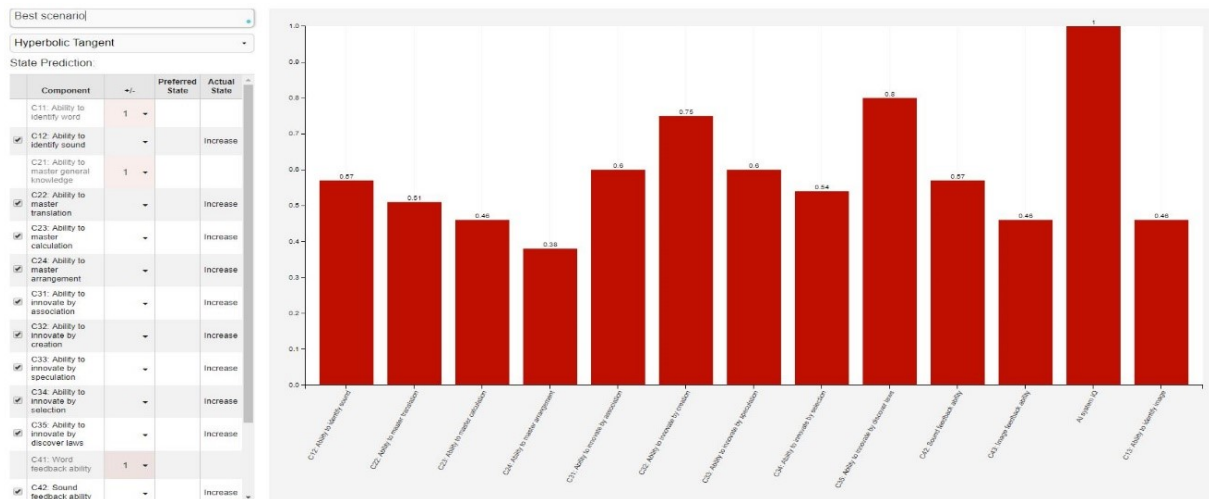


Figure 5: The driver concept effects for the best scenario

basically infers the influence of all other concepts C_j to C_i . This research selected Standard Kosko's activation rule inference method, below is the activation function:

$$A_t(K + 1) = f \left\{ \sum_{j=1, j \neq i}^N W_{ji} * A_j(k) \right\}$$

Also, the threshold function uses the sigmoid function, which shown as:

$$f(x) = \frac{1}{1 + e^{-\lambda x}}$$

Where x is the value $A_i(K)$ at the equilibrium point, and λ is a real positive number ($\lambda > 0$) that determines the steepness of the continuous function f . Using sigmoid threshold ensure that the activation value belongs to the interval $[0, 1]$.

When running the simulation, all the concepts were assigned an initial value of 0. After a few simulation steps, all the values were expected to be convergence status. Theoretically, after reaching the equilibrium end states, larger activation value means playing a more important role in this FCM. All the driver and ordinary concepts were used for the simulation task. Figure 6 shows the corresponding concept activation levels per each iteration with all 18 concepts ranging from 0 to 1. Table 8 gives us the inference concept values. All the inference simulations were run through "FCM Expert" software in this research.

Based on the plotter and the table results illustrated by the inference simulation process, it is easy to confirm that the top two critical roles are "C32: Ability to innovate by creation" and "C35: Ability to innovate by discover laws".

4 Summary and conclusion

In 2015, Liu *et al.* tested the selected 100 AI system based search engines IQ based on the Delphi weight approach [4]. This research article compares the new weight calculated through FCM approach to its original subjective approach and two other approaches while using the same data set as the input. Mean Square Error (MSE) is used here as a performance indicator,



Figure 6: Simulation Activation level values per each iteration

Table 8: Inference concepts values

Step	C11	C12	C13	C21	C22	C23	C24	C31	C32	C33	C34	C35	C41	C42	C43	AI system IQ
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354	0.354
2	0.354	0.522	0.482	0.354	0.498	0.482	0.456	0.536	0.667	0.533	0.512	0.704	0.354	0.522	0.482	0.999
3-8	0.354	0.522	0.482	0.354	0.498	0.482	0.456	0.536	0.736	0.533	0.512	0.776	0.354	0.522	0.482	1
9	0.354	0.522	0.482	0.354	0.498	0.482	0.456	0.536	0.736	0.533	0.512	0.776	0.354	0.522	0.482	1
10	0.354	0.522	0.482	0.354	0.498	0.482	0.456	0.536	0.736	0.533	0.512	0.776	0.354	0.522	0.482	1

its equation can be found as below:

$$MSE = \frac{1}{N} \sum_i^N (y_i - \hat{y}_i)^2$$

Table 9 presents the MSE value for each approach. Dichotomous and polytomous [21] are two other old school methods. For the purpose of choosing the best approach, MSE works as a prediction error indicator here. It is to say, lowest MSE value means less prediction error. Based on MSE values, it is easy to say FCM approach is among the four approaches.

Table 9: MSE results for four methods

APPROACH	MSE
Delphi Weight	37.63363
Polytomous	49.51347
Dichotomous	31.23294
FCM approach	19.16389

This article presents a new method to assign weights for the edges of the FCM. The MSE criteria show the FCM approach has a better performance than the other three approaches.

According to the proposed FCM, it is easy to conclude that the AI system IQ score is not just determined by linear concept dependence combinations. Actually, it is a nonlinear one, because there are a few significant relationships between concepts.

The dynamic scenario analysis has shown that the driver concepts together have a significant positive impact on the AI system IQ and other related concepts. Due to the reference limitation, we didn't find sufficient negative relationships exist in this FCM.

Based on the inference simulation results, it is coherent to reveal that the higher importance of "C32: Ability to innovate by creation" and "C35: Ability to innovate by discover laws" and other concepts. The simulation after seven iterations illustrates that all the concepts adjusted to a convergence status, which means changing values of concepts, could affect but will be reaching an equilibrium end state.

There are also some limitations in the present study. Different literature resources may use different words, which are synonyms of the concepts. For example, some paper may use "verbal" to replace "sound". Another is the low quality of the original data. The original test result data set is highly distributed left. Which means the MSE performance indicator may have a bias. Also, there may be unidentified interrelationships between the concepts, which needs further literature investigation. Furthermore, This FCM used the methodology of fuzzy membership function and other techniques to capture the nature of the AI system IQ test, there is a lot of room for improvement in identifying the characteristics. For example, more sub-characteristics can be added into future FCM, even the most determined concepts affecting the AI system IQ score can be identified. Another thing that can be improved is the relationship between concepts, currently, most of the relationship edges are one-way directions, maybe some relationship can be a two-way direction. For example, AI system IQ may also have an impact to C23. After all the possible improvements, an advanced FCM dynamic scenario may be used to analyze and re-design the FCM to reduce some not significant edges.

Data availability

The data used in the research paper are available from the corresponding author upon request.

Conflict of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Funding statement

This research is supported in part by a grant from Chinese Academy of Sciences (#46-0806-0009). It is also supported by the Graduate Research and Creative Activity (GRACA) (#42-1209-9116) grant of the University of Nebraska at Omaha, and the grants of the National Science Foundation of China (No.7193000078, No.91546201).

Acknowledgment

We are using this opportunity to express our gratitude to Shihang Li and Joel McMaken from University of Nebraska at Omaha. We are thankful for their aspiring writing skill guidance, invaluable constructive advice during this research paper.

Bibliography

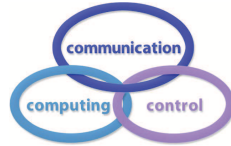
- [1] Afuah, A.; Afuah, A. (2003). *Innovation management: strategies, implementation and profits*, 2003.
- [2] Agrawal, R.; Mannila, H.; Srikant, R.; Toivonen, H.; Verkamo, A. I. (1996). Fast discovery of association rules. *Advances in knowledge discovery and data mining*, 12(1), 307-328, 1996.
- [3] Alexander, P. A.; Jetton, T. L.; Kulikowich, J. M. (1995). Interrelationship of knowledge, interest, and recall: Assessing a model of domain learning, *Journal of educational psychology*, 87(4), 559, 1995.
- [4] Askew, M. (1998). *Teaching Primary Mathematics: A guide for newly qualified & student teachers*. Hodder & Stoughton, 1998.
- [5] Baroody, A. J. (1999). Children's relational knowledge of addition and subtraction, *Cognition and Instruction*, 17(2), 137-175, 1999.
- [6] Bereiter, C.; Scardamalia, M. (1989). Intentional learning as a goal of instruction. Knowing, learning, and instruction: *Essays in honor of Robert Glaser*, 361-392, 1989.
- [7] Bostic, K. (2013). *Nuance confirms its voice technology is behind Apple's Siri*, AppleInsider, 2013.
- [8] Chen, G. S.; Jheng, Y.; Liu, H.; Chen, S. (2007). A novel scoring method for stroke order based on choquet integral with fuzzy measure, *Proceedings of the 7th Conference on 7th WSEAS international Conference on Applied Computer Science*, 7, 82-87, 2007.
- [9] Collombat, I. (2006). *General knowledge: A basic translation problem solving Tool*. Translation Studies in the new Millennium, Bilkent University, 2006.
- [10] Cowan, R.; Donlan, C.; Shepherd, D. L.; Cole-Fletcher, R., Saxton, M.; Hurry, J. (2011). Basic calculation proficiency and mathematics achievement in elementary school children. *Journal of Educational Psychology*, 103(4), 786, 2011.
- [11] De Smedt, B.; Reynvoet, B.; Swillen, A.; Verschaffel, L.; Boets, B.; Ghesquiere, P. (2009). Basic number processing and difficulties in single-digit arithmetic: Evidence from Velo-Cardio-Facial Syndrome, *Cortex*, 45(2), 177-188, 2009.
- [12] De Smedt, B.; Gilmore, C. K. (2011). Defective number module or impaired access? Numerical magnitude processing in first graders with mathematical difficulties, *Journal of experimental child psychology*, 108(2), 278-292, 2011.
- [13] Delisle, J. (2003). *Manuel d'initiation a la traduction professionnelle de l'anglais vers le francais* La traduction raisonnee, 2e edition, University of Ottawa Press, 2003.
- [14] Dzitac, I.; Filip, F. G.; Manolescu M.J. (2017). Fuzzy Logic Is Not Fuzzy: World-renowned Computer Scientist Lotfi A. Zadeh, *International Journal of Computers Communications & Control*, 12(6), 748-789, 2017.
- [15] Feigenson, L.; Dehaene, S.; Spelke, E. (2004). Core systems of number. *Trends in cognitive sciences*, 8(7), 307-314, 2004.
- [16] Gopnik, A.; Meltzoff, A. N. (1984). Semantic and cognitive development in 15-to 21-month-old children, *Journal of child language*, 11(3), 495-513, 1984.

-
- [17] Hull, J. J. (1994). A database for handwritten text recognition research, *IEEE Transactions on pattern analysis and machine intelligence*, 16(5), 550-554, 1994.
- [18] Klahr, D.; Dunbar, K. (1988). Dual space search during scientific reasoning. *Cognitive science*, 12(1), 1-48, 1988.
- [19] Klir, G.; Yuan, B. (1995). *Fuzzy sets and fuzzy logic*, 4, New Jersey, Prentice Hall, 1995.
- [20] Koperski, K.; Han, J. (1995). Discovery of spatial association rules in geographic information databases, *International Symposium on Spatial Databases*, Springer, Berlin, Heidelberg, 47-66, 1995.
- [21] Lewis-Beck, M.; Bryman, A. E.; Liao, T. F. (2003). *The Sage encyclopedia of social science research methods*, Sage Publications, 2003.
- [22] Linnenbrink-Garcia, L.; Pugh, K. J.; Koskey, K. L.; Stewart, V. C. (2012). Developing conceptual understanding of natural selection: The role of interest, efficacy, and basic prior knowledge. *The Journal of Experimental Education*, 80(1), 45-68, 2012.
- [23] Liu, F.; Shi, Y.; Wang, B. (2015). World search engine IQ test based on the internet IQ evaluation algorithms, *International Journal of Information Technology & Decision Making*, 14(02), 221-237, 2015.
- [24] Liu, F.; Zhang, Y.; Shi, Y.; Chen, Z.; Feng, X. (2018). Analyzing the Impact of Characteristics on Artificial Intelligence IQ Test: A Fuzzy Cognitive Map Approach, *Procedia computer science*, 139, 82-90, 2018.
- [25] Luhn, H. P. (1958). The automatic creation of literature abstracts. *IBM Journal of research and development*, 2(2), 159-165, 1958.
- [26] MacDonald, N. (1983). *Trees and networks in biological models*, 1983.
- [27] Mago, V. K.; Morden, H. K.; Fritz, C.; Wu, T.; Namazi, S.; Geranmayeh, P.; Dabbaghian, V. (2013). Analyzing the impact of social factors on homelessness: a Fuzzy Cognitive Map approach. *BMC medical informatics and decision making*, 13(1), 94, 2013.
- [28] Mandler, J. M.; Bauer, P. J. (1988). The cradle of categorization: Is the basic level basic?, *Cognitive development*, 3(3), 247-264, 1988.
- [29] Miyake, N.; Norman, D. A. (1979). To ask a question, one must know enough to know what is not known, *Journal of verbal learning and verbal behavior*, 18(3), 357-364, 1979.
- [30] Nation, K.; Snowling, M. J. (1998). Semantic processing and the development of word-recognition skills: Evidence from children with reading comprehension difficulties. *Journal of memory and language*, 39(1), 85-101, 1998.
- [31] Njoo, M.; De Jong, T. (1993). Exploratory learning with a computer simulation for control theory: Learning processes and instructional support. *Journal of research in science teaching*, 30(8), 821-844, 1993.
- [32] Piatetsky-Shapiro, G. (1996). *Advances in knowledge discovery and data mining (Vol. 21)*. U. M. Fayyad, P. Smyth, R. Uthurusamy (Eds.). Menlo Park: AAAI press, 1996.
- [33] Poole, D. L.; Mackworth, A. K.; Goebel, R. (1998). *Computational intelligence: a logical approach*, 1, New York: Oxford University Press, 1998.

- [34] Qian, G.; Alvermann, D. (1995). Role of epistemological beliefs and learned helplessness in secondary school students' learning science concepts from text. *Journal of educational psychology*, 87(2), 282, 1995.
- [35] Rugg, G.; McGeorge, P. (1997). The sorting techniques: a tutorial paper on card sorts, picture sorts and item sorts, *Expert Systems*, 14(2), 80-93, 1997.
- [36] Rusell, S.; Norvig, P. (2003). *Artificial intelligence: A modern approach*. Prentice Hall Series in Artificial Intelligence, 1, 2003.
- [37] Salmeron, J. L. (2012). Fuzzy Cognitive Maps for Artificial Emotions Forecasting , *Applied Soft Computing*. 12 (2), 3704-3710, 2012.
- [38] Scardamalia, M.; Bereiter, C. (1992). Text-based and knowledge based questioning by children, *Cognition and instruction*, 9(3), 177-199, 1992.
- [39] Stanovich, K. E.; Bauer, D. W. (1978). Experiments on the spelling-to-sound regularity effect in word recognition, *Memory & Cognition*, 6(4), 410-415, 1978.
- [40] Stanovich, K. E. (1991). Word recognition: Changing perspectives. *Handbook of reading research*, 2, 418-452, 1991.
- [41] Talaya, A. E. (2008). *Principios de marketing*. Esic Editorial, 2008.
- [42] Van Joolingen, W. (1998). *Cognitive tools for discovery learning*, 1998.
- [43] Wang, K.; Babenko, B.; Belongie, S. (2011). End-to-end scene text recognition. *2011 International Conference on Computer Vision*, IEEE, 1457-1464, 2011.
- [44] Zhu, Y.; Tan, T.; Wang, Y. (2001). Font recognition based on global texture analysis. *IEEE Transactions on pattern analysis and machine intelligence*, 23(10), 1192-1200, 2001.

An Empirical Study of AML Approach for Credit Card Fraud Detection–Financial Transactions

A. Singh, A. Jain



Ajeet Singh

University School of Information, Communication & Technology
Guru Gobind Singh Indraprastha University, Delhi, India
ajeet.usit.025164@ipu.ac.in

Anurag Jain*

University School of Information, Communication & Technology
Guru Gobind Singh Indraprastha University, Delhi, India
*Corresponding author: anurag@ipu.ac.in

Abstract: Credit card fraud is one of the flip sides of the digital world, where transactions are made without the knowledge of the genuine user. Based on the study of various papers published between 1994 and 2018 on credit card fraud, the following objectives are achieved: the various types of credit card frauds has identified and to detect automatically these frauds, an adaptive machine learning techniques (AMLTs) has studied and also their pros and cons has summarized. The various dataset are used in the literature has studied and categorized into the real and synthesized datasets. The performance matrices and evaluation criteria have summarized which has used to evaluate the fraud detection system. This study has also covered the deep analysis and comparison of the performance (i.e sensitivity, specificity, and accuracy) of existing machine learning techniques in the credit card fraud detection area. The findings of this study clearly show that supervised learning, card-not-present fraud, skimming fraud, and website cloning method has been used more frequently. This Study helps to new researchers by discussing the limitation of existing fraud detection techniques and providing helpful directions of research in the credit card fraud detection field.

Keywords: Credit card fraud, cashless transaction, data mining technique, fraud detection.

1 Introduction

Nowadays, the use of credit cards has significantly increased on both online and offline purchases because of the fast growth of the e-commerce and online banking system. When someone uses other persons credit card for personal benefit without the knowledge of the owner of the credit card is known as credit card fraud. The Association of Certified Fraud Examiners defines a fraud as *"the use of one's occupation for personal enrichment through the deliberate misuse or application of the employing organization's resources or assets"* [63]. Individuals and government suffer large financial losses across the world every year due to the lack of sophisticated fraud detection system.

In recent years, a million dollars losses due to the card frauds and many countries have affected. According to the fraud facts report-2017, the UK payment credit cards losses has been increased 9% in 2016 from Euro 567.5 million in 2015 to Euro 618.0 million. This point out

that payment card fraud is increasing yearly. The total spending on cards has reached Euro 904 billion in 2016, with 19.1 billion transactions happened during the 2015 [66].

In India, the State Bank of India (SBI) has blocked 0.6 million (6 lakh) debit cards due to a cyber attack (malware-related breach) to a YES Bank ATM network on October 19, 2016. It was one of the latest and largest security breaches where in Indian banking history, millions of the debit cards were compromised. The biggest financial data breaches reached almost 3.2 million (32lakhs) debit cards across 19 private banks (i.e. HDFC Bank, etc.).

According to the National Payments Corporation of India report, 90 ATMs suffered losses and 641 customers lost 13 million (1.3 Crores) Indian Rupee due to fraudulent transactions.

According to the Nilson Report, the card fraud losses reached \$21.84 billion in 2015, \$24.71 billion in 2016 and \$27.69 billion in 2017. This is also informed that the actual amount of losses could increase in 2020 [64].

According to the annual report of Internet crime complain 2018 (IC3), online crime has increased from 2008 to 2017 due to many types of frauds such as credit card fraud, identity fraud, etc.

The total loss has increased from 239.1 million in 2008 to \$1,418.7 million in 2017 due to frauds. Table1 presents the thousands of complaints between 2017 and 2008 received by the IC3 and happened financial loss in millions of USA dollar [65].

Table 1: Financial loss due to cyber crime

Year	Complaint	Money Loss	Year	Complaint	Money Loss
2017	301,580	\$1,418.7	2012	289,874	\$ 581.4
2016	298,728	\$1,450.7	2011	314,246	\$ 485.25
2015	288,012	\$1,070.7	2010	303809	\$121.71
2014	269,422	\$ 800.5	2009	336,655	\$559.7
2013	262,813	\$ 781.8	2008	275,284	\$265.0

It is clearly observed that financial loss has been increased due to card frauds while the number of complaints in some year has also decreased. These enormous numbers of losses define the importance of fraud prevention and detection system [51]. This study focuses on the banking domain in particular for credit card frauds. The common credit card frauds are application fraud, counterfeiting, identity theft fraud, phishing, and skimming fraud.

Frauds have to be explored and identified as quickly as possible in order to stop fraudulent activities [10, 34]. To address these frauds, various fraud prevention and detection mechanisms are deployed to detect and prevent credit card fraud. The purpose of credit card fraud prevention mechanism is to prevent and stop a fraudulent transaction before it happens in the initial phase, and also prevent the occurrence of different cyber attacks on your computer system, networks and your data by using numbers of prevention methods namely communal detection spike detection, PIN, Internet Security System, firewall and cryptography algorithms [1, 25].

Fraud detection is second stage mechanism to detect a fraud by applying various data mining, machine learning and bio-inspired techniques namely Decision Tree, Artificial Neural Network, Artificial Immune Systems (AIS), K Nearest Neighbor(KNN), Support Vector Machine(SVM), Genetic Algorithm (GA) and Hidden Markov Model (HMM) [12, 46, 55, 60]. These techniques are usually suitable for both types of transactions as normal and fraudulent in order to learn fraud patterns and customer patterns. The goal of the credit card fraud detection system is to maximize true positive and minimize false positive predictions of legitimate transactions.

The main contribution of this research is to identify the frequently occurred credit card frauds and methods committed to obtain credit card information illegally. A systematic review of the

existing machine learning techniques (MLTs) for credit card fraud detection are also discussed, and their advantages and limitations are reported in this paper. Based on the outcome of this paper, the research gap is identified among the existing fraud detection techniques. Various credit card fraud datasets are also compared on the basis of their features and used these datasets to implement various existing machine learning techniques.

The research process of this paper is explained in figure 1 based on adaptive existing machine learning techniques to credit card fraud detection.

The rest of the paper is designed as follows. Section 2 explores the different category of credit card frauds and methods. Section 3 discusses credit card fraud detection issues and challenges and Section 4 presents the various credit card fraud detection techniques. The various dataset, primary and derived attributes are summarized in Section 5. Section 6 presents performance matrices and evaluation criteria to evaluate the fraud detection system. Research conclusion and discussion are presented in Section 7.

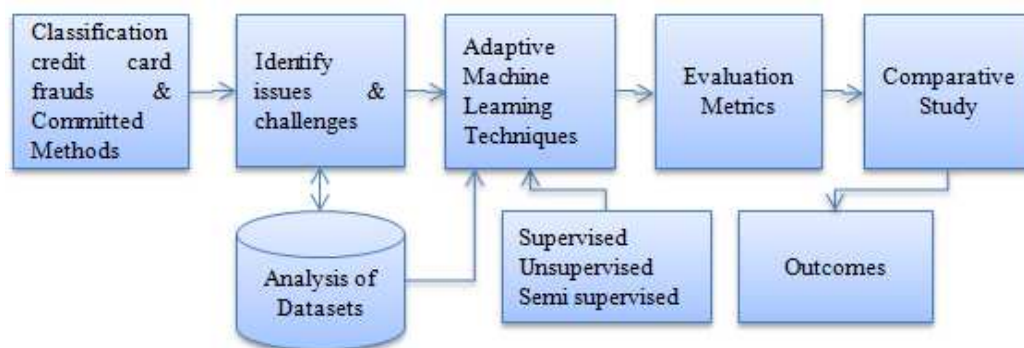


Figure 1: Flow diagram of the machine learning-based credit card fraud detection system

2 Classification of credit card frauds

Criminals use a variety of methods and tools for obtaining card information needed for online transactions and gets access to the cardholders account.

The various credit card frauds are observed based on literature. The common types of credit card frauds include application fraud, transaction fraud, bankruptcy fraud ([16]), and counterfeit fraud ([12, 50]) are summarized in table 2.

3 Credit card fraud detection issues and challenges

Researchers are facing several issues and challenges to detect fraud on time efficient manner. Credit card issuing banks required efficient and well-organized fraud detection system to run their business in a healthy way. The numbers of issues and challenges are summarized in table 3 based on literature.

4 Fraud detection techniques based on Machine Learning

The credit card fraud detection techniques (CCFDTs) are grouped into two general categories such as fraud analysis (misuse detection), and user behaviors analysis (anomaly detection). The CCFDTs are also further categorized as supervised learning which uses labeled training

Table 2: Various credit card frauds

Fraud Name	Definition	Method	Location of Occurs
Application [1, 12, 50]	If a fraudsters fill the application form with fake information, or maybe even real, but stolen identity information.	Steal identity namely bank statements, telephone bill, and electricity bill, etc.	Financial organization.
Transaction [1, 12, 47]	Used stolen card details: When someone obtains others card details to make a fraudulent transaction without legitimate cardholder knowledge	Keylogger, Sniffers, Site cloning, Physical stolen card.	Anywhere.
Account Takeover	When fraudsters pose as a genuine cardholder to gain access and control of an account then withdraw funds, makes illegal transactions, and may change account details.	Brute force botnet attacks, phishing, & malware.	Anywhere.
Counterfeit [12, 50]	It is the practice of illegally copying a legitimate credit card details	Fake websites, Site cloning, ATM skimming device.	ATM/ Place where CC uses.
Card-Not-Present [1, 12, 50]	When fraudsters obtain card information for personal use	Internet, Hacking, Email phishing campaigns.	Anyplace.
Skimming	Keeps the credit card into a skimming machine to make a copy and save the important card information.	Skimming Machine	Shopping mall, Restaurants, etc.
Shoulder Surfing	When fraudsters looking over the cardholders shoulder to steal credit card details while cardholder enter card details an electronic device and a Web.	Digital devices like camera	ATM, POS.

data, and unsupervised learning uses unlabeled training data, and a hybrid technique called semi-supervised learning.

4.1 Supervised learning method

Supervised learning is the machine learning technique. The supervised learning and classification technique are used for fraud analysis (misuses detection) at the transaction level and transactions categorized as a fraud or normal transaction based on the historical data. The supervised learning techniques are ruled induction, decision trees, case-based reasoning, support vector machines (SVMs), neural networks techniques, linear regression, logistic regression, naive Bayes, linear discriminate analysis, and k-nearest neighbor algorithm which used to credit fraud detection.

Table 3: Various issue and challenge for credit card fraud detection

Issues	Description
No standard credit card dataset [25, 60]	It is the biggest issues in fraud detection domain. There is no standard, real, and benchmark dataset available to evaluate proposed fraud detection methods. In most of the cases, researchers have been used their own dataset (Synthetic dataset) for doing research .
Skewed class distribution [1, 46, 50, 60]	The skewed distribution (or imbalanced class) is one of the most serious problems. Very small percentages of all card transitions are fraudulent as compare to normal transition. In a supervised learning technique, imbalance problem occurs when the minority class percentage is not very high.
Cost-sensitive classification problem [45, 50]	Credit card Transactions are misclassification (fraudulent transaction as a legitimate transaction and legitimate transaction as a fraudulent transaction) due to this financial impact ranging from a few to thousands of money.
Presently no suitable evaluation criterion [50, 60]	Standard evaluation criterion is not available for assessing and comparing the results of a fraud detection system. The accuracy is not suitable metrics CCFD because data set is imbalanced.
Lack of proper algorithm [50]	A powerful algorithm is required to detecting a new type of normal and fraudulent pattern. The Data mining and Machine Learning algorithm has its own advantages and disadvantages (table4).
Fraudsters behaviour dynamic [60]	Fraudsters are changed their behaviour from time to time for getting card details and bypass detection system or modify fraud styles.
Cardholder Behavior(Concept Drift) [1].	The cardholder is always changing their behaviour may be specific situation/ occasions (e.g New Year), the buying power of users will be enhanced. If the CCFD system does not consider this as normal changes, will be considered as fraud behaviour
Pattern Recognition Algorithm [1]	Pattern recognition algorithm is used to recognize fraudster pattern and customer pattern to minimize fraud cases.

4.2 Unsupervised learning method

The user behavior analysis can be performed by using unsupervised learning and clustering technique that identifies a transaction based on the account behavior of users. In unsupervised learning, all transactions are unlabeled and the algorithms learn to the inherent structure from the input transactions. Unsupervised learning is a more powerful technique to identify fraud and non-fraud transaction. The most common unsupervised techniques are k-means, Self-organizing Map (SOM) technique, and Hidden Markov Model (HMM) technique.

4.3 Semi-supervised learning method

The semi-supervised learning method falls between supervised and unsupervised learning method. Semi-supervised learning is a machine learning task that makes use a very small number of labeled data (previously known) and a large number of unlabeled data (unknown data) to detect a card fraud. Semi-supervised learning could decrease the effort needed by supervisors to classify training data. The supervised, unsupervised and semi supervised techniques are introduced following which was used to detect credit card fraud (CCF).

4.4 Artificial Neural Networks

ANNs constitute a set of interconnected nodes designed to imitate the functioning of the human brain (Maes et al. [31]). A neural network based fraud detection system has trained with the earlier data of cardholder spending behavior and the tested software on synthetically generated data (Guo and Li [21]). ANNs has been configured by supervised, unsupervised, and semi-supervised learning methods for classification or clustering of transaction group. Chen et al. [14] employs SVM and ANN techniques to investigate the time-varying fraud problem. The performance of the ANN is compared with SVM, outcomes show that ANN has the highest training accuracy. ANN two techniques namely Back Propagation Neural Network (BPNN) and Self-organizing Maps Neural Network (SOMNN) are mostly used for credit card fraud detection.

Back Propagation Neural Network

BPNN is a supervised learning technique, a generalization of the delta rule, and suitable for the feed-forward network, that has no feedback. The feed forward network contains three layers namely input, hidden, and output layers to credit card frauds detection. Chen et al. [14] deployed SVM and BPNN (ANN) techniques to investigate the time-varying fraud problem. The performance of the BPNN (78%) is compared with SVM (67%); outcomes show that ANN has the highest training accuracy. Another research (Ghosh et al. [20]) deployed a multilayer feed forward neural network model to fraud detection from Mellon Bank and reduction total fraud losses from 20% to 40%.

Self-organizing map

Self-organizing Map (SOM) [27] is a neural network model based on unsupervised learning method for the analysis and visualization of high-dimensional data. SOM neural network used to detect credit card fraud based on customer behaviour. SOM consist of two layer namely input mapping layer. The input layer forward the incoming transactions to the mapping layer for performing the clustering technique. The mapping layer is to map all transactions with cardholder's behavior for detecting hidden patterns. Finally, the mapping layer produces results in the form of fraudulent and genuine transaction.

According to Quah and Sriganes [42], the SOM used to decipher, filter and analyze customer behavior for the detection of credit card fraud in the banking sector.

Olszewski [39] has suggested a fraud detection method based on the user accounts visualization. The proposed SOM visualization method was applied in three different areas such as telecommunication, computer intrusion, and credit card fraud detection. This method is more suitable for the credit card as compared to the other areas. The CC dataset contains 10,000 accounts details from 1 January 2005 to 1 March 2005 and identified 100 instances as fraudulent.

The SOM visualization method was determined based on the produced values of the Precision (1.0000 vs 0.8257, 0.7200, 0.5696) Recall (1.0000 vs 0.9000, 0.9000, 0.9000) Accuracy (1.0000 vs 0.8550, 0.7750, 0.6100), F1 score (1.0000 vs 0.8612, 0.8000, 0.6977) and AUROC (1.0000 vs. 0.9415, 0.9285, and 0.8265) for a credit card. This is because of less unbalance dataset and small size of dataset. There may be chance of the accuracy and sensitivity will get dropped if dataset become large and more unbalance.

4.5 Bayesian network

Bayesian Network is a probabilistic graphical model denoting a set of random variables and their conditional dependencies through a directed acyclic graph introduced Cooper and Herskovits in 1992 (Panigrahi et al. [41]).

Bayesian Network used the concept of Bayes theorem to determine the probability of a given hypothesis to be true.

$$P(\text{Fraudulent}/\text{Evidence}) = \frac{(P(\text{Evidence}/\text{Fraudulent}) * P(\text{Fraudulent}))}{P(\text{Evidence})} \quad (1)$$

Where $P(\text{Fraudulent}/\text{Evidence})$ is the posterior probability condition on Hypothesis. Moreover, $P(\text{Fraudulent})$ and $P(\text{Evidence})$ is the prior probability of Hypothesis. $P(\text{Evidence}/\text{Fraudulent})$ is called the likely hood. The Fraud probability represented by $P(\text{Fraudulent}/\text{Evidence})$ gives the observed user behavior. Bayesian network (BN) has suggested for the purpose of credit card fraud detection based on user behavior. Bayesian belief networks and artificial neural networks (ANN) techniques have used credit card fraud detection by (Maes et al. [31]). Result presented that Bayesian network has superior fraud detection capability than ANN.

According to Kirkos et al. [26], the Bayesian Belief Network model achieved the best performance to correctly classify 90.3% of the validation sample in a 10-fold cross validation procedure. The accuracy rates of the Neural Network and Decision Tree model were 80% and 73.6%, respectively.

4.6 K-Nearest Neighbor

K-Nearest Neighbor (KNN) is a supervised learning technique [53]. The Euclidean distance method is used to calculate the distance between two transactions (input data transaction and current transaction) for every data transaction in the dataset and distances are arranged in increasing order. The k items have the lowest distance to the input data transaction point are selected. KNN technique classifies any new incoming transaction by calculating the nearest point if the nearest neighbor is a fraud than transaction considers as fraud and if the nearest neighbor is not fraud than transaction consider as legal.

The Euclidean distance (D_{ij}) between two input vectors (X_i, X_j) is given by \sum

$$D_{ij} = \sqrt{\sum_{k=1}^n (X_{ik} - Y_{jk})^2}, (k = 1, 2, 3, \dots, n.) \quad (2)$$

A simple matching coefficient is frequently used for categorical attributes. In this method, both legitimate and fraudulent transactions are to be fed in order to train the data sets. The K-Nearest Neighbor technique has optimized for better distance metrics. The various papers (Seeja and Zareapoor [46]), (Zareapoor et al. [60]) have performed a KNN technique to detect a credit card fraud and compare their result with other data mining techniques and This method is fast with minimum false alerts.

4.7 Artificial immune system

The artificial immune system (AIS) is part of artificial intelligence based on the biological symbol of the human immune system or natural immune system developed by Neal in 1998 [38]. It is a user-based model to discriminate the incoming transaction as genuine or fraudulent. According to Tuo et al. [54], artificial immune systems have four algorithms negative selection, clonal selection, immune network, and dendritic cells to identify fraudulent transaction detection. These algorithms have been applied to real data to detect fraud for achieving high accuracy.

Worng et al. [57] has developed a system called artificial immune system for fraud detection of credit card (AISCCFD). AISCCFD has a high level system model and consisted of the

database, two subsystems (system interface) and AIS engine. AISCCFD System has identified input transactions as non-fraudulent or fraudulent.

Halvaiee and Akbari [22] introduced a new credit card fraud detection model using AIS called "AIS-based Fraud Detection Model". The model has added some enhancements to the Artificial Immune Recognition System algorithm which helped to raise the precision, reduces cost, and system training time. AIS-based Fraud Detection Model enhanced fraud detection rate of 23%, reduced cost 85%, and training time 40%. This research has implemented a parallel model in a test environment for fair minimization in training time.

Gadi et al. [19] has employed the Artificial Immune Systems on credit card dataset for fraud detection and outcomes are compared with Neural Network, Bayesian Network, Naive Bayes, and Decision Trees based on three strategies such as default 35.66 (3.21%), optimized 24.97 (5.43%), and robust 23.30 (2.29%). The AIS produced the best classifiers and give high accuracy compared with other fraud detection methods respectively.

Huang et al. [23] have applied the AIS model for fraud detection. The AIS based model combines two AIS algorithms with behavior-based intrusion detection using Classification and Regression Trees (CART). This hybrid method applied on same data with combination CART algorithm (TP1%,TN85%, FP15%,FN19%), CSPRA algorithm (3% undetected: TP81%, TN 89% , FP11%, FN 16%), DCA algorithms (TP78%, TN90%, FP10%,FN22%) and Stacking Bagging algorithm (TP89%, TN95%, FP5%, FN 11%) to calculate each algorithm performance by using standard evaluation criteria. It was observed that the performance of AIS is better than other techniques.

4.8 Decision tree

The Decision tree (DT) is a supervised learning and statistical data mining technique. The research (Koikkinaki [28]) implemented decision trees by using various machines learning-based algorithms such as the Iterative Dichotomiser3 (ID3), Successor of ID3 (C4.5), Random forest, Classification and Regression Tree (CART). These techniques have been applied to a credit card database for fraud detection based on detection time and accuracy. DT technique divides the complex problems into smaller problems and resolves through repeatedly using the procedure (Bai et al. [5]).

According to Sachin and Duman, 2011 [44], decision rules have applied to determine the class of an incoming transaction as a genuine or fraudulent. Gadi et al. [19] used DT technique to computing result based on three strategies such as default 32.76 (4.83%), optimized 27.84 (4.16%), and robust 27.87 (4.21%).

Minegishi and Niim [35] has developed a decision tree learning based method called Very Fast Decision Tree learner (VFDT) to solve the imbalanced data stream problem.

Sahin et al. [45] has developed and implemented a cost-sensitive decision tree induction algorithm to identify fraudulent credit card transactions on a real world credit card data set. The performance of this approach was compared with the traditional classification models on a real data set and result showed that cost-sensitive decision tree algorithm outperforms the existing traditional classification methods.

4.9 Support Vector Machine

The SVM is a statistical and supervised machine learning (ML) technique used for both regression and classification tests [15]. SVM has found to be effective and popular in a diversity of classification tasks because it is mostly used for solving classification problems. SVMs contain two

important properties that are the margin optimization and kernel called a radial basis function that can be used to learn complex regions.

The kernel function is used to transform the dataset. The role of this function is a mapping of transactions between the input space and a higher dimensional space [13].

The kernel function is described by:

$$K(X1, X2) = \Phi\{(X1), (X1)\} \quad (3)$$

where $\Phi : X \rightarrow H$ map transactions in input space X to higher dimensional space H.

The hyperplane is used to separate the transactions, after applying the kernel function to the dataset.

Hyperplane is described by:

$$\{W, X\} + B = 0 \quad (4)$$

The main role of the hyperplane is to maximize the separation between both transactions, which helps to reduce potential errors caused by over training.

Therefore, the classification for a support vector machine defined as:

$$\sum_i \alpha_i Y_i K(X_i, X) + B = 0 \quad (5)$$

The Gaussian radial basis function and polynomial function are the most common kernel functions used which is dependent on the dataset and classification requirements [30]. An instance of transaction class is that separated by a hyperplane. Transaction classes of two distinct cards are represented in blue and black bullets (data samples). Support vectors work as a boundary to each class of credit card transaction. If transactions lie outside support vector boundary, considered as an Outlier or fraud activity. New samples are classified based on measuring its distance from the hyperplane (Nguwi and Cho [37]).

SVM has been classified into four categories namely Binary support vector system (Chen et al. [12]), classification model based on decision tree and SVM (Sachin and Duman [44]). Novel questionnaire responder transaction approach with SVM (Chen et al. [13], and Class Weighted SVM model (Lu and Ju [30]). It has been developed on Class Weighted Support Vector Machine for credit card fraud detection.

The model is more appropriate for solving fraud detection problem with high. The Various research (Zareapoor et al. [60], Seeja and Zareapoor [46], Bhattacharyya et al. [6] have used SVM Technique for credit card detect fraudulent transactions.

4.10 Hidden Markov model

Hidden Markov Model (HMM) is a probability and statistical Markov model which can be used to model sequential data. It is a double embedded random process with two states, one is unobserved ("hidden") and other is open to all. It is a finite set of states, each of which is associated with a probability distribution. HMM are effectively applied to many areas such as speech recognition, robotics, bio-informatics, data mining etc. This paper focuses on credit card fraud detection using HMM. The cardholder spending profile is divided into a low, medium, and high. The cardholder profile consists of a set of spending information namely money spent on each transaction, purchase time of last good, type of purchasing goods, the name of the merchant and last place purchase goods, etc. HMM is trained based on the cardholders normal behavior and if incoming credit card transaction is not accepted by the model with high probability that transaction is considered as a fraudulent transaction. HMM is also maintaining a log of the previous transaction. Bhusari and Patil [7] discussed how HMM used to detect credit card

transaction fraud with a low false alarm 8% and found out more than 88% transactions are genuine. Another researches([2,18,24]) are also used HMM to detect a credit card fraud. These machine learning techniques are also contained some pros and cons.

Table 4 presents a comparison of these techniques based on learning, classification and clustering approach to detect credit card fraud, Learning Approach/Categories (LA/C).

5 Dataset and its attributes

The performance of any technique is purely dependent on the quality of the dataset. The datasets used by the various researcher to evaluate their proposed techniques and implemented methodologies are studied and summarized in table 5. The credit card datasets have been categorized as real world datasets (like Mellon Bank) and synthetic datasets (like UCSD-2009), and their primary and derived attributes discussed in details which play an important role in enhanced fraud detection rate and accuracy.

The credit card dataset contains two types of attributes, namely primary and derived attributes. These attributes were used in various studies [6, 25, 32, 36, 61] to detect credit card transaction frauds.

Primary attributes:

When credit card users are made transactions, a set of primary transnational attributes are generated. Based on the research papers mentioned in table 5, following attributes in table 6 are diagnosed as primary features of the credit card.

These primary attributes (features) help to design a good fraud detection system.

Beside primary attributes, **derived attributes** are also important but it is a very difficult task to extract the appropriate derived attribute from primary attributes.

Withrow et al. [56] have suggested transaction aggregation strategy approach to extract derived attributed based on the following three steps from the primary attributes available in the credit card transaction datasets:

- (a) Grouping transactions by card identification number.
- (b) Selecting transactions made in a previous period.
- (c) Grouping selected transactions on the basis of one of the primary feature.

The derived attributes are used to accurate analysis of cardholders buying behaviors. The derived attributes are summarized in table 7.

6 Performance matrices and evaluation criteria

The standard evaluation criteria have been followed by many researchers [4, 30, 36, 46, 49, 61] for evaluating their proposed model of credit card fraud detection.

The main objectives of these evaluation parameters (criteria) are to minimize false detection of fraud/non-fraud transactions and maximize the actual detection of fraud /non-fraud transactions. The formulae used by the many researchers for evaluation of their model have been presented in table 8 (P= Positive, N = Negative, FP = False Positive, FN = False Negative, TP = True Positive, TN = True Negative).

The performance metrics are discussed in table 8 that used by the various researcher to evaluate their method and determine the performance of fraud detection techniques.

Table 4: Comparison of various fraud detection techniques

	Techniques (LA/C)	Pros	Cons
Classification Supervised/	Back Propagation Neural Network	To determine the best performance of the system, we need a retrain of parameters such as the number of hidden neurons, learning rate, and momentum	It requires long training time and extensive testing.
	Bayesian Network	System processing, accuracy, and detection speed are very high.	Required excessive training and expensive.
	K-nearest neighbor (KNN)	There is no requirement of the predictive model before transaction classification in a dataset.	The fraud detection accuracy depends on the measure of distance between two neighbors. This technique cannot detect the fraud at the time of transaction.
	Support Vector Machine (SVM)	It is capable of detecting the fraudulent activity at the time of the transaction and solving nonlinear classification problems. SVM technique provides a unique solution for the optimality problem is bulging.	This technique is hard for auditors to process outcomes due to the transformation of input set and sometimes it fails to detect fraud cases. It is expensive, medium accuracy and has a low speed of detection. Lack of results transparency.
	Decision Tree (DT)	A decision tree is simple to use, implement, display and easy to understand. It can handle well non-linear data. It requires low computational power for training, high flexibility, good explainable.	This technique involves the complex algorithm and even a small change in the data can distract the structure of the tree. Need to check each transaction one by one. Choosing splitting criteria are also complex.
Clustering Unsupervised/	Self-organizing Map	This technique is simple to implement and very easy for auditors are given visual nature of outcomes.	Visualization requires auditor observation. This technique is not being fully automated.
	Hidden Markov Model (HMM)	HMM technique is fast in fraud detection and capable of detecting the fraudulent activity at the time of the transaction. HMM-based models reduce the False Positive (FP) transactions predict as fraud, though they are genuine User.	It cannot detect the fraud in the initial few transactions. It is highly expensive and low accuracy. It cannot scalable to large size datasets.
Classification Semisupervised	Artificial immune system	This is highly suitable for classification problems with imbalanced data. Pattern recognition capability is also a high and powerful technique for learning. It is diversity, dynamically changing coverage, multi-layered, and Inexpensive.	Need a very high computational power for operation to make it unsuitable for real-time functions. The handling missing data are poor and need higher training time.

Table 5: Analysis of credit card dataset used between 1994 and 2019

Year	Dataset sample size	Source
1994	1,100,000 transactions authorized in a two month period.	Mellon Bank [20]
1999	500,000 records of both banks. Chase Bank (20% fraud and 80% non-fraud distribution) and First Union Bank (15% fraud, non-fraud 85%).	Chase Bank and First Union Bank [9]
2002	Data Come from SQL server database containing sample Visa Card transactions.	Synthetically created Data [52].
2005	6000 credit card data, normal accounts (84%) and fraudulent account(16%).	Major US bank [29]
2008	About 50 million transactions (49,858,600 transactions), one million (1,167,757 credit cards) credit cards from a single country.	International CC operators transactions [40]
2009	25,000 payment observations, fraud (5,529) and non-fraud (19,471).	Taiwan bank [59]
2010	462279 unique customers data have 4 million transactions & 5417 fraud transaction	Financial institute in Ireland(WebBiz) ³ [8]
2011	250,000 transactions, fraud (1050), & remaining none fraud.	Turkish bank [17]
2012	640361 transactions contain by 21746 credit cards.	A Large Australian bank [57]
2013	22 million CC transactions, fraud (978) and remaining non-fraud.	Bank's CC data warehouses [45]
2014	Details of 41647 transactions and 3.74% is fraudulent.	Brazilian bank transaction [39]
2014	100000 transaction. But 21000 transaction for training and 19918 for testing out of 40,918 unspecified transactions.	UCSD-FICO [46]
2015	9,387 transactions, 939 fraud and 8,448 non fraud	Real life dataset from an anonymous bank in Turkey [32].
2016	10000 records, numeric data with 334 input attributes.	UCSD-2009 (Synthesized) [55]
2017	10000 transactions, 20 attributes of German Credit data	UCI respiratory [3]
2018	30,000,000 individual transactions, 82,000 transactions fraud	E-commerce company of China [58]
2019	German Credit card 1000 transaction & 21 attributes.	UCI ML respiratory (Real data) [48, 49]
2019	Ten million credit card transactions with 8 variables	https://packages.revolutionanalytics.com (Real data) [33]

Table 6: Primary attributes of credit card

Attribute Name	Description
Account Number	Identification number of the Credit Cardholders
Card Number	Is a Credit Card number
Cardholders Age	Present an age of Credit Cardholders
Cardholders Gender	Gender of the Credit card holder (male, female, other)
Type of Card	Visa debit, Master Card, American Express, etc.
Transaction ID	Transaction identification number
Transaction Place	Place where transaction made (Determine by System IP Address, if online)
Entry Mode	Chip and pin, magnetic stripe
Transaction Time/Date	Time and Date of the transaction
Amount	Amount of the transaction n USD, EURO, INR, etc.
Terminal Type	Transactions by the Internet, ATM, POS, Mobile, etc.
Country Transaction	Where transaction made by cardholders
Country Home	Residence country of cardholders
Merchant Name	Name of merchant who is provides service to cardholders
Merchant Code	Is a merchant identification number
Merchant Group	Merchant group identification
Merchant City, Country	Name of merchant city & country

Table 7: Derived attributes of credit card

Attribute Name	Description
Amount-Same-Day	Total amount spent on the same day up to this transaction
Number-Same-Day	Total number of transactions on the same day up to this transaction
Amount-Same-Month	Total amount in the same month up to this transaction.
Average-Same-Month	Average amount spent over a month up to this transaction.
Amount-same-Merchant	All transactions amount spent in the same merchant up to present transaction.
Number-Same-Merchant	Total number of transactions with the same merchant during 6 month
Number-Same-Hour	Total number of transactions in the same hour up to present transaction.
Amount-Same-Hour	Total amount spent in the same hour up to present transaction.
Transaction amount over a month	Average amount spent per transaction over a month on all transactions up to present transaction.
Previous-Amount	Previous amount of transaction.
Average amount over 3 months	Average amount spent over the course of 1 week during the past 3 months

Table 8: Evaluation criteria for Credit card fraud detection

Measure	Formula	Description
Accuracy (Detection rate)	$TN+TP/TP+TN+FP+FN$	The percentage of correctly predicated transactions.
Precision (Hit rate)	$TP/TP+FP$	It is the number of classified fraud transactions that actually are fraud transactions, and gives the accuracy of the fraud transaction.
False Positive Rate (False alarm rate)	$FP/FP+TN$	The ratio of credit card fraud detected incorrectly.
True Positive Rate (Sensitivity or recall)	$TP/TP+FN$	It is the number of correctly classified fraud transaction and gives the accuracy of the fraud transaction.
True negative rate (Specificity)	$TN/TN+FP$	It is the amount of correctly classified non-fraud and gives the accuracy of the non fraud transaction.
False Negative Rate	$FN/P=1-TP$ rate	It is the number of credit card transaction classified as a non-fraud as a percentage of all fraudulent.
ROC	True positive rate plotted against false positive rate	Relative Operating Characteristic curve, a comparison of TPR and FPR as the criterion changes.
Cost	$100 * FN + 10 *(FP +TP)$	Present a cost of FDS.
F-measure	$2*(Precision*Recall)/ (Precision + Recall)$	The Weighted average of the precision and recall, Gives the harmonic mean of precision and recall.
Balanced Classification Rate	$1*(TP/P+TN/N)$	It is the average sensitivity and specificity.
Mathews Correlation Coefficient	$(TP*TN)-(FP*FN)/ \{(TP+FP)(TP+FN)(TN+FP)(TN+FN)\}$	Used as a measure of the quality of binary classification, correlation coefficient between the observed and predicate binary classification.
Geometric Mean	$(Sensitivity *Specificity).05$	Gives the geometric of fraud and non-fraud accuracies.
Weighted-Accuracy	$W*Sensitivity+(1-w)*Specificity$	Provide performance summary that indicators of each tradeoff.

Table 9: The Performance comparison of various DM & ML Techniques

Reference	Method	Sensitivity	Specificity	Accuracy
[22]	AIS	33.6-52.6%	97.8-98.1%	94.6-96.4%
[6]	LR	24.6-74.0%	96.7-99.8%	96.6-99.4%
	SVM	43.0-68.7%	95.7- 99.8 %	95.5-99.4%
	RF	42.3-81.2%	97.9-99.8%	97.8-99.6%
[36]	KNN	81.82%	97.61%	96.52%
	KNN+DRF	81.97 %	98.62%	97.47%
[4]	NB	82.10-95.15%	97.54-98.96%	97.52-97.69%
	KNN	82.85-93.75%	100-100 %	97.15-97.92%
	LR	71.55-58.33%	29.39-53.13%	36.39-54.86 %
[43]	SVM	55.43-73.60%	70.41- 73.41%	70.41-73.41%
	GP	85.64-95.09%	89.27-94.14%	89.27-94.14%
	NN (FF)	67.24-80.21%	75.32-78.77%	75.32-78.77%
	GMDH	87.44-93.46%	88.34-95.18%	88.14-93.00%
	LR	62.91-65.23%	70.66-78.88%	66.86-70.86%
	NN(Prob)	87.53 -98.09%	94.07-98.09%	95.64-98.09%
[11]	RUSMRN	53.36%	88.13%	79.73%
	RUSBoost	50.3%	86.16%	77.8%
	AdaBoost	31.4%	83.1%	57.73%
	Naive Bayes	40.2%	78.8%	70.13%

6.1 Comparative study of learning technique

In this study, the performance of a variety of Data mining & machine learning technique in terms of sensitivity, specificity, and accuracy are presented in table 9. This study has been classified credit card fraud detection researches based on these performance measures. The result of various researches showed in table 9 and identify that specificity and accuracy were slightly better of *KNN+DRF* technique [36] with compare to other methods. The sensitivity, specificity, and accuracy have been better of NB and KNN technique [4]. It clearly identified that some results are vary based on credit card transactions dataset size and detection techniques. If credit card dataset is too large than accuracy could be decreased. This study has been classified credit card fraud detection researches based on these performance measures. The result of various researches showed in table 9, sensitivity and accuracy was slightly better for Self-organization map [8] with compare to other methods. The sensitivity, specificity, and accuracy have been better of NB and KNN technique [4]. It clearly identified that some results are vary based on credit card transactions dataset size and detection techniques. If credit card dataset is too large than accuracy could decrease.

7 Conclusion and future work

In this paper, various research papers based on credit card fraud are studied and discussed based on the finding of these papers, the various credit card frauds are classified and among them, card-not-present fraud and skimming frauds are more frequently occurred. The fraudsters mostly used website cloning, the false merchant website, and phishing methodology to steal credit card detail. The challenges and issues to prevent and detect the fraud have also been discussed and identified that one of the biggest issues is benchmark dataset which has unskewed, balanced and free from the anomaly and real-world dataset.

The pros and cons of numerous fraud detection techniques are discussed and concluded that the major researchers were performed under a supervised learning method based on available datasets. Different convention dataset was used to compare the performance of various methodologies on the base of various performance measures using the sensitivity, specificity, and accuracy. This paper also presented a comparative analysis of different fraud detection techniques and identified that NB (95.15%, 98.96%, and 97.69%), KNN (93.75%, 100%, and 97.92%) & KNN-DRF (81.97%, 98.62%, and 97.47%) gives better results among the studied techniques. The primary and derived attributes of credit card dataset have been playing an important role in enhanced fraud detection rate and accuracy.

In this paper, techniques based on machine learning are discussed. The study can be extended for bio-inspired algorithms which have not explored in the paper and the result can be compared with traditional MLT. More effects can be made to get the real dataset from the credit card issuing and managing organization, so that the exact techniques can be compared on the real dataset.

In future, this work can further be extended on the enhancement of fraud detection techniques based on the detection accuracy, precision, MCC and improvement of fraud detection evaluation criteria. Security guidelines are needed for credit card users to make them aware of how to use and secure card details.

Acknowledgment

We gratefully acknowledge the funding agency, the University Grant Commission (UGC), Delhi, Government of India for providing financial support to complete this work. And also,

USICT, Guru Gobind Singh Indraprastha University, Delhi, India to provided the facilities to complete research and Editors-in-Chief of IJCCC.

Bibliography

- [1] Abdallah, A.; Maarof, M. A.; Zainal, A.(2016). Fraud detection system: A survey, *Journal of Network and Computer Applications*, 68, 90-113, 2016.
- [2] Agrawal, A.; Jain,A.; Kumar, B. S.(2019). Deep Learning Based Classification for Assessment of Emotion Recognition in Speech, *Available at SSRN 3356238*.
- [3] Alam, F.; Pachauri, S. (2017). Detection using weka, *Advances in Computational Sciences and Technology*, 10(6), 1731-1743, 2017.
- [4] Awoyemi, J. O.; Adetunmbi, A. O.; Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis, *2017 International Conference on Computing Networking and Informatics (ICCNI)*, IEEE, 1-9, 2017.
- [5] Bai, B.; Yen, J.; Yang, X. (2008). False financial statements: characteristics of China's listed companies and cart detecting approach, *International journal of information technology & decision making*, 7(2), 339-359, 2008.
- [6] Bhattacharyya, S.; Jha, S.; Tharakunnel, K. Westland, J. C. (2011). Data mining for credit card fraud: A comparative study, *Decision Support Systems*, 50(3), 602-613, 2011.
- [7] Bhusari, V.; Patil, S.(2011). Application of hidden markov model in credit card fraud detection, *International Journal of Distributed and Parallel systems* 2(6), 203, 2011.
- [8] Brabazon, A.; Cahill, J.; Keenan,P.; Walsh,D.(2010).Identifying online credit card fraud using artificial immune systems, *Evolutionary Computation (CEC), 2010 IEEE Congress on IEEE*, 1-7, 2010.
- [9] Chan, P. K.; Fan, W.; Prodromidis, A. L.; Stolfo, S. J.(1999). Distributed data mining in credit card fraud detection, *IEEE Intelligent Systems and Their Applications*, 67-74, 1999.
- [10] Chandola, V.; Banerjee, A.; Kumar, V. (2009). Anomaly detection: A survey, *ACM computing surveys (CSUR)*, 41(3), 1-72, 2009.
- [11] Charleonnan, A. (2016). Credit card fraud detection using RUS and MRN algorithms, *2016 Management and Innovation Technology International Conference (MITicon)*, IEEE, MIT73-MIT76, 2016.
- [12] Chaudhary, K.; Yadav, J.; Mallick, B. (2012). A review of fraud detection techniques: Credit card, International, *Journal of Computer Applications* , 45 (1), 39-44, 2012.
- [13] Chen, R.C.; Chiu, M.L.; Huang, Y.L.; Chen, L.T. (2004). Detecting credit card fraud by using questionnaire responded transaction model based on support vector machines, *nternational Conference on Intelligent Data Engineering and Automated Learning*, Springer, 800-806, 2004.
- [14] Chen, R.C.; Luo, S.T.; Liang, X.; Lee, V.(2005). Personalized approach based on svm and ann for detecting credit card fraud, *International Conference on Neural Networks and Brain*, IEEE, 810-815, 2005.

-
- [15] Cortes, C.; Vapnik, V.(1995). Support-vector networks, *Machine learning*, 20(3), 273-297.
- [16] Craciun, M.; Ratiu, C.; Bucerzan, D.; Manolescu, A. (2013). Actuality of Bankruptcy Prediction Models used in Decision Support System, *International Journal of Computers Communications & Control*, 8(3), 375-383, 2013.
- [17] Duman, E.; Ozelik, M.H.(2011). Detecting credit card fraud by genetic algorithm and scatter search, *Expert Systems with Applications*, 38(10), 13057-13063, 2011.
- [18] Falaki, S.; Alese, B.; Adewale, O.; Ayeni, J.; Aderounmu, G.; Ismaila, W.(2012). Probabilistic credit card fraud detection system in online transactions, *Int. J. Softw. Eng. Appl*, 6 , 69-78, 2012.
- [19] Gadi, M. F. A.; Wang, X.; do Lago, A. P. (2008). Credit card fraud detection with artificial immune system, *in:International Conference on Artificial Immune Systems*, Springer, 119-131, 2008.
- [20] Ghosh, S.; Reilly, D. L.(1994). Credit card fraud detection with a neural-network,In System Sciences, *Proceedings of the Twenty-Seventh Hawaii International Conference on*, IEEE, 3, 621-630, 1994.
- [21] Guo, T.; Li, G.Y. (2008). Neural data mining for credit card fraud detection, *2008 International Conference on Machine Learning and Cybernetics*, IEEE, 7, 3630-3634, 2008.
- [22] Halvaiee, N. S.; Akbari, M. K.(2014). A novel model for credit card fraud detection using artificial immune systems, *Applied Soft Computing*, 24, 40-49, 2014.
- [23] Huang, R.; Tawfik, H.; Nagar, A.K. (2010). A novel hybrid artificial immune inspired approach for online break-in fraud detection, *Procedia Computer Science*, Elsevier, , 1(1), 2733-2742, 2010.
- [24] Iyer, D.; Mohanpurkar, A.; Janardhan, S.; Rathod, D.; Sardeshmukh, A. (2011). Credit card fraud detection using hidden markov model, *Information and Communication Technologies (WICT), World Congress on*, IEEE, 1062-1066, 2011.
- [25] Jha, S.; Guillen, M.; Westland, J. C. (2012). Employing transaction aggregation strategy to detect credit card fraud, *Expert systems with applications*, 39(16), 12650-12657, 2012.
- [26] Kirkos, E.; Spathis, C.; Manolopoulos, Y.(2007). Data mining techniques for the detection of fraudulent financial statements, *expert systems with applications* , 32(4), 995-1003, 2007.
- [27] Kohonen, T. (1990). The self-organizing map, *Proceedings of the IEEE*, 78(9), 1464-1480, 1990.
- [28] Kokkinaki, A. I. (1997). On atypical database transactions: identification of probable frauds using machine learning for user Profiling, *Knowledge and Data Engineering Exchange Workshop, IEEE proceedings*, 107-113, 1997.
- [29] Kou, G.; Peng, Y.; Shi, Y.; Wise, M.; Xu,W. (2005). Discovering credit cardholders behavior by multiple criteria linear programming, *Annals of Operations Research*, 135, 261-274, 2005.
- [30] Lu, Q.; Ju, C. (2011). Research on credit card fraud detection model based on class weighted support vector machine, *Journal of Convergence Information Technology*, 6, 2011.

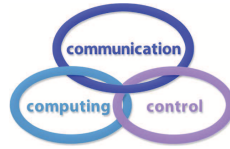
-
- [31] Maes, S.; Tuyls, K.; Vanschoenwinkel, B.; Manderick, B. (2002). Credit card fraud detection using bayesian and neural networks, *Proceedings of the 1st international naiso congress on neuro fuzzy technologies*, 261-270, 2002.
- [32] Mahmoudi, N.; Duman, E. (2015). Detecting credit card fraud by modified Fisher discriminant analysis, *Expert Systems with Applications*, 42(5), 2510-2516.
- [33] Makki, S.; Assaghir, Z.; Taher, Y.; Haque, R.; Hacid, M. S.; Zeineddine, H. (2019). An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection, *IEEE Access*, 7, 93010-93022, 2019.
- [34] Meyer, A.; Zimmermann, H.-J. (2011). Applications of Fuzzy Technology in Business Intelligence, *International Journal of Computers Communications & Control*, 6(3), 428-441, 2011.
- [35] Minegishi, T.; Niimi, A. (2011). Detection of fraud use of credit card by extended VFDT, *Internet Security (WorldCIS), 2011 World Congress on*, IEEE, 152-159, 2011.
- [36] Nami, S.; Shajari, M. (2018). Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors, *Expert Systems with Applications*, 110, 381-392, 2018.
- [37] Nguwi, Y.Y.; Cho, S.Y. (2010). An unsupervised self-organizing learning with support vector ranking for imbalanced datasets, *Expert Systems with Applications*, 37 (12), 8303-8312, 2010.
- [38] Nunes, C. L.; De Castro, L. N.; Timmis, J. (2002). *Artificial immune systems: a new computational intelligence approach*, Springer Science and Business Media, 2002.
- [39] Olszewski, D. (2014). Fraud detection using self-organizing map visualizing the user profiles, *Knowledge-Based Systems*, 70, 324-334, 2014.
- [40] Paasch, C. A. (2008). *Credit card fraud detection using artificial neural networks tuned by genetic algorithms*, Hong Kong University of Science and Technology, Hong Kong, 2008.
- [41] Panigrahi, S.; Kundu, A.; Sural, S.; Majumdar, A. K. (2009). Credit card fraud detection: A fusion approach using Dempster-Shafer theory and bayesian learning, *Information Fusion*, 10(4), 354-363, 2009.
- [42] Quah, J. T.; Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence, *Expert systems with applications*, 35 (4), 1721-1732.
- [43] Ravisankar, P.; Ravi, V.; Rao, G. R.; Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques, *Decision Support Systems*, 50(2), 491-500.
- [44] Sahin, Y. G.; Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines, *Processing of the international multi conference Engineering and computer Scientist*, 1, 2011.
- [45] Sahin, Y.; Bulkan, S.; Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection, *Expert Systems with Applications*, 40(15), 5916-5923, 2013.
- [46] Seeja, K.; Zareapoor, M. (2014). Fraudminer: a novel credit card fraud detection model based on frequent item set mining, *The Scientific World Journal*, ID 252797, 2014.

-
- [47] Singh, A.; Jain, A. (2018). Study of cyber attacks on cyber-physical system, *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIOTCT)*, 26-27, 2018.
- [48] Singh, A.; Jain, A. (2019). Adaptive Credit Card Fraud Detection Techniques Based on Feature Selection Method, *Advances in Computer Communication and Computational Sciences*, Springer, Singapore, 167-178, 2019.
- [49] Singh, A.; Jain, A. (2019). A Novel Framework for Credit Card Fraud Prevention and Detection (CCFPD) Based on Three Layer Verification Strategy, *Proceedings of ICETIT 2019*, Springer, Cham, 935-948, 2019.
- [50] Sorournejad, S.; Zojaji, Z.; Atani, R. E.; A. H. Monadjemi (2016). A survey of credit card fraud detection techniques: Data and technique oriented perspective, *arXiv preprint arXiv:1611.06439*, 2016.
- [51] Stolfo, S.; Fan, D. W.; Lee, W.; Prodromidis, A.; Chan, P. (1997). Credit card fraud detection using meta-learning: Issues and initial results, *In AAAI-97 Workshop on Fraud Detection and Risk Management*, 83-90, 1997.
- [52] Syeda, M. ; Zhang, Y.-Q.; Pan, Y. (2002). Parallel granular neural networks for fast credit card fraud detection, *Fuzzy Systems, 2002. FUZZ-IEEE'02. Proceedings of the 2002 IEEE International Conference*, IEEE, 1, 572-577, 2002.
- [53] Tripathi, K. K.; Pavaskar, M. A. (2012). Survey on credit card fraud detection methods, *International Journal of Emerging Technology and Advanced Engineering*, 2(11), 721-726, 2012.
- [54] Tuo, J.; Ren, S.; Liu, W.; Li, X.; Li, B.; Lei, L. (2004). Artificial immune system for fraud detection, *IEEE International Conference on Systems, Man and Cybernetics*, IEEE, 2, 1407-1411, 2004.
- [55] West, J.; Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review, *Computers & security*, 57, 47-66, 2016.
- [56] Whitrow, C.; Hand, D.; Juszczak, P.; Weston, D.; Adams, N. (2009). Transaction aggregation as a strategy for credit card fraud detection, *Data Mining and Knowledge Discovery*, 18 (1), 30-55, 2009.
- [57] Wong, N.; Ray, P.; Stephens, G.; Lewis, L. (2012). Artificial immune systems for the detection of credit card fraud: an architecture, prototype and preliminary results, *Information Systems Journal*, 22 (1), 53-76, 2012.
- [58] Xuan, S.; Liu, G.; Li, Z.; Zheng, L.; Wang, S.; Jiang, C. (2018). Random forest for credit card fraud detection, *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, IEEE, 1-6, 2018.
- [59] Yeh, I.C.; Lien, C.h. (2009). The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients, *Expert Systems with Applications*, 36(2), 2473-2480, 2009.
- [60] Zareapoor, M.; Seeja, K.; Alam, M. A. (2012). Analysis on credit card fraud detection techniques: Based on certain design criteria, *International Journal of Computer Applications*, 52 (3), 35-42, 2012.

- [61] Zhang, X.; Han, Y.; Xu, W.; Wang, Q.(2019). HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture, *Information Sciences*, In Press, 2019.
- [62] <http://www.economictimes.indiatimes.com>, October 31, 2016. R. Dave, *Credit, debit card frauds and how you can avoid them*, Accessed on Nov 10, 2018.
- [63] <https://www.acfe.com>
- [64] <https://www.nilsonreport.com/upload>
- [65] <https://www.ic3gov.in>
- [66] <https://www.financialfraudaction.org.uk>

A Cluster-based Approach for Minimizing Energy Consumption by Reducing Travel Time of Mobile Element in WSN

J. Siva Prashanth, S.V. Nandury



J. Siva Prashanth*

Academy of Scientific and Innovative Res., CSIR-IICT Campus,
CSIR-Indian Institute of Chemical Technology, Hyderabad, India
*Corresponding author: sivaprashanth.j@gmail.com

Satyanarayana V. Nandury

Academy of Scientific and Innovative Res., CSIR-IICT Campus,
CSIR-Indian Institute of Chemical Technology, Hyderabad, India.
nvs@iict.res.in

Abstract: Envoy Node Identification (ENI) and Halting Location Identifier (HLI) algorithms have been developed to reduce the travel time of Mobile Element (ME) by determining Optimal Path(OP) in Wireless Sensor Networks. Data generated by cluster members will be aggregated at the Cluster Head (CH) identified by ENI for onward transmission to the ME and it likewise decides an ideal path for ME by interfacing all CH/Envoy Nodes (EN). In order to reduce the tour length (TL) further HLI determines finest number of Halting Locations that cover all ENs by taking transmission range of CH/ENs into consideration. Impact of ENI and HLI on energy consumption and travel time of ME have been examined through simulations.

Keywords: Envoy Nodes, Halting Locations, travel time, latency.

1 Introduction

Wireless Sensor Networks(WSN) are established by thousands of sensors distributed spatially over a specified geographical region for monitoring the changes in the environment. WSNs have wide range of applications like, health care monitoring, earth sciences, environmental sciences, military applications to detect intrusion of enemies disaster,tracking vehicular movement, etc. Sensor Nodes(SNs) are typically small electronic devices operated by battery with finite amount of energy. Each SN senses the environment and gathers the information about physical changes in the environment.Data generated by SN either periodically or continuously have to be submitted to the centralized processing unit called stationary Base Station (BS).

Contingent upon nature of the application, information detected by WSNs send either straightforwardly to a stationary BS or Mobile Element (ME). Usually BS location is fixed. In case if BS is located within the transmission range of a SN, then it will directly submit data to the BS. Otherwise, SN will send the data to its nearest neighbor, which will try to identify the shortest path and relay the data to the BS. There are few challenges associated with this traditional mechanism. Sometimes BS may be located far away from the area of interest, in such scenario SNs will not be able to communicate with the BS, apart from this, in large WSN considerable amount of energy will be spent for transmitting and receiving messages, this leads to high energy consumption and increased network traffic.

SNs nearest to BS have to allocate time slots for traffic coming from neighbor SNs, this result in traffic congestion. These nodes devour compared to other nodes. Such situation may prompt WSN's breakdown, as no information would reach BS if these nodes channel out the whole of their battery life.

The Above mentioned challenges can be addressed by employing a ME that travels along WSN space to gather data from SNs. The data gathered by the ME, is then submitted to BS [19]. However, it increases network latency. Latency can be minimized by identifying Envoy Nodes (EN), where EN is a node that ME must visit, in order to collect data. ME need not to visit exact geographical location of a EN, instead it can collect the data from any location within the transmission range of EN. Inspired by this ME's tour can be shortened further by identifying a set of locations in such a way that, ME will be able to collect data from all ENs by visiting these locations, these locations are referred to as Halting Locations (HL).

In literature various approaches makes use of heuristic approaches like Travelling Salesmen Problem (TSP) and Genetic Algorithms (GA) for defining ME's optimal tour [7, 12, 20].

In our previous work we have adopted a clustering method to minimize the energy consumption and decrease latency where every SN in a cluster is inside the transmission range of its Cluster Head (CH) [22]. As an extension to the previous work we try to investigate the effect of ME's TL on energy consumption. In this approach, Envoy Node Identification (ENI) algorithm has been developed to identify the number of ENs to be visited by the ME.

ME's tour consists of visit to all ENs. Optimal path(OP) that covers all ENs in WSN is identified using traditional TSP solver. Tour that has been given by TSP solver can further be reduced by visiting the HLI identified by Halting Location Identifier (HLI) algorithm. Adequacy of ENI and HLI have been evaluated in terms of optimizing the energy consumption and travel time of ME through simulation. An examination of simulation result shows that ENI, HLI outflank the COM and CSS.

Overview of research works related to clustering, energy issues and TL-optimization of ME discussed in Section 2. Section 3 presents an overview of proposed optimization approach. ENI and HLI algorithms described in Section 4. Section 5 showcases performance results through simulations carried out.

2 Related work

2.1 Minimizing the TL of mobile element

The problem of reducing TL of ME is addressed in [35]. First it carries out the cluster formation process as per [6], then the deployment region is partitioned into virtual grids and intersection points are identified. CHs have to choose one of these intersection points, so that ME can collect data from CHs by visiting these intersection points. Order of nodes to be visited is identified by a TSP solver.

A convex hull based method for reducing latency by considering amount of data to be collected is proposed in [36]. In this method a convex hull that covers all nodes is constructed. This process is applied progressively by eliminating nodes on previous layer of convex hull. This process is repeated until no nodes are left for further processing. All possible permutations for visiting nodes in layer - n and n-1 are explored in order to identify an OP. This process is applied progressively until all the layers are covered. Optimal TL of ME is obtained by adjusting speed of ME.

Two different approaches are presented in [32, 34] for optimizing TL. The first approach enables ME to move unreservedly over the network deployment area, TL optimization depends on the requirement that information from SNs should reach BS in a given deadline. Second

approach pre-characterizes ME's path and TL is optimization will be achieved by identifying HLI along the pre-characterized path.

Optimal disc coverage is a technique which gives Centre and radius of the optimal disc that covers given set of points.

In [11], an attempt made to reduce ME's TL by using COM and CSS algorithms. An OP connecting all nodes has been identified by employing a TSP. In this approach the location to be visited by ME is referred as collection site. Optimal disc coverage technique [31] was employed by COM for identifying collection sites that must be included in ME's.

Location of two nodes will be given as input to decisional Welzl's algorithm, if Welzl's radius is less than or equal to transmission range then the two nodes will be replaced by Welzl's centre in ME's tour. CSS identifies the common intersection areas and establishes rendezvous points(RP) in it. The optimality of TL in these methodologies is restricted by the TSP solver. ENI and HLI made an attempt to overcome this limitation.

2.2 Clustering

In WSN, when clustering approaches are adopted, members of cluster submit the data to its CHs and CHs submits the data to the BS, in such networks, the CHs near the BS usually tend to become the conduit point for bulk data transmissions between the BS and far away clusters. As a consequence, the energy of CHs nearer to the BS may drain out quickly.

To maximize the lifetime of CHs nearer to BS variable size clustering has been proposed in [17,19]. In both the approaches size of the clusters is defined by the distance of CH from BS. Since clusters nearer to BS will be of smaller size, the intra cluster communication and energy consumption for cluster routines is minimized so that the residual energy of CH can be utilized for relaying the incoming data to the BS.

Depending on the network topology it may happen that, some clusters accommodate more number of members. When a cluster has more number of cluster members, it leads to high energy consumption at cluster head and cluster head may drain out its energy very early. A clustering algorithm for addressing this problem is given in [27], size of the cluster and degree of a node are the two parameters that played key role in minimizing energy consumption.

A clustering algorithm based on common intersection area of SNs is proposed in [7], it groups the nodes having common intersection area in a cluster. Order of to be visited by ME is obtained by using GA. A genetic algorithm based cluster was proposed for reducing latency in [12].

Initially way points to be visited by ME are identified, then using weighing scheme nodes select one of the waypoint. These way points are optimized using genetic algorithms for minimizing ME's tour. An approach for determining optimized path from source to destination was proposed in [8].

As size of the cluster increases CH has to relay more number of packets and it leads to delayed transmission of data. This problem is address by exploiting nodes in common intersection area of clusters [9]. In this approach when waiting time of a packet at CH is more than the pre-defined threshold value, then node submits its data to neighbor CH through nodes in common intersection area. This phenomenon reduces packet loss and minimizes latency.

A protocol for minimizing the energy consumption by making use of beacon signal of ME is proposed in [23]. In this protocol a SN senses the environment periodically and goes to the sleep state, when a SN receive a Long Range beacon Signal from ME, it enters into active state. Node transmits data to ME when it receives Short Range beacon Signal and enters into sleep state.

Apart from latency and energy consumption fault tolerance is another issue associated with WSN. Even if the node detects fault and decides to reject the data, it takes considerable amount of time and energy. This problem is addressed by introducing Composite Interference Model

(CIM) in [4].

To determine Interference Fault-free Transmission (IFFT) schedule for all active links, a new approach Time Division Multiple Frequency (TDMF) is defined. Based on CIM and TDMF an algorithm for maximizing network throughput, Composite Interference-based Transmission Scheduling (CITS) is developed.

2.3 Energy issues

LEACH is one of the popular algorithm which has addressed the energy issues by adopting clustering mechanism [13]. An Energy Efficient Optimal Chain Protocol (EEOC) is proposed in [1].

EEOC has shown better performance than best known approaches in terms of first node die and last node alive. For extending the network lifetime and reducing data redundancy, a novel approach which is combination of chain based data transmission and clustering is proposed in [25].

A new clustering approach for achieving energy efficiency and reliability with the help of backup nodes is proposed in [26]. An attempt to achieve energy efficiency in delay sensitive applications is made in [24].

Raja et.al. tried to minimize the energy consumption by introducing multicasting mechanism and unequal size clustering [29].

Energy efficient and reliable routing is achieved using neural networks in [30].

Adoptive sectoring mechanism is used to prolong the network lifetime and reliable routing in [5]. A data collection strategy based on software defined network for enhancing network lifetime is proposed in [18].

A hybrid model of tree and cluster based approach is adopted for addressing hotspot issues, traffic congestion and energy issues in [15, 16, 21].

Shahinaz M. Al-Tabbakh adopted a tree based heuristic aggregation mechanism to enhance the network lifetime. A protocol for network lifetime improvisation is proposed in [10], it introduced a collection tree protocol to maintain dynamic routing table along with link state quality indicator.

Considerable amount of energy will be spent in WSN for data aggregation, this problem is addressed by using compressed sensing in [3].

3 Clustering approach to identify Envoy Nodes

Assuming a set of SNs $S = s_0, s_1, \dots, s_n$ have been deployed in an area where a set of phenomena are being monitored. Duty of ME is to collect data from all SNs in S . It minimizes multi hop communication and energy consumption, but it leads to increase in latency as ME needs to visit all nodes.

Latency can be reduced by identifying a set of Envoy Nodes $SEN = en_0, en_1 \dots en_n$ such that the sensed data of all nodes in the deployment region can be collected by ME by visiting all Envoy Nodes in SEN . The goal is to minimize the number of Envoy Nodes as many as possible.

In this paper we propose Cluster mechanism to further reduce the number of Envoy Nodes.

3.1 Cluster head selection

Geographical region that has to be monitored by WSN is divided into virtual square grids of side equivalent to $2 * T_r$.

Partitioning process will be started from centre of the optimal disc given by Welzl's algorithm [31].

Making use of the following equation, assuming d_0, d_1 as the distance from node s_0, s_1, \dots to centre cen_i of each grid G_i select a cluster head ch_i .

$$Ch_i = s_j \mid d_j \text{ is min } \{d_0, d_1, \dots\} \quad (1)$$

From (Eq.1) the node s_j that is nearer to cen_i will be ch_i for the grid G_i . Since length of each side of grid is $2 * T_r$, locating CH nearby centre of the grid guaranties single hop communication with maximum number of nodes within the grid, also maximizes node coverage within the grid.

3.2 Cluster formation

After obtaining set of cluster heads $CLH = ch_0, ch_1, \dots$, the nodes that are within one hop distance from a cluster head ch_i are made to join the cluster CL_i .

There is possibility that some CHs are closely located, it may lead to the situation that a CH becomes the member of other cluster. In order to avoid such situation cluster heads have to be excluded from cluster formation process as mentioned in (Eq. 2).

$$S' = S - CLH \quad (2)$$

A node s_j in S' joins the cluster CL_i if it belongs to the grid G_i and within the transmission range of CH ch_i .

$$S_j \in CL_i \forall s_j \in G_i \text{ if } dist(s_j, ch_i) < T_r \quad (3)$$

CH collects information from fellow cluster members and aggregates, this aggregated information will be transmitted to ME. Each node in CL_i submits it's data to ch_i . A node can join only one cluster. As soon as node joins a cluster it will be excluded from further clustering process. However, there is a possibility that few nodes may not fall into any cluster because of the reason that they are not within the transmission range of any of the cluster heads.

3.3 Envoy Node Identification

A node s_j in S is either a cluster member or a CH or a left over node. If s_j joins one of the clusters then it must belong to the set $CL_0, CL_1 \dots U CL_m$ it's data is represented by the cluster head ch_i and ch_i belongs to cluster head set CLH .

The edge or corner SNs which have not joined any of clusters form a set of left over nodes L are identified as per the equation given below:

$$L = S - \{CLH U \{CL_0 U CL_1 \dots CL_m\}\} \quad (4)$$

In addition to the cluster heads, set of envoy nodes SEN must also include the leftover nodes for ME's tour in order to ensure all nodes are visited.

$$SEN = CLH U L \quad (5)$$

ME can collect data from cluster members of CL_i by visiting it's cluster head ch_i i.e. ME covers all nodes in L_i by visiting ch_i . This altogether diminishes the quantity of ENs to be visited by the ME prompting significant reduction in the TL.

An optimised path for ME's tour covering all ENs in SEN is determined by using the best known TSP solver Lin-Kernighan [14].

Theorem 1. *Set of Envoy Nodes $SEN=en_0, en_1, \dots, en_k$ covers all nodes deployed in the network.*

Proof: Let S be a set of all nodes in the network.

Suppose s_j be a node in the network i.e $s_j \in S$

Case i: s_j is a cluster head. Since s_j is a CH it will included in CLH, from (5) SEN covers all CHs, it implies s_j is covered by SEN.

Case ii: s_j is a member of cluster cl_i in the network. Since $s_j \in cl_i$, it is represented by its cluster head ch_i , and from (6) all cluster heads are covered by SEN, it implies that node s_j is covered by SEN.

Case iii: s_j is a left over node in the network. Since s_j is a left over node it must belong to L, from (5)SEN covers all nodes in L, it implies node s_j is covered by SEN. Let s_j does not belong to S. If $s_j \notin S$ it implies it does not belong to the network. Hence it need not be covered by SEN. From above it can be concluded that SEN covers all nodes in the network. □

4 Halting location based path optimization

To further shorten the ME's path, Halting Locations are identified wherever possible, for each Envoy Nodes in SEN. The HLI optimizes the path determined by ENI by employing the HLIT technique introduced in this paper. TL of ME can be minimized by locating HLs along the tour given by TSP solver. Few ENs may have common intersection area or region, then ME can collect data by identifying a HL in the overlapping region.

Set of Halting Locations $SHL= hl_0, hl_1..hl_k$ along ME's tour that covers all Envoy Nodes in SEN are established by HLI using HLIT technique. Each hl_i covers one or more Envoy Nodes in SEN. For identifying the HLs, we developed HL Identification Technique (HLIT), it identifies an optimal HLs to substitute some of the ENs along ME's path.

HLIT exploits the fact that the ENs can transmit their information to ME even if they are at a distance T_r from the ME. HLIT enables ME to collect the data of EN form a distance of T_r from the EN where T_r is transmission range of EN .HLIT identifies optimal HLs covering all ENs.

$$\sum_{j=1}^{j=k} |hl_j| = \sum_{i=1}^{i=m} |en_i| = |S| \tag{6}$$

$|hl_j|$ denotes number of SNs covered by Halting Location hl_j .

$|en_i|$ denotes number of SNs covered by en_i

$|S|$ denotes total number of SNs.

m and k represents total number of ENs and HLs respectively.

Fig.1. is an illustrative example of our approach. Our objective is to achieve (6) with optimal values of k and m for obtaining optimal TL of ME. Contingent upon the separations between the ENs, HLIT decides HL dependent on three criteria depicted underneath:

Criterion 1: Overlapped Unit disc regions of Envoy Nodes.

Let us consider a scenario where the node deployment and ME's tour is as shown in Fig.1.(a).In Fig.1.(b) it can be observed that distance between EN_1 , EN_2 is $< 2*T_r$ i.e. there is an overlap region between EN_1 and EN_2 , any location within the overlap region will be at a distance less than T_r from both the ENs, hence ME can collect data from both ENs by visiting any location within the overlap region.

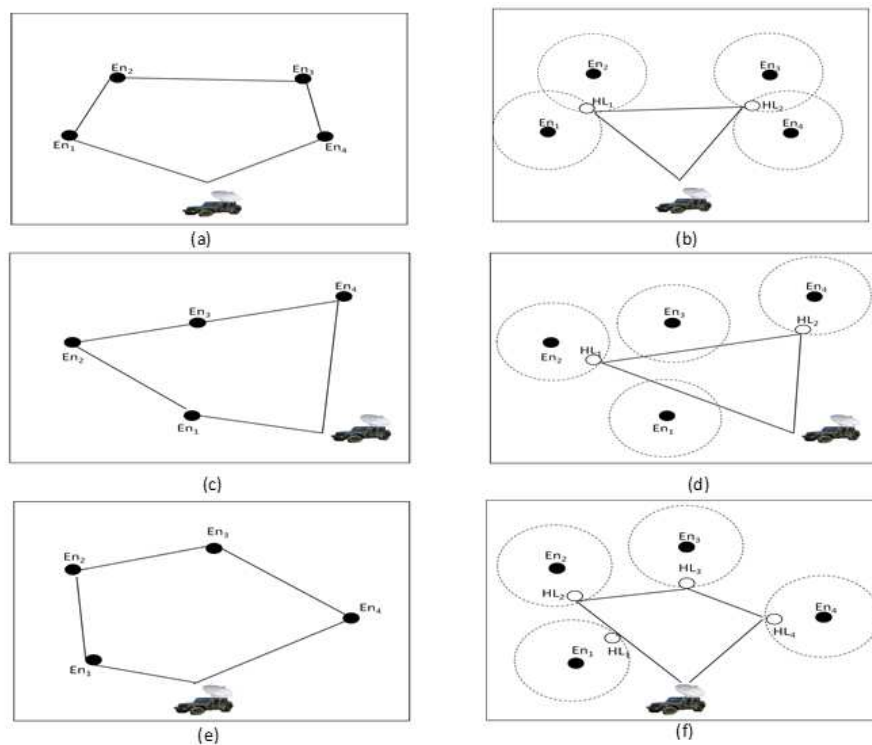


Figure 1: Illustrative example of Halting Location Identification Technique. (a), (c), (e) Actual tour of ME (b) HLIT based OP for Criterion 1. (d) Optimized HLIT based OP for Criterion 2. (f) HLIT based OP for Criterion 3

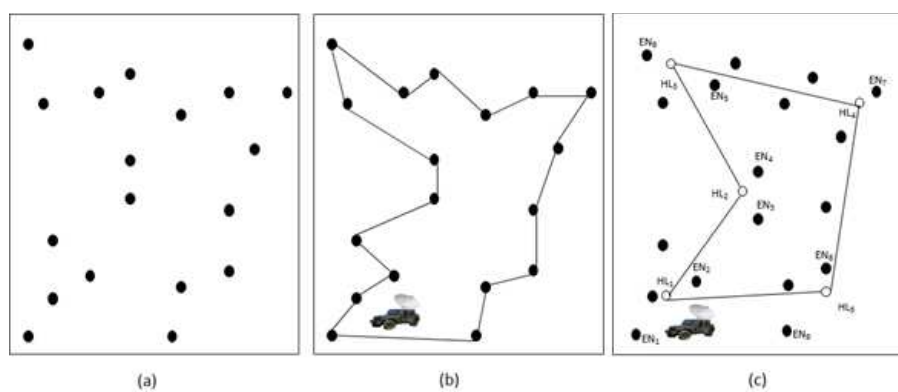


Figure 2: (a) Node Deployment (b) Tour given by TSP solver (c) Tour identified by HLI

HLIT determines a HL in the overlapping region of EN_1 and EN_2 , such that the distances from HL and either of two points is $\leq T_r$.

HLIT modifies SHL as per the equation given below:

$$SHL = SEN - \{en_{i+2}, en_{i+1}\} \cup \{hl_{i+1} \text{ if } \exists en_{i+1} \mid dist(en_{i+2}, en_{i+1}) \leq 2 * T_r \} \quad (7)$$

Halting Location hl_{i+1} in (7) is a location in the common intersection area nearest to ME's path from which ME will be able to receive data from both en_{i+1} , en_{i+2} . The ENs en_{i+1} , en_{i+2} are replaced by hl_{i+1} in SHL Since ME covers both en_{i+1} , en_{i+2} by visiting hl_{i+1} .

Criterion 2: en_{i+1} is at a distance $\leq T_r$ from the path en_i to en_{i+2}

Let us consider other node deployment scenario as shown in fig 1.(b). While ME is moving from its starting point to EN_2 , the path is intersecting with the unit disc region of EN_1 , that means distance from EN_1 to ME in the intersecting region is $\leq T_r$, hence ME can collect data from that EN while it is moving.

$$SHL = SEN - \{en_{i+1}\} \text{ if } \exists \{en_{i+1} \mid pre_dist(en_i, en_{i+1}, en_{i+2}) \leq T_r \} \quad (8)$$

In fig.1(d) EN_1 is at a distance $\leq T_r$ from the path defined from starting point to EN_2 , hence so ME can receive data from EN_1 when it is moving along the path from starting point to EN_2 .

In this case neither ME has to visit the exact location of EN_1 nor there is a need of identifying HL for EN_1 since ME can collect the data while it is moving, hence HLIT modifies HLI based on this criterion as per (8).

Criterion 3: en_{i+1} is at a distance $> T_r$ from the path en_i to en_{i+2}

Let us assume the node deployment scenario as per Fig.1.(e).

In this case ENs neither have overlap region nor it is covered by ME's path as discussed in Criterion 2, then a HL within the unit disc region of EN has to be identified for covering each EN.

Following equation determines HL for this scenario:

$$SHL = SEN - en_{i+1} \cup hl_{i+1} \quad \text{if } \exists en_{i+1} \mid per_dist(en_i, en_{i+1}, en_{i+2}) > T_r \quad (9)$$

Perpendicular distance is the minimum distance from a point to the line, inspired by this as per (9) perpendicular distance from en_{i+1} to the path from en_i to en_{i+2} will be calculated, if it is more than the transmission range then HLIT determines an HL hl_{i+1} at a distance T_r from en_{i+1} along the direction perpendicular to path from en_i to en_{i+2} . Fig.1(f) is an illustrative example of this approach.

While ME is moving from its starting point, perpendicular distance from EN_1 to the path from starting point to EN_2 is more than the transmission range, hence HLI based on HLIT identifies a halting location HL_1 as shown in fig.1(e), fig.2 shows the impact of our approach on TL, for the node deployment given in fig.2(a) ME's tour is identified by a TSP solver, fig.2(b) represents ME's tour.

Finally, after applying HLI the tour of ME will be as shown in fig.2(c). Algorithm 3 represents HLIT based HLI algorithm to identify HLs.

Lemma 2. *If unit disc regions of each Envoy Nodes in $SEN = \{en_i, en_{i+1}, \dots, en_l\}$ with transmission range T_r have common intersection area then Halting Location hl_p located in the intersection area covers all the Envoy Nodes in SEN .*

Algorithm 2 Envoy Node Identification - ENI

Input:

- 1: • Set of Envoy Nodes $SEN = \{ en_1, en_2, \dots, en_n \}$
- Transmission range T_r

Output:

- 2: • Set of Halting Locations

Start:

- 3: $q=0$
- 4: **for** $i = 0$ to $n - 2$ **do**
- 5: $k \leftarrow i+1$
- 6: **if** en_i and en_{i+1} have common intersection area **then**
- 7: **while** envoy nodes en_i, \dots, en_k have common intersection are **do**
- 8: $k \leftarrow k+1$
- 9: **end while**
- 10: Find envoy nodes hl_q within the common intersection area of $\{ en_i, \dots, en_{k-1} \}$ which is nearer to path from en_i to en_k
- 11: $SEN \leftarrow SEN - \{ en_i, \dots, en_{k-1} \} \cup hl_q$
- 12: **else if** t **then** the path from en_i to $en_k + 1$ covers en_k
- 13: **while** the path from en_i to en_{k+1} covers set of Envoy Nodes $\{ en_i + 1, \dots, en_k \}$ **do**
- 14: $k \leftarrow k+1$
- 15: **end while**
- 16: $SEN \leftarrow SEN - \{ en_i + 1, \dots, en_k - 1 \}$
- 17: **else**
- 18: $hl_q \leftarrow$ point-to-point $en_i + 1, en_i + 2, \dots, T_r$
- 19: $SEN \leftarrow SEN - en_{i+1} \cup hl_{i+1}$
- 20: **end if**
- 21: $q \leftarrow q+1$
- 22: **end for**
- 23: $SHL \leftarrow$ Lin - Kernighan(SEN)

Algorithm 3 Point_at_dist (P_1, P_2, T_r)

Input:

- 1: • Two points P_1 and $P_2 \mid P_i \leftarrow (x_i, y_i)$
- Transmission range T_r

Output:

- 2: • Point P at a distance T_r from P_1 along the line (P_1, P_2)

Start:

- 3: $d = \text{dist}(P_1, P_2)$
- 4: $x = x_1 + (x_2 - x_1) * (T_r / d)$
- 5: $y = y_1 + (y_2 - y_1) * (T_r / d)$
- 6: $P = (x, y)$

Proof: Since hl_p is in common intersection area, distance from hl_p to any Envoy Nodes in SEN is less than or equal to T_r . Therefore hl_p covers all the ENs in SEN and hence Envoy Nodes in SEN can be replaced by hl_p in SEN. □

Lemma 3. *The path from en_i to en_{i+2} covers Envoy Nodes en_{i+1} if the distance from Envoy Nodes to the path is less than or equal to transmission range T_r .*

Proof: From (7) if distance from a Envoy Nodes en_{i+1} to the path from en_i to en_{i+2} is less than or equal to T_r mobile element can collect data from the en_{i+1} in its journey. Therefore path from en_i to en_{i+2} covers en_{i+1} and hence en_{i+1} can be eliminated from SEN. □

Lemma 4. *Envoy Node en_{i+1} is covered by Halting Location hl_p if it is neither having common intersection area with any other Envoy Nodes nor it is covered by the path from en_i to en_{i+2}*

Proof: From (10) HLI establishes a Halting Location hl_p at a distance of T_r from en_{i+1} in a direction perpendicular to the path from en_i to en_{i+2} if en_{i+1} is neither having common intersection area with any other Envoy Nodes nor it is covered by the path from en_i to en_{i+2} . Distance from hl_p to en_{i+1} is equal to T_r . Therefore hl_p covers en_{i+1} . □

Theorem 5. *Set of Halting Locations $SHL = \{hl_0, hl_1, \dots, hl_m\}$ covers all the nodes in $S = \{s_0, s_1, \dots, s_n\}$ deployed across the network.*

Proof: Let us assume that en_i be a Envoy Node in SEN.

Case i: Unit disc region of en_i with transmission range T_r as radius has common intersection area with a set of Envoy Nodes SEN.

From Lemma 2 Halting Location hl_p established by HLI covers all ENs in SEN. It implies SEN covers en_i .

Case ii: Distance from en_i to a point on the path from en_{i-1} to en_{i+1} is less than T_r .

From Lemma 3 path from en_{i-1} to en_{i+1} covers en_i . It implies SEN covers en_i .

Case iii: en_i is any EN in SEN, other than the one stated in case i and case ii.

From Lemma 4 HLI establishes a Halting Location hl_p within transmission range of en_i . It implies SEN covers en_i . In case i, ii and iii it has proven that SHL covers all ENs in SEN and from theorem 1 SEN covers all nodes in S, hence it can be concluded that SHL covers all nodes in S. □

Lemma 6. *Number of elements in SHL is less than or equal to the number elements in SEN.*

Proof: Let m be the total number of Envoy Nodes in SEN.

Let SEN represents a set of Envoy Nodes having common intersection area and k be the total number of Envoy Nodes in SEN.

From Lemma 2 Halting Location hl_p established by HLI covers all ENs in SEN, so ENs in SEN can be replaced by in SHL, total number of elements in SEN are $m - k$. If $k = 0$ total number of elements in SHL are m.

Therefore it can be concluded that, number of elements in SHL is less than or equal to the number elements in SEN. □

Theorem 7. *TL of SHL is less than the TL of SEN.*

Proof: Let us assume t be the TL to cover all the ENs in SEN.

Case i: Let us assume that few of ENs in SEN have common intersection area.

From Lemma 2 Halting Locations in SHL established by HLI covers all ENs in SEN. Let us assume t_1 be the TL to cover all the HLs in SHL. Number of HLs in SHL is lesser than the number of ENs, hence $t_1 < t$. It implies TL of SHL is less than tour length of SEN. Reduced TL contributes to minimize the travel time of ME.

Case ii: Let k number of ENs are not having common intersection area with any of the ENs in SEN. From Lemma 4 HLI establishes Halting Location hl_p at a distance equal to T_r , the resultant TL will be less than or equal to $t-k * T_r$, it implies TL of SHL is less than the TL of SEN. \square

5 Simulations and performance analysis

Simulations are carried out to examine the efficiency of proposed algorithms in terms of identifying ENs, minimizing TL and travel time of ME, minimizing latency and energy consumption by varying number of nodes, transmission ranges. This section details about the simulation model and analysis on efficiency of proposed approach.

5.1 Simulation model

WSN deployment area of size $500 \times 500 \text{ m}^2$ have considered for implementing and evaluating the performance of the proposed algorithms ENI and HLI.

Homogeneous WSN environment is adopted, where all SNs nodes are equipped with equal transmission range. In order to evaluate the performance of ENI and HLI for higher node density, number of SNs in deployment region varied from 1000 to 5000. Identification of ENs and HLs have been carried out by ENI and HLI respectively.

It is assumed that ME requires halting time H_T to collect data from ENs. In the simulations value of H_T is considered as 2 sec. For calculating the energy consumption in the network values of two terms E_{elec} and ε_{amp} are taken as 50 nJ/bit and 100 pJ/bit/m^2 , where E_{elec} is energy spent for running the electric circuitry, and ε_{amp} is energy spent for amplification [13], E_{Tx} , E_{Rx} represents transmission and receiving energies respectively.

TSP solver Lin-Kernighan algorithm is employed for defining ME's optimal tour to cover given set of ENs or HLs. It is assumed that ME moves with a uniform velocity of 10 m/sec . Results represented in each graph is mean of 50 simulations

Table 1: Simulation parameters

Parameter	Value
Field size	$500 \times 500 \text{ m}^2$
Node deployment	1000- 5000
Transmission range T_r	20m, 30m, 40m
Speed of ME	10 m/sec
Halting time H_T	2 sec
E_{elec}	50 nJ/bits
ε_{amp}	100 pJ/bit/m ²

5.2 Optimizing halting locations

In order to test the performance of ENI in terms of number of locations to be visited by ME, a new term Ratio of Halting Locations to the Total number of Nodes deployed (RHLTN) is introduced. RHLTN is calculated as follows:

$$RHLTN = 100 * \frac{Number\ of\ Halting\ Locations}{Total\ Number\ of\ Nodes\ Deployed} \quad (10)$$

Value of RHLTN is inversely proportional to the efficiency of an algorithm, low value of RHLTN indicates that ME can collect the data of all SNs by visiting very few locations, it means algorithm efficiency is high. We have calculated the RHLTN value of HLI and CSS for different transmission ranges (20, 30 and 40) and total number of nodes varying from 1000 to 5000. The graph is plotted by taking number of nodes on X-axis and RHLTN value on Y-axis. In graphs *HLI_20*, *HLI_30* and *HLI_40* indicates the RHLTN values of HLI for transmission ranges 20, 30 and 40 respectively. From the fig.3 it can be predicted that, irrespective of transmission ranges HLI outperforms CSS. When total number of nodes is 5000, RHLTN value of HLI is 20. It means ME needs to visit only 20 percent of the nodes in order to complete its tour for collecting the data, whereas for CSS it has to visit 45-50 percent. This phenomenon will have adverse effect on Travel time of ME and energy consumption in the network.

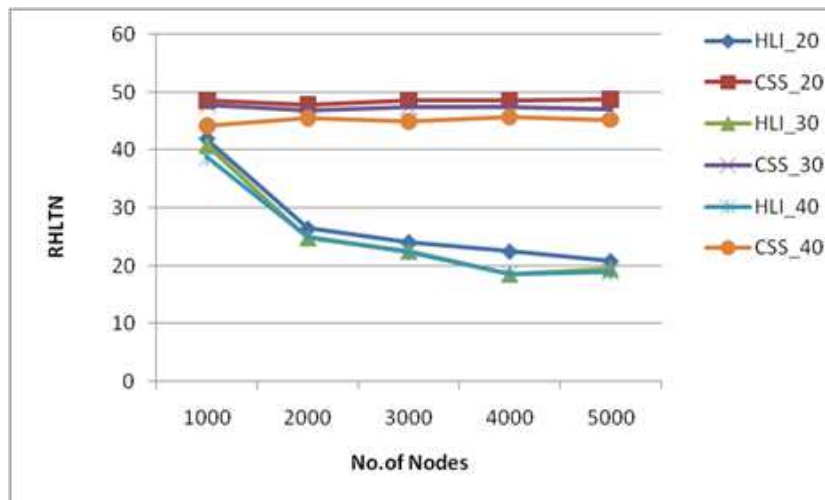


Figure 3: Ratio of halting locations to the total number of nodes

Minimizing travel time

TL refers to the total distance that has to be covered by ME for visiting a set of EN or HLs. Increase in number of ENs result in increased TL of ME. The TL has an immediate impact on the latency engaged with overhauling a query or a demand from a given SN. In order to obtain the OP covering set of ENs identified by ENI a TSP solver Lin-Kernighan algorithm [14] is employed. After obtaining the order of nodes to be visited, HLI establishes HLs using HLIT technique for minimizing the TL. A HL represents one or more ENs. Travel time of ME depends on number of ENs to be visited, speed of it and time taken for transferring data (halting time of ME) from EN to ME .

Assuming $d_{i,i+1}$ is the distance between Halting Locations HL_i and HL_{i+1} ; $v_{i,i+1}$ is the speed of ME while moving from HL_i to HL_{i+1} ; and HT_i is the halting time of ME at HL_i , the

amount of time T required by ME to collect data from all Envoy Nodes is calculated as follows:

$$T = \sum_{i=1}^n \frac{d_{i,i+1}}{v_{i,i+1}} + HT_i \quad (11)$$

If ME is moving with uniform speed v with a constant halting time HT then (11) becomes

$$T = \frac{\sum_{i=1}^n d_{i,i+1}}{v} + n * HT \quad (12)$$

In our simulations total travelling time of ME is calculated as per (12). It is assumed that ME is moving with a constant speed of 10 m/sec and halting time at each EN is 2 sec. As ME's speed and halting time are fixed travelling time depends on number of HLs to be visited. Graphs are plotted between total number of nodes deployed and travelling time as shown in the fig.4, in order to study the efficiency of HLI in terms of travelling time of ME. With the help of simulations it is proven that criterions considered in HLIT resulted in reduced travel time of ME.

From the graph it can be concluded that latency of the network can be reduced considerably with HLI. Travelling time of ME is very low for different transmission ranges. Simulation results prove that HLI is more suitable for applications in which data is time critical i.e. data has to reach the base station with in the stipulated time interval otherwise the data becomes obsolete. It can be concluded that HLIT technique adopted for identifying HLs in HLI has shown its impact in reducing the travel time of ME considerably irrespective of transmission ranges and number of nodes deployed. ENI and HLI offer better QOS compared to COM and CSS in terms of travel time and energy consumption.

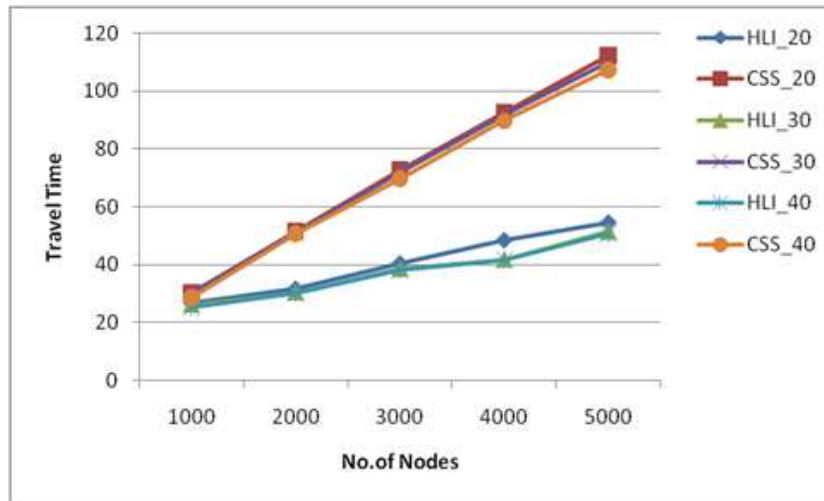


Figure 4: Travel Time .

5.3 Minimizing energy consumption

Every SN is equipped with finite amount of energy, this energy will be utilized for monitoring the targeted area, transmission and receiving of messages etc. For calculating energy consumption in the network the following equation is borrowed from [28].

$$E_{Tx} = E_{elec} * k + \varepsilon_{amp} * k * d^2 \quad (13)$$

$$E_{Rx} = E_{elec} * k \quad (14)$$

$$E_{Total} = E_{Tx} + E_{Rx} \quad (15)$$

Where (13) gives the energy consumption occurred E_{Tx} for transmitting k number of bits over a distance d . Energy consumption for receiving k number of bits E_{Rx} is given by (14). Total energy consumption E_{Total} is given by (15). In the literature it is observed that energy spent to hold the data, till the data is transferred to ME is not taken into consideration. We have tried to identify the energy consumption at each ENs for transferring the data to ME. It is assumed that Amount of time taken by ME to reach halting location i from halting location 1 is Holding time T_{iHold} is the amount of time the Envoy Nodes i has to hold the data.

From (11) T_{iHold} can be calculated as follows:

$$T_{iHold} = \sum_{i=1}^n \frac{\sum_{i=1}^n d_{i,i+1}}{v} + i * HT \quad (16)$$

Here T_{iHold} is the time taken by ME to reach HL hl_i since from the starting point of it's tour, i represents the index of HL in SHL, $d_{j,j-1}$ is the distance from hl_j to hl_{j-1} . v is the speed of ME. By taking holding time into consideration (13) is modified as follows:

$$E_i = 0.1 * E_{elec} * k * T_{iHold} + \epsilon_{amp} * k * d_i^2 \quad (17)$$

Total energy consumption in the network is calculated as follow:

$$E_{Total} = \sum_{k=1}^{k=n} E_k \quad (18)$$

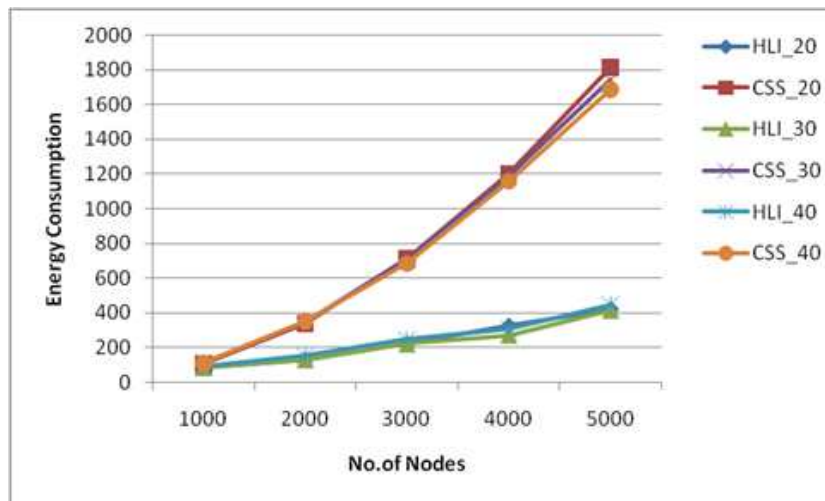


Figure 5: Ratio of Halting Locations to the Total number of Nodes.

Through the simulations we have tried to investigate the energy consumption of the network after applying HLI and compared it with CSS. In fig.5, initially there is not much difference whether it is HLI or CSS, but when total number of nodes is 5000, there is huge difference. We tried to diagnose the reason for this phenomenon, it is observed that travel time of ME is

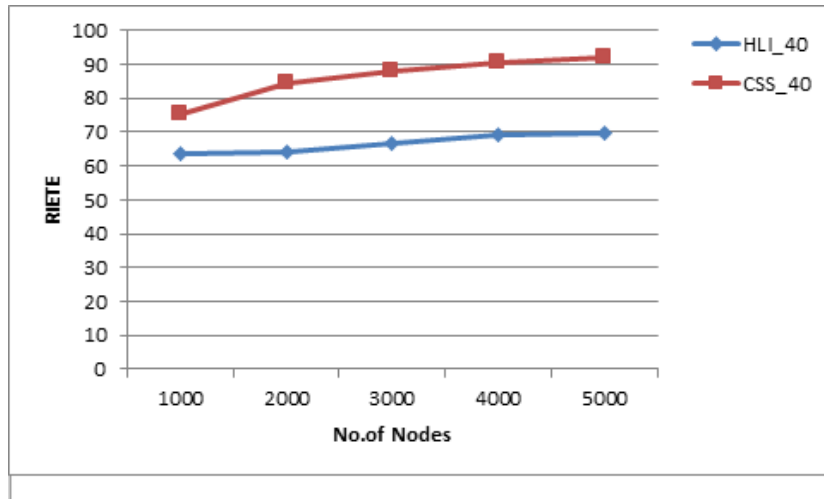


Figure 6: Ratio of Idle time Energy consumption to the Total Energy consumption .

influencing the energy consumption in the network, in order to substantiate this conclusion we have analyzed (17), in (17) all parameters are constants except T_{iHold} .

Hence energy consumption of a node $E_{ik} \propto T_{ihold}$. Increased travel time of ME results in high energy consumption in a node which shortens the network lifetime. In order to investigate the impact of waiting time on energy consumption of a node, we have introduced a term Ratio of Idle time Energy consumption to the Total Energy consumption (%):

$$RIETE = 100 * \frac{IdleTimeEnergyconsumption}{TotalEnergyconsumption} \quad (19)$$

From the above equation $RIETE \propto$ Idle time Energy it indicates that higher Idle time Energy consumption leads to the higher value of RIETE. The algorithm with lower RIETE value is more efficient.

Fig.6 indicates that more than the 60% of the energy spent by a node due to Idle time. From the graphs it is clear that T_{iHold} is the key factor influencing the energy consumption. Even for higher node densities energy consumption is low with HLI, the reason for this is T_{Hold} for HLI is low when compared to CSS.

6 Conclusion

ENI diminishes the TL of ME by limiting the ENs to be covered by ME. The TL so acquired by ENI is additionally abbreviated by deciding an ideal number of Halting Locations to supplant a portion of the ENs by utilizing the HLIT.

Simulations have demonstrated that ENI beats COM by a significant separation for all estimations of T_r and node density.

The HLI significantly decreases TL contrasted with best known algorithm, CSS. ENI, HLI offers desirable QOS in terms of latency and resource utilization.

Bibliography

- [1] Agarwal, A.; Gupta, K.; Yadav, K.P. (2016). A novel energy efficiency protocol for WSN based on optimal chain routing, *2016 3rd International Conference on Computing for Sus-*

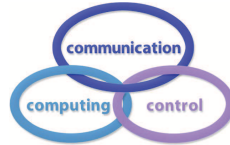
- tainable Global Development (INDIACom)*, IEEE, 368–373, 2016.
- [2] Al-Tabbakh, S.M. (2017). Novel technique for data aggregation in wireless sensor networks, *2017 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, IEEE, 1–8, 2017.
 - [3] Amarlingam, M.; Mishra, P. K.; Rajalakshmi, P.; Giluka, M.K.; Tamma, B.R. (2018). Energy efficient wireless sensor networks utilizing adaptive dictionary in compressed sensing, *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, 383–388, 2018.
 - [4] Begum, B.A.; Satyanarayana, N.V. (2015). Composite interference mapping model for interference fault-free transmission in WSN, *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, IEEE, 2118–2125, 2015.
 - [5] Chaudhari, M.; Koleva, P.; Poulkov, V.; Deshpande, V. (2017). Energy efficient reliable data transmission in resource constrained ad-hoc communication networks, *2017 Global Wireless Summit (GWS)*, IEEE, 17–21, 2017.
 - [6] Chen, T.C.; Chen, T.S.; Wu, P.W. (2008). Data collection in wireless sensor networks assisted by mobile collector, *2008 1st IFIP Wireless Days*, IEEE, 1–5, 2008.
 - [7] Chiu, K.-M.; Liu, J.-S. (2011). Robot routing using clustering-based parallel genetic algorithm with migration, *2011 IEEE Workshop on Merging Fields of Computational Intelligence and Sensor Technology*, IEEE, 42–49, 2011.
 - [8] Cirstea, C.; Davidescu, R.; Jianu, A. (2013). Optimum communication paths for mobile WSNs using genetic algorithms, *2013 36th International Conference on Telecommunications and Signal Processing (TSP)*, IEEE, 299–303, 2013.
 - [9] Devendra Rao, B.V.; Vasumathi, D.; Nandury, S. V. (2015). Exploiting Common Nodes in Overlapped Clusters for Path Optimization in Wireless Sensor Networks, *Proceedings of the Second International Conference on Computer and Communication Technologies: IC3T 2015*, Springer, 3, 209, 2015.
 - [10] Diaz, S.; Mendez, D. (2019). Dynamic minimum spanning tree construction and maintenance for Wireless Sensor Networks, *Revista Facultad de Ingeniería*, 93, 57–69, 2019.
 - [11] He, L.; Pan, J.; Xu, J. (2012). A progressive approach to reducing data collection latency in wireless sensor networks with mobile elements, *IEEE Transactions on Mobile Computing*, IEEE, 12(7), 1308–1320, 2012.
 - [12] He, L.; Xu, J.; Yu, Y.; Li, M.; Zhao, W. (2009). Genetic algorithm based length reduction of a mobile BS path in WSNs, *2009 Eighth IEEE/ACIS International Conference on Computer and Information Science*, IEEE, 797–802, 2009.
 - [13] Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks, *Proceedings of the 33rd annual Hawaii international conference on system sciences*, IEEE, 2, 1–10, 2000.
 - [14] Helsgaun, K. (2000). An effective implementation of the Lin–Kernighan traveling salesman heuristic, *European Journal of Operational Research*, 126(1), 106–130, 2000.
 - [15] Jothikumar, C.; Venkataraman, R. (2019). EODC: An Energy Optimized Dynamic Clustering Protocol for Wireless Sensor Networks using PSO Approach, *International Journal of Computers Communications & Control*, 14(2), 183–198, 2019.

-
- [16] Kakde, K.R.; Kadam, M. (2017) Performance analysis of tree cluster based data gathering for WSNs, *2017 International Conference on Intelligent Computing and Control (I2C2)*, 1–5, 2017.
- [17] Konstantopoulos, C.; Pantziou, G.; Gavalas, D.; Mpitiopoulos, A.; Mamalis, B. (2011). A rendezvous-based approach enabling energy-efficient sensory data collection with mobile sinks, *IEEE Transactions on Parallel and Distributed Systems*, 23, 809–817, 2011.
- [18] Liao, W.-H.; Kuai, S.-C. (2017). An Energy-Efficient SDN-Based Data Collection Strategy for Wireless Sensor Networks, *2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2)*, 91–97, 2017.
- [19] Liao, Y.; Qi, H.; Li, W. (2012). Load-balanced clustering algorithm with distributed self-organization for wireless sensor networks, *IEEE Sensors Journal*, 13, 1498–1506, 2012.
- [20] Liu, J.-S.; Wu, S.-Y.; Chiu, K.-M. (2013). Path planning of a data mule in wireless sensor network using an improved implementation of clustering-based genetic algorithm, *2013 IEEE Symposium on Computational Intelligence in Control and Automation (CICA)*, 30–37, 2013.
- [21] Misbahuddin, M.; Putri Ratna, A.A.; Sari, R.F. (2018). Dynamic Multi-hop Routing Protocol Based on Fuzzy-Firefly Algorithm for Data Similarity Aware Node Clustering in WSNs, *International Journal of Computers Communications & Control*, 13(1), 99-116, 2018.
- [22] Prashanth, J.S.; Nandury, S.V.(2015). Cluster-based rendezvous points selection for reducing tour length of mobile element in WSN, *2015 IEEE International Advance Computing Conference (IACC)*, 1230–1235, 2015.
- [23] Restuccia, F.; Anastasi, G.; Conti, M.; Das, S.K. (2013). Analysis and optimization of a protocol for mobile element discovery in sensor networks, *IEEE Transactions on Mobile Computing*, 13(9),1942–1954, 2013.
- [24] Rubel, M.D.S.I.; Kandil, N.; Hakem, N.; Zuyal, M.D.S.I. (2017). Clustering approach delay sensitive application in wireless sensor network (WSN), *2017 IEEE International Conference on Telecommunications and Photonics (ICTP)*, 82–86, 2017.
- [25] Sen, S.; Chowdhury, C.; Neogy, S. (2016). Design of cluster-chain based WSN for energy efficiency, *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 150–154, 2016.
- [26] Singh, V.K.; Kumar, R.; Sahana, S. (2017). To enhance the reliability and energy efficiency of WSN using new clustering approach, *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 488–493, 2017.
- [27] Venkataraman, G.; Emmanuel, S.; Thambipillai, S. (2005). DASCA: a degree and size based clustering approach for wireless sensor networks, *2005 2nd International Symposium on Wireless Communication Systems*, 508–512, 2005.
- [28] Venkataraman, G.; Emmanuel, S.; Thambipillai, S. (2008). Energy-efficient cluster-based scheme for failure management in sensor networks, *IET communications*, 2(4), 528–537, 2008.
- [29] Vikram, G.R.; Krishna, A.V.N.; Chatrapati, K.S. (2017). Variable initial energy and unequal clustering (VEUC) based multicasting in WSN, *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 82–86, 2017.

- [30] Vinutha, C.B.; Nalini, N.; Veeresh, B.S. (2017). Energy efficient wireless sensor network using neural network based smart sampling and reliable routing protocol, *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2081–2085, 2017.
- [31] Welzl, E. (1991). Smallest enclosing disks (balls and ellipsoids), *New results and new trends in computer science*, 359–370, 1991.
- [32] Xing, G.; Li, Mi.; Wang, T.; Jia, W.; Huang, J. (2011). Efficient rendezvous algorithms for mobility-enabled wireless sensor networks, *IEEE Transactions on Mobile Computing*, 11(1), 47–60, 2011.
- [33] Xing, G.; Wang, T.; Jia, W.; Li, Mi. (2008). Rendezvous design algorithms for wireless sensor networks with a mobile base station, *Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*, 231–240, 2008.
- [34] Xing, G.; Wang, T.; Xie, Z.; Jia, W. (2008). Rendezvous planning in wireless sensor networks with mobile elements, *IEEE Transactions on Mobile Computing*, 7,1430–1443, 2008.
- [35] Xu, Ji.; He, L.; Chen, Z.; Huang, G.; Yuan, T. (2008). Reducing the path length of a mobile BS in WSNs, *2008 International Seminar on Future BioMedical Information Engineering*, 271–274, 2008.
- [36] Xu, R.; Dai, H.; Wang, F.; Jia, Z. (2013). A convex hull based optimization to reduce the data delivery latency of the mobile elements in wireless sensor networks, *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing*, IEEE, 2245–2252, 2013.

Hierarchical Decision-making using a New Mathematical Model based on the Best-worst Method

M.H. Tabatabaei, M. Amiri, M. Ghahremanloo,
M. Keshavarz-Ghorabae, E.K. Zavadskas, J. Antucheviciene



Mohammad Hashemi Tabatabaei

Department of Industrial Management
Faculty of Management and Accounting, Allameh Tabataba'i University, 14348-63111 Tehran, Iran
M.h.tabatabaei@atu.ac.ir, Tabatabaei.mhm@gmail.com

Maghsoud Amiri

Department of Industrial Management
Faculty of Management and Accounting, Allameh Tabataba'i University, 14348-63111 Tehran, Iran
Amiri@atu.ac.ir

Mohammad Ghahremanloo

Department of Management
Faculty of Industrial Engineering and Management, Shahrood University of Technology, 36199-95161 Shahrood, Iran
ghahremanloo@yahoo.com, m.ghahremanloo@shahroodut.ac.ir

Mehdi Keshavarz-Ghorabae

Department of Management
Faculty of Humanities (Azadshahr Branch), Gonbad Kavous University, 49717-99151 Gonbad Kavous, Iran
m.keshavarz@gonbad.ac.ir, m.keshavarz_gh@yahoo.com

Edmundas Kazimieras Zavadskas*

Department of Construction Management and Real Estate
Vilnius Gediminas Technical University, Sauletekio al. 11, LT-10223 Vilnius, Lithuania
*Corresponding author: edmundas.zavadskas@vgtu.lt

Jurgita Antucheviciene

Department of Construction Management and Real Estate
Vilnius Gediminas Technical University, Sauletekio al. 11, LT-10223 Vilnius, Lithuania
jurgita.antucheviciene@vgtu.lt

Abstract: Decision-making processes in different organizations often have a hierarchical and multilevel structure with various criteria and sub-criteria. The application of hierarchical decision-making has been increased in recent years in many different areas. Researchers have used different hierarchical decision-making methods through mathematical modeling. The best-worst method (BWM) is a multi-criteria evaluation methodology based on pairwise comparisons. In this paper, we introduce a new hierarchical BWM (HBWM) which consists of seven steps. In this new approach, the weights of the criteria and sub-criteria are obtained by using a novel integrated mathematical model. To analyze the proposed model, two numerical examples are provided. To show the performance of the introduced approach, a comparison is also made between the results of the HBWM and BWM methodologies. The analysis demonstrates that HBWM can effectively determine the weights of criteria and sub-criteria through an integrated model.

Keywords: decision model, MCDM, best-worst method, hierarchical decision-making, pairwise comparison.

1 Introduction

Often in most decision-making cases, a number of alternatives are ranked and selected according to different criteria; but it's not always a simple task. In various issues of today's complex world, which require correct and timely decisions, we often deal with a hierarchical and multilevel structure with various criteria and sub-criteria, which should be considered in decision making according to their significance [4]. Multi-criteria decision-making (MCDM) approach helps to select appropriate alternatives through mathematical and computational techniques [35]. The need for this category of multi-criteria decisions is felt to solve today management problems [13, 21]. Recently, some researchers have developed MCDM methods, Jiang and Huang [12] introduced a new fuzzy MCDM approach to evaluate the performance of green supply chain management. Xu et al. [41] developed the TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) using Neutrosophic Approach. Also, Ren et al. [24] developed TODIM (an acronym in Portuguese for Interactive MCDM) Method for MADM Problem in Fuzzy Environment.

From a scientific perspective, there are two basic elements to support the hierarchical decision-making process: 1) How to create a hierarchical decision-making model to describe the decision-making process; and 2) Finding the optimal method for calculating the weights of criteria and choosing the alternatives [16]. Various techniques of MCDM have been widely used in the last few years to find solutions for many real-world problems [11]. Interested readers are referred to some review articles that presented and analyzed different MCDM approaches in different fields of real-world decision problems [11, 16]. In 2015, the best-worst method (BWM) was introduced as a new MCDM method. The best and the worst criteria mean the most and the least significant criteria, respectively. After making the comparisons, a Min-Max mathematical programming model was formulated to determine the optimal weights of the criteria. It was also found that the BWM was better than the analytical hierarchy process method because it requires less data, and it's easier to use [26].

In this paper, given the importance of hierarchical decision making, we present an MCDM method based on BWM. In this novel method, an integrated mathematical model is used to calculate weights of criteria and sub-criteria simultaneously. In the original BWM, if we have j criteria and k sub-criteria, we must solve the BWM model $(j + 1)$ times in order to obtain the weights of the criteria and sub-criteria, but in the HBWM, we will obtain the weights of the criteria and sub-criteria in an integrated model based on BWM with running the model once. The HBWM also provides a global weight for each sub-criterion. In addition, the proposed method allows the calculation of the compatibility rate of criteria and sub-criteria for pairwise comparisons.

The remainder of the paper is organized as follows. We describe the hierarchical decisions, development and application of the BWM in Section 2. In Section 3, we present the proposed HBWM methodology along with its steps, integrated mathematical model, variables, and parameters. In Section 4, two numerical examples are provided and the results of the HBWM model are compared with the original BWM model. Finally, we discuss the results and present suggestions for future research in the conclusion section.

2 Literature review

2.1 Hierarchical decision-making

AHP was introduced by [29, 30]. It is a decision-making support tool that can be used to solve complex decision problems. It uses a multi-level hierarchical structure of goals, criteria,

sub-criteria, and alternatives [38]. The analytic network process (ANP) is known as one of the AHP developments, and it structures a decision problem as a network [31]. Many researchers have used these methods to obtain optimal weights of decision-making sub-criteria [5, 23, 36]. In addition, other well-known methods in the MCDM field, such as TOPSIS, VIKOR (in Serbian: VIŠakriterijumska optimizacija i KOmpromisno ReŠenje) and ELECTRE (in French: ELimination Et Choix Traduisant la REalitŠ) methods have also been developed in a multilevel and hierarchical environment [3, 15, 43]. These methods made changes in the original method to obtain the optimum weights of the criteria and sub-criteria and to rank the alternatives. However, in recent years, some researchers have successfully developed new methods for multicriteria decision-making. For example, Rezaei [26] developed a new MCDM method, which had less computation and pairwise comparisons are more consistent than the AHP method, and it was also used in the hierarchical environment [8].

2.2 Developments and applications of BWM

The best-worst methodology was introduced as an efficient MCDM method based on pairwise comparisons. In this method, the best (the most favorable) and the worst (the least favorable) criteria are chosen by decision makers without performing pairwise comparison and the rest of the criteria are compared with them in a pairwise manner, then a max-min problem is formulated and solved to obtain the optimum weight of the criteria [26]. Many researchers have used this method to obtain the optimal weights of decision-making criteria and ranking the alternatives in various real-world decision problems such as supplier selection [2, 8, 28], calculating the efficiency [9, 33], sustainability study [25, 40] performance evaluation [42, 44, 45], web service selection [34] and power source evaluation [39]. Meanwhile, other researchers developed the BWM and added new capabilities to its basic model. Rezaei [27] added new features to the model; he introduced a linear mathematical programming model that yielded a unique solution.

Mou et al. [20] presented a new BWM-based group decision-making model in uncertain conditions and used it to solve health management problems. Guo et al. [6] presented the BWM model in a fuzzy environment using a nonlinear mathematical model, and used real-world case studies to describe the model. Hafezalkotob & Hafezalkotob [10] discussed and evaluated the fuzzy BWM model in group decision-making that used two linear programming models. In their approach, the final decision was made based on composition of decisions of senior decision-makers and experts. Also, Aboutorab et al. [1] presented the Z-number version of the BWM under the condition of uncertain input data and solved the supplier selection problem in the form of a case study by using the mentioned methodology. Safarzadeh et al. [32] used a new BWM model with two new mathematical models in group decision-making and evaluated the new model using numerical examples and the real-world case studies. Tabatabaei et al. [37] developed the BWM model in the form of group decision making. This method is applicable when a decision-group, including a manager and several experts, is required to evaluate several options or criteria.

Pamucar et al. [22] proposed a new integrated model based on the interval rough numbers (IRN), BWM, Weighted Aggregates Sum Product Assessment (WASPAS) and Multi-Attributive Border Approximation area Comparison (MABAC) to evaluate third-party logistics (3PL) providers. In another study, the fuzzy BWM was used as a MCDM methodology to prepare the strategy of a manufacturing company in Iran. The proposed method provided a new approach to determine weight vector from matrices of the fuzzy pairwise comparisons. For this purpose, a nonlinear optimization model was developed [14]. A group hierarchical decision-making algorithm was introduced by Maghsoodi et al. [17] based on the principles of Axiomatic design and the BWM in a fuzzy environment, then a case study about selecting the conceptual design of a speaker prototype was examined using the proposed method.

Table 1: Notations and their descriptions

Type	Notation	Description
Sets	$j \in C = \{1, 2, \dots, n\}$	Criterion
Sets	$k \in C_k = \{1, 2, \dots, m\}$	Sub-criterion
Parameters	a_{Bj}	Priority of the best criterion over j -th criterion
Parameters	a_{jW}	Priority of j -th criterion over the worst criterion
Parameters	a_{Bk}^j	Priority of the best sub-criterion over k -th sub-criterion for j -th criterion
Parameters	a_{kW}^j	Priority of k -th sub-criterion over the worst sub-criterion for j -th criterion
Variables	w_B	Weight of the best criterion
Variables	w_j	Weight of j -th criterion
Variables	w_W	Weight of the worst criterion
Variables	w_B^j	Weight of the best sub-criterion for j -th criterion
Variables	w_k^j	Weight of k -th sub-criterion for j -th criterion
Variables	w_W^j	Weight of worst sub-criterion for j -th criterion
Variables	Gw_k^j	Global weight of k -th sub-criterion for j -th criterion

In this paper, considering the basic model of the BWM and its details, and considering the need for decision making in the hierarchical and multilevel conditions, we introduce a multi-criteria hierarchical best-worth method (HBWM) with an integrated non-linear mathematical model. In the next section, details of the HBWM are described. In order to evaluate the new model, two numerical examples, which previously solved by a simple BWM model in hierarchical conditions and by involvement of sub criteria, will be examined by the new model and the results will be compared. The advantages of the new HBWM model are as follows:

- Reducing the number of repetitions of basic BWM model for hierarchical decisions from $(j + 1)$ to one, where j represents the number of criteria.
- Calculating the weights of criteria, sub-criteria as well as the global weight in an integrated mathematical model.
- Possibility to calculate the consistency rate for comparisons performed for criteria and sub-criteria only by solving the model once.

3 The HBWM

In decision-making, determining some sub-criteria along with main criteria is essential for assessment of alternatives. It can be helpful to provide a model that has the ability to involve sub-criteria in decision-making and requires less data and information to make decisions while preserving the benefits of previous approaches. The model developed in this study which is based on the BWM for hierarchical decision making, can be used as an efficient tool by researchers and managers in various organizations. The proposed model allows the calculation of consistency rate of the decisions made based on pairwise comparisons performed for criteria and sub-criteria.

3.1 Proposed model

In the proposed model, a "global weight" is calculated by combining the weights of all sub-criteria of the decision-making problem. The notations and their descriptions are presented in Table 1.

The procedure of the HBWM are as follows:

Step 1. Identifying the decision criteria and sub-criteria: In this step, the decision criteria and sub-criteria are defined as $\{c_1, c_2, \dots, c_n\}$ and $\{c_{1k}, c_{2k}, \dots, c_{nk}\}$ respectively.

Step 2. Identifying the best (most important, most desirable) and the worst (least important, least desirable) criteria and sub-criteria: the best and the worst criteria and sub-criteria are selected. No comparison will be made at this step.

Step 3. At this step, the priority of the best criterion over each of other criteria is determined as a number between 1 and 9, which is expressed as $A_B = (a_{B1}, a_{B2}, \dots, a_{Bn})$ where a_{Bi} is the priority of the best criterion over i -th criterion and $a_{BB} = 1$, Eq. (2).

Step 4. At this step, the priority of each criterion over the worst criterion is determined as a number between 1 and 9, which is expressed as $A_W = (a_{1W}, a_{2W}, \dots, a_{nW})$, where a_{jW} is the priority of j -th criterion over the worst criterion and $a_{WW} = 1$, Eq. (3).

Step 5. At this step, the priority of the best sub-criterion over each of other sub-criterion is determined as a number between 1 and 9, which is expressed as $A_B = (a_{B1}^j, a_{B2}^j, \dots, a_{Bk}^j)$, where a_{Bk}^j is the priority of the best sub-criterion over k -th sub-criterion in j -th criterion and $a_{BB}^j = 1$, Eq. (4).

Step 6. At this step, the priority of each sub-criterion over the worst sub-criterion is determined for each criterion as a number between 1 and 9, which is expressed as $A_B = (a_{1W}^j, a_{2W}^j, \dots, a_{kW}^j)$, where a_{kW}^j is the priority of k -th sub-criterion over the worst sub-criterion for j -th criterion and $a_{WW}^j = 1$, Eq. (5).

Step 7. Calculating the weights of the criteria $(w_1^*, w_2^*, \dots, w_n^*)$ and sub-criteria $(w_1^{j*}, w_2^{j*}, \dots, w_k^{j*})$.

Eq.(1) is the objective function of the model and yields the minimum deviations of the comparisons made for the criteria and sub-criteria.

Eq.(6) calculates the global weights of the sub-criteria.

Eq.(7) shows that sum of the criteria weights must be equal to 1 and the weight of each criterion must be non-negative.

Eq.(8) shows that sum of the weights of sub-criteria of the j -th criteria must be equal to 1 and the weight of each sub-criterion must be non-negative.

We can write the model of HBWM as follows, Eqs. (1) to (8):

$$\text{Min } \xi^L + \sum_j \xi_j^L \quad (1)$$

$$|w_B - a_{Bj}w_j| \leq \xi^L, \forall j \quad (2)$$

$$|w_j - a_{jW}w_W| \leq \xi_j^L, \forall j \quad (3)$$

$$|w_B^j - a_{Bk}^j w_k^j| \leq \xi_j^L, \forall j \ \& \ \forall k \quad (4)$$

$$|w_k^j - a_{kW}^j w_W^j| \leq \xi_j^L, \forall j \ \& \ \forall k \quad (5)$$

$$Gw_k^j = w_j w_k^j, \forall k \quad (6)$$

$$\sum_j w_j = 1, w_j \geq 0 \quad (7)$$

$$\sum_k w_k^j = 1, w_k^j \geq 0 \quad (8)$$

The HBWM includes seven steps, as shown in Fig. 1.

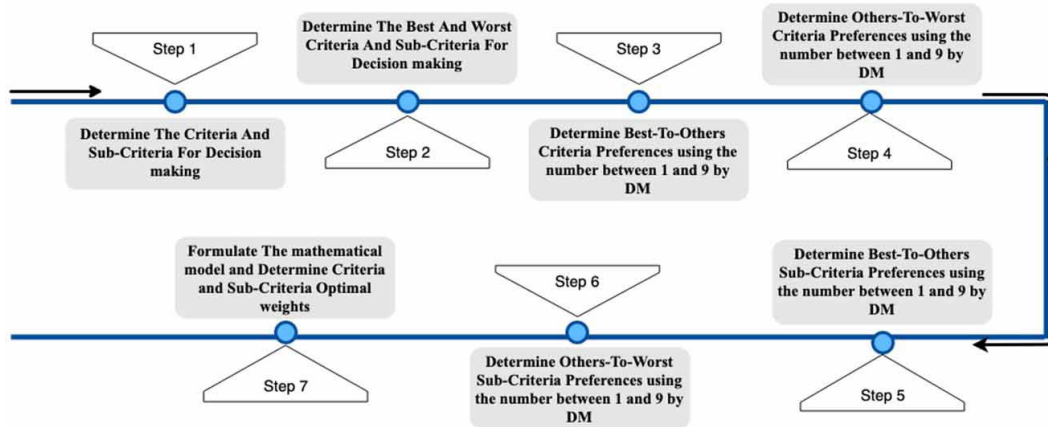


Figure 1: Decision-making process in HBWM

3.2 Calculating the consistency rate

Given that in the HBWM ξ^L of comparisons performed for the criteria and ξ_j^L of comparisons performed for the sub-criteria of each criteria are determined separately by the model, and the results are calculated in a similar way to the basic BWM, the consistency index provided for the basic BWM can be used to calculate the consistency rate of the comparisons performed for the criteria and sub-criteria. The consistency rate in the BWM is obtained with respect to the value of the priority of the best criterion over the worst criterion and the priority of the best sub-criterion over the worst sub-criterion of j -th criterion. its values are shown in Table 2 [26].

Table 2: Consistency index in BWM

a_{BW}, a_{BW}^j	1	2	3	4	5	6	7	8	9
Consistency Index (Max ξ)	0.00	0.44	1.00	1.63	2.30	3.00	3.73	4.47	5.23

Given the minimum deviations of the comparisons performed for the criteria (ξ^*) and the sub-criteria of each criterion (ξ_j^*) which are calculated through the BWM, and the inconsistency rate provided in Table 2, we can calculate the consistency rate for the criteria and sub-criteria of each criterion using Eqs. (9) and (10).

$$\text{Consistency rate} = \frac{\xi^*}{\text{Consistency index}} \quad (9)$$

$$\text{Consistency rate} = \frac{\xi_j^*}{\text{Consistency index}} \quad (10)$$

4 Numerical examples

Several authors have tried in their papers to measure the weights of criteria and sub-criteria in decision making using the BWM. We can show that it is possible to calculate the weights of criteria and sub-criteria in a single integrated hierarchical decision making model and achieve the same results as the best-worst method. For this purpose, we use the criteria and sub-criteria and the questionnaire data provided in two previously done studies and compare the results of the basic model and the proposed HBWM.

4.1 Example 1

In reference [7] Gupta and Barua, a study was conducted to identify important factors of technological innovations in the field of MSME (Micro-Small and Medium Enterprises) in India. The authors used the research literature and experts' judgments to identify the factors of technological innovation. They calculated the optimum weights of the criteria and sub-criteria using the basic model of the BWM.

In the first numerical example, the criteria and sub-criteria and their study information are examined using the new model (HBWM) and the new model is evaluated by comparing the results. Evaluation criteria are shown in Figure 2.

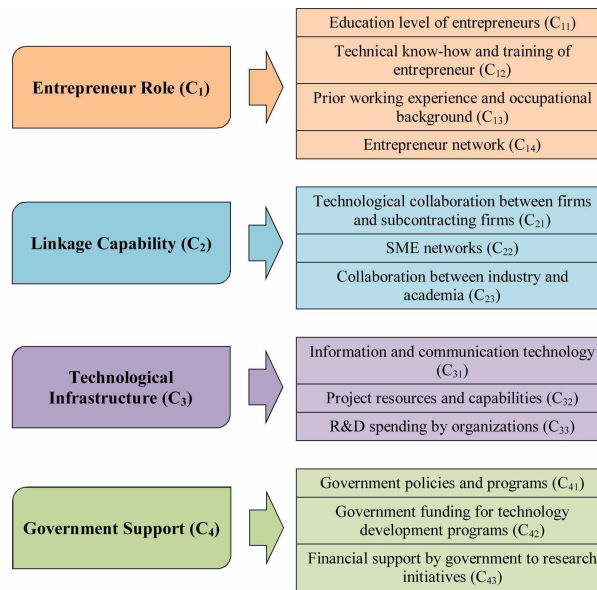


Figure 2: Main criteria and sub-criteria for Example 1

In Example 1, criteria and sub-criteria and questionnaire data provided in the study of Gupta and Barua [7] have been used. In their paper, they tried to identify significant factors of technological innovation. Table 3 represents BWM questionnaire data obtained by them and the pairwise comparisons of criteria and sub-criteria including best-to-others(BO) and others-to-worst(OW).

Table 3: The comparisons for the criteria and sub-criteria in Example 1

Criteria	BO	OW	Sub-criteria	BO	OW	Sub-criteria	BO	OW
C_1	2	4	C_{11}	8	1	C_{21}	1	6
C_2	5	1	C_{12}	1	8	C_{22}	6	1
C_3	1	5	C_{13}	3	2	C_{23}	3	2
C_4	3	2	C_{14}	2	3			
Sub-criteria	BO	OW	Sub-criteria	BO	OW			
C_{31}	5	1	C_{41}	1	8			
C_{32}	1	5	C_{42}	3	4			
C_{33}	4	2	C_{43}	8	1			

Table 4 shows the results of basic BWM and HBWM for the first numerical example. The results show that the weights obtained for criteria and sub-criteria by HBWM are same as the

weights obtained by BWM. In the study of Gupta and Barua [7], the basic BWM was solved $(j+1)$ times to obtain the weights of criteria and sub-criteria; however, in the proposed approach, weights are obtained by solving the integrated model of HBWM only one time. Table 5 represents the values of ξ^L and ξ_j^L for criteria and sub-criteria in Example 1.

Table 4: Local weights(LW) and Global weights(GW) for Example1

	LW of Basic BWM	LW of HBWM	GW of Basic BWM	GW of HBWM
C_1	0.267	0.267	–	–
C_2	0.082	0.082	–	–
C_3	0.473	0.473	–	–
C_4	0.178	0.178	–	–
C_{11}	0.069	0.069	0.018	0.018
C_{12}	0.517	0.517	0.138	0.138
C_{13}	0.172	0.172	0.046	0.046
C_{14}	0.241	0.241	0.064	0.064
C_{21}	0.667	0.667	0.055	0.055
C_{22}	0.111	0.111	0.009	0.009
C_{23}	0.222	0.222	0.018	0.018
C_{31}	0.125	0.125	0.059	0.059
C_{32}	0.687	0.687	0.325	0.325
C_{33}	0.188	0.188	0.089	0.089
C_{41}	0.667	0.667	0.120	0.120
C_{42}	0.246	0.246	0.044	0.044
C_{43}	0.077	0.077	0.014	0.014

Table 5: The values of ξ^L and ξ_j^L for criteria and sub-criteria in Example 1

Comparisons	Basic BWM	HBWM
C_1, C_2, C_3, C_4	0.061	0.061
$C_{11}, C_{12}, C_{13}, C_{14}$	0.034	0.034
C_{21}, C_{22}, C_{23}	0	0
C_{31}, C_{32}, C_{33}	0.062	0.062
C_{41}, C_{42}, C_{43}	0.061	0.061

4.2 Example 2

In the study of Gupta and Barua [8], supplier selection in SMEs was investigated based on the green innovation criteria. They first selected the green innovation criteria by reviewing the related literature and interviewing with decision makers, then determined the weights of criteria and sub-criteria using basic BWM, and finally ranked the alternatives using the fuzzy TOPSIS method. In the second numerical example, the results of their study are examined and compared with the HBWM model to evaluate the performance of the new model. The criteria and sub-criteria are shown in Figure 3.

In Example 2, criteria and sub-criteria and questionnaire data provided in the study of Gupta and Barua [8] are used. In their paper, they tried to identify significant factors of green innovation. Table 6 represents BWM questionnaire data obtained by them and the pairwise comparisons of criteria and sub-criteria including BO and OW.

Table 6: The comparisons for the criteria and sub-criteria in Example 2

Criteria	BO	OW	Sub-criteria	BO	OW	Sub-criteria	BO	OW
C_1	8	2	C_{11}	4	2	C_{21}	8	1
C_2	2	4	C_{12}	3	3	C_{22}	2	4
C_3	1	9	C_{13}	2	4	C_{23}	1	8
C_4	9	1	C_{14}	1	9	C_{24}	4	2
C_5	3	3	C_{15}	7	2	C_{25}	3	3
C_6	6	2	C_{16}	9	1	C_{26}	4	3
C_7	2	5						
Sub-criteria	BO	OW	Sub-criteria	BO	OW	Sub-criteria	BO	OW
C_{31}	8	2	C_{41}	8	1	C_{51}	2	4
C_{32}	9	1	C_{42}	2	4	C_{52}	5	2
C_{33}	6	2	C_{43}	1	8	C_{53}	1	9
C_{34}	6	2	C_{44}	3	3	C_{54}	3	3
C_{35}	1	9	C_{45}	6	2	C_{55}	9	1
C_{36}	2	4						
C_{37}	4	2						
Sub-criteria	BO	OW	Sub-criteria	BO	OW			
C_{61}	8	9	C_{71}	9	1			
C_{62}	1	2	C_{72}	1	9			
C_{63}	2	4	C_{73}	5	2			
C_{64}	4	3	C_{74}	2	4			
C_{65}	5	2	C_{75}	3	3			
C_{66}	9	1	C_{76}	4	2			
C_{67}	7	2						

Table 7 shows the results of basic BWM and HBWM for the second numerical example. The results show that the weights obtained for criteria and sub-criteria by HBWM are same as the weights obtained by BWM, while the advantage of HBWM is that it formulates and calculates all necessary parameters in a single integrated model. Also, by comparing the values of ξ^L and ξ_j^L in both methods as shown in Table 8, no difference is observed between these values. Comparing the results, it is observed that the weights for criteria and sub-criteria are not different, but HBWM obtained the results by solving an integrated model while Gupta and Barua [8] solved 8 times the basic BWM to obtain the results. Also, in HBWM there is no need to manually calculate the global weight because it is provided by the model itself.

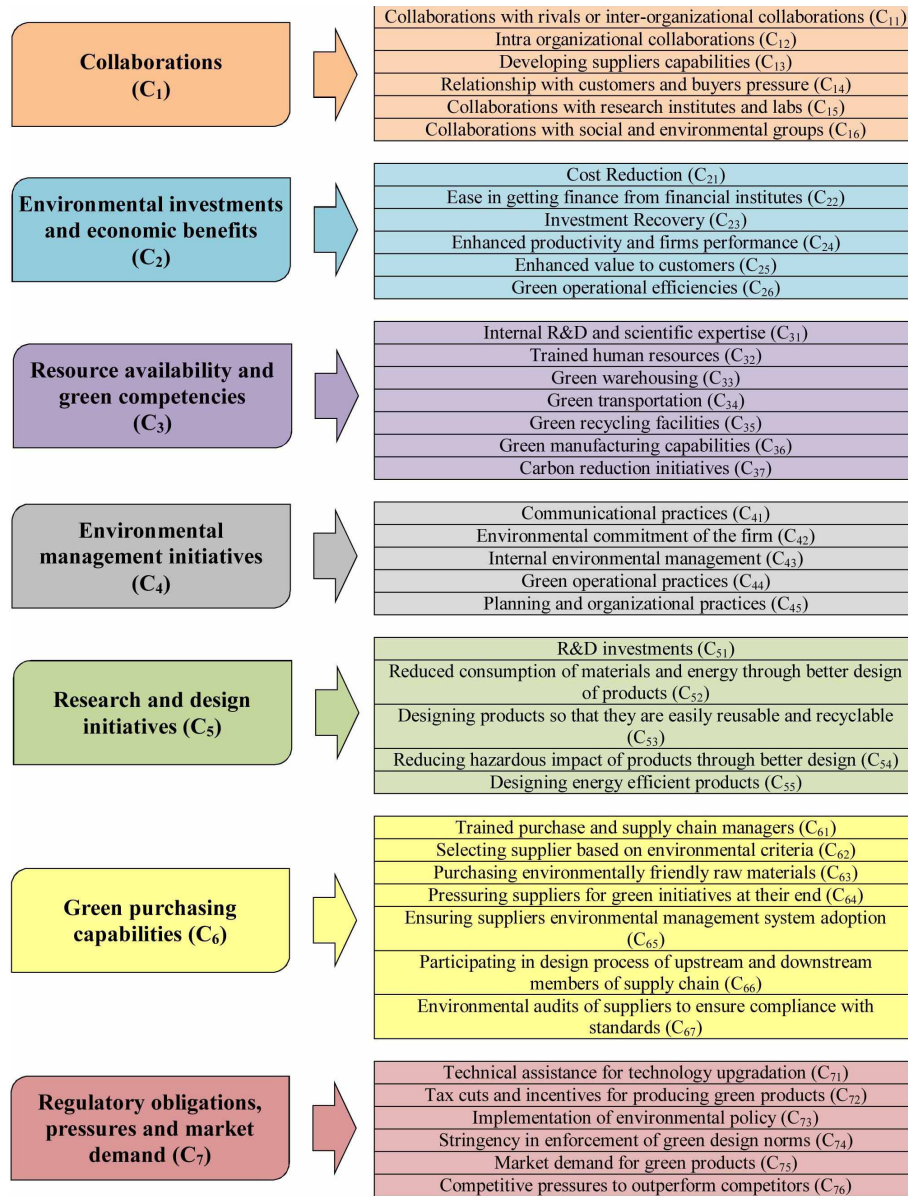


Figure 3: Main criteria and sub-criteria for Example 2

Table 7: Local weights(LW) and Global weights(GW) for Example2

	LW of Basic BWM	LW of HBWM	GW of Basic BWM	GW of HBWM
C_1	0.048	0.048	–	–
C_2	0.173	0.173	–	–
C_3	0.358	0.358	–	–
C_4	0.037	0.037	–	–
C_5	0.128	0.128	–	–
C_6	0.064	0.064	–	–
C_7	0.192	0.192	–	–
C_{11}	0.113	0.113	0.005	0.005
C_{12}	0.150	0.150	0.007	0.007
C_{13}	0.203	0.203	0.010	0.010
C_{14}	0.426	0.426	0.020	0.020
C_{15}	0.064	0.064	0.003	0.003
C_{16}	0.045	0.045	0.002	0.002
C_{21}	0.045	0.045	0.008	0.008
C_{22}	0.211	0.211	0.037	0.037
C_{23}	0.392	0.392	0.068	0.068
C_{24}	0.106	0.106	0.018	0.018
C_{25}	0.141	0.141	0.024	0.024
C_{26}	0.106	0.106	0.018	0.018
C_{31}	0.057	0.057	0.020	0.020
C_{32}	0.044	0.044	0.016	0.016
C_{33}	0.076	0.076	0.027	0.027
C_{34}	0.076	0.076	0.027	0.027
C_{35}	0.426	0.426	0.153	0.153
C_{36}	0.206	0.206	0.074	0.074
C_{37}	0.114	0.114	0.041	0.041
C_{41}	0.054	0.054	0.002	0.002
C_{42}	0.243	0.243	0.009	0.009
C_{43}	0.459	0.459	0.017	0.017
C_{44}	0.162	0.162	0.006	0.006
C_{45}	0.081	0.081	0.003	0.003
C_{51}	0.226	0.226	0.029	0.029
C_{52}	0.096	0.096	0.012	0.012
C_{53}	0.465	0.465	0.059	0.059
C_{54}	0.160	0.160	0.020	0.020
C_{55}	0.053	0.053	0.007	0.007
C_{61}	0.057	0.057	0.004	0.004
C_{62}	0.424	0.424	0.027	0.027
C_{63}	0.206	0.206	0.013	0.013
C_{64}	0.114	0.114	0.007	0.007
C_{65}	0.091	0.091	0.006	0.006
C_{66}	0.044	0.044	0.003	0.003
C_{67}	0.065	0.065	0.004	0.004
C_{71}	0.047	0.047	0.009	0.009
C_{72}	0.416	0.416	0.080	0.080
C_{73}	0.086	0.086	0.016	0.016
C_{74}	0.201	0.201	0.039	0.039
C_{75}	0.143	0.143	0.027	0.027
C_{76}	0.107	0.107	0.020	0.020

Table 8: The values of ξ^L and ξ_j^L for criteria and sub-criteria in Example 2

Comparisons	Basic BWM	HBWM
$C_1, C_2, C_3, C_4, C_5, C_6, C_7$	0.026	0.026
$C_{11}, C_{12}, C_{13}, C_{14}, C_{15}, C_{16}$	0.025	0.025
$C_{21}, C_{22}, C_{23}, C_{24}, C_{25}, C_{26}$	0.030	0.030
$C_{31}, C_{32}, C_{33}, C_{34}, C_{35}, C_{36}, C_{37}$	0.031	0.031
$C_{41}, C_{42}, C_{43}, C_{44}, C_{45}$	0.027	0.027
$C_{51}, C_{52}, C_{53}, C_{54}, C_{55}$	0.013	0.013
$C_{61}, C_{62}, C_{63}, C_{64}, C_{65}, C_{66}, C_{67}$	0.031	0.031
$C_{71}, C_{72}, C_{73}, C_{74}, C_{75}, C_{76}$	0.012	0.012

5 Conclusion

In this paper, we introduced a new hierarchical MCDM method called HBWM based on the basic BWM. The BWM calculates the weights based on pairwise comparisons of the alternatives with the best and the worst options and achieves consistent results. In this paper, this approach is extended for a situation in which the decision process involves criteria and sub-criteria for evaluating or selecting the alternatives. In order to show that the weights obtained by HBWM are as optimal as the weights obtained in BWM, we used data from two papers that used the basic BWM to obtain the weights of the criteria and sub-criteria. BWM uses $(j + 1)$ repetitions (where j represents the number of the criteria) to obtain the optimal weights of the criteria and sub-criteria, while the HBWM calculates the weights by an integrated model without repetitions. Also, in HBWM there is no need to manually calculate the global weight because it is provided by the model itself. The results of this paper show that HBWM can be useful for situations that require the simultaneous evaluation of criteria and sub-criteria. The proposed method can be used in combination with other MCDM methods or solely. Also this method can be extended to examine the cases in which there are relationships between sub-criteria of two different criteria.

Author contributions. Conflict of interest

The authors contributed equally to this work. The authors declare no conflict of interest.

Bibliography

- [1] Aboutorab, H., Saberi, M., Asadabadi, M.R., Hussain, O., Chang, E. (2018). ZBWM: The Z-number extension of Best Worst Method and its application for supplier development, *Expert Systems with Applications*, 107, 115-125, 2018.
- [2] Badi, I.; Ballem, M. (2018). Supplier selection using the rough BWM-MAIRCA model: A case study in pharmaceutical supplying in Libya, *Decision Making: Applications in Management and Engineering*, 1(2), 16-33, 2018.
- [3] Baky, I.A. (2014). Interactive TOPSIS algorithms for solving multi-level non-linear multi-objective decision-making problems, *Applied Mathematical Modelling*, 38(4), 1417-1433, 2014.
- [4] Ecer, F. (2018). Third-party logistics (3PLs) provider selection via Fuzzy AHP and EDAS integrated model, *Technological and Economic Development of Economy*, 24(2), 615-634, 2018.
- [5] Farias, L.M.S.; Santos, L.C.; Gohr, C.F.; Rocha, L.O. (2019). An ANP-based approach for lean and green performance assessment, *Resources, Conservation and Recycling*, 143, 77-89, 2019.
- [6] Guo, S.; Zhao, H. (2017). Fuzzy best-worst multi-criteria decision-making method and its applications, *Knowledge-Based Systems*, 121, 23-31, 2017.
- [7] Gupta, H.; Barua, M.K. (2016). Identifying enablers of technological innovation for Indian MSMEs using best-worst multi criteria decision making method, *Technological Forecasting and Social Change*, 107, 69-79, 2016.

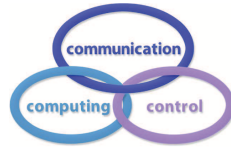
-
- [8] Gupta, H.; Barua, M.K. (2017). Supplier selection among SMEs on the basis of their green innovation ability using BWM and fuzzy TOPSIS, *Journal of Cleaner Production*, 152, 242-258, 2017.
- [9] Gupta, P.; Anand, S.; Gupta, H. (2017). Developing a roadmap to overcome barriers to energy efficiency in buildings using best worst method, *Sustainable Cities and Society*, 31, 244-259, 2017.
- [10] Hafezalkotob, A.; Hafezalkotob, A. (2017). A novel approach for combination of individual and group decisions based on fuzzy best-worst method, *Applied Soft Computing*, 59, 316-325, 2017.
- [11] Ilieva, G.; Yankova, T.; Klisarova-Belcheva, S. (2018). Decision analysis with classic and fuzzy EDAS modifications, *Computational and Applied Mathematics*, 37(5), 5650-5680, 2017.
- [12] Jiang, W.; Huang, C. (2018). A multi-criteria decision-making model for evaluating suppliers in green SCM, *International Journal of Computers Communications & Control*, 13(3), 337-352, 2018.
- [13] Khan, M.S.A. (2019). The Pythagorean fuzzy Einstein Choquet integral operators and their application in group decision making, *Computational and Applied Mathematics*, 38(3), 128, 2019.
- [14] Khanmohammadi, E.; Zandieh, M. (2018). Drawing a Strategy Canvas Using the Fuzzy Best-Worst Method, *Global Journal of Flexible Systems Management*, 20(1), 57-75, 2018.
- [15] Lei, L.; Zhang, W.F. (2013). Extended VIKOR method for multi-level hybrid multi-attribute group decision making, *25th Chinese Control & Decision Conference(CCDC)*, 1718-1722, 2013.
- [16] Lu, J.; Han, J.; Hu, Y.; Zhang, G. (2016). Multilevel decision-making: A survey, *Information Sciences*, 346, 463-487, 2016.
- [17] Maghsoodi, A.I.; Mosavat, M.; Hafezalkotob, A.; Hafezalkotob, A. (2019). Hybrid hierarchical fuzzy group decision-making based on information axioms and BWM: Prototype design selection, *Computers & Industrial Engineering*, 127, 788-804, 2019.
- [18] Mardani, A.; Jusoh, A.; Nor, K.; Khalifah, Z.; Zakwan, N.; Valipour, A. (2015). Multiple criteria decision-making techniques and their applications-a review of the literature from 2000 to 2014., *Economic Research-Ekonomika IstraŽivanja*, 28(1), 516-571, 2015.
- [19] Mardani, A.; Jusoh, A.; Zavadskas, E.K. (2015). Fuzzy multiple criteria decision-making techniques and applications-Two decades review from 1994 to 2014, *Expert Systems with Applications*, 42(8), 4126-4148, 2015.
- [20] Mou, Q.; Xu, Z.; Liao, H. (2016). An intuitionistic fuzzy multiplicative best-worst method for multi-criteria group decision making, *Information Sciences*, 374, 224-239, 2016.
- [21] Naz, S.; Akram, M. (2019). Novel decision-making approach based on hesitant fuzzy sets and graph theory, *Computational and Applied Mathematics*, 38(1), 7, 2019.
- [22] Pamucar, D.; Chatterjee, K.; Zavadskas, E.K. (2019). Assessment of third-party logistics provider using multi-criteria decision-making approach based on interval rough numbers, *Computers & Industrial Engineering*, 127, 383-407, 2019.

- [23] Patriarca, R.; Di Gravio, G.; Costantino, F.; Falegnami, A.; Bilotta, F. (2018). An Analytic Framework to Assess Organizational Resilience, *Safety and Health at Work*, 9(3), 265-276, 2018.
- [24] Ren, H.; Liu, M.; Zhou, H. (2019). Extended TODIM method for MADM problem under trapezoidal intuitionistic fuzzy environment, *International Journal of Computers Communications & Control*, 14(2), 220-232, 2019.
- [25] Ren, J.; Liang, H.; Chan, F.T.S. (2017). Urban sewage sludge, sustainability, and transition for Eco-City: Multi-criteria sustainability assessment of technologies based on best-worst method, *Technological Forecasting and Social Change*, 116, 29-39, 2017.
- [26] Rezaei, J. (2015). Best-worst multi-criteria decision-making method, *Omega*, 53, 49-57, 2015.
- [27] Rezaei, J. (2016). Best-worst multi-criteria decision-making method: Some properties and a linear model, *Omega*, 64, 126-130, 2016.
- [28] Rezaei, J.; Wang, J.; Tavasszy, L. (2015). Linking supplier development to supplier segmentation using Best-Worst Method, *Expert Systems with Applications*, 42(23), 9152-9164, 2015.
- [29] Saaty, T.L. (1977). A scaling method for priorities in hierarchical structure, *Journal of Mathematical Psychology*, 15(3), 234-281, 1977.
- [30] Saaty, T.L. (1990). How to make a decision: the analytic hierarchy process, *European Journal of Operational Research*, 48(1), 9-26, 1990.
- [31] Saaty, T.L.; Takizawa, M. (1986). Dependence and independence: From linear hierarchies to nonlinear networks, *European Journal of Operational Research*, 26(2), 229-237, 1986.
- [32] Safarzadeh, S.; Khansefid, S.; Rasti-barzoki, M. (2018). A group multi-criteria decision-making based on best-worst method, *Computers & Industrial Engineering*, 126, 111-121, 2018.
- [33] Salimi, N., Rezaei, J. (2016). Measuring efficiency of university-industry Ph. D. projects using best worst method, *Scientometrics*, 109(3), 1-28, 2016.
- [34] Serrai, W.; Abdelli, A.; Mokdad, L.; Hammal, Y. (2017). Towards an efficient and a more accurate web service selection using MCDM methods, *Journal of Computational Science*, 22, 253-267, 2017.
- [35] Sharaf, I.M. (2018). TOPSIS with similarity measure for MADM applied to network selection, *Computational and Applied Mathematics*, 37(4), 4104-4121, 2018.
- [36] Sitorus, F.; Cilliers, J.J.; Brito-Parada, P.R. (2018). Multi-Criteria Decision Making for the Choice Problem in Mining and Mineral Processing: Applications and Trends, *Expert Systems with Applications*, 121, 393-417, 2018.
- [37] Tabatabaei, M.H.; Amiri, M.; Khatami Firouzabadi, S.M.A.; Ghahremanloo, M.; Keshavarz-Ghorabae, M.; Saparauskas, J. (2019). A new group decision-making model based on bwm and its application to managerial problems, *Transformations in Business and Economics*, 18(2), 197-214, 2019.

- [38] Triantaphyllou, E.; Mann, S.H. (1995). Using the Analytic Hierarchy Process for Decision Making in Engineering Applications: Some Challenges, *International Journal of Industrial Engineering: Applications and Practice*, 2(1), 35-44, 1995.
- [39] Van De Kaa, G.; Scholten, D.; Rezaei, J.; Milchram, C. (2017). The battle between battery and fuel cell powered electric vehicles: A BWM approach, *Energies*, 10(11), 1707, 2017.
- [40] Wei, G.; Wang, J. (2017). A comparative study of robust efficiency analysis and Data Envelopment Analysis with imprecise data, *Expert Systems with Applications*, 81, 28-38, 2017.
- [41] Xu, G.; Wang, S.; Yang, T.; Jiang, W. (2018). A neutrosophic approach based on TOPSIS method to image segmentation, *International Journal of Computers Communications & Control*, 13(6), 1047-1061, 2018.
- [42] You, P.; Guo, S.; Zhao, H.; Zhao, H. (2017). Operation performance evaluation of power grid enterprise using a hybrid BWM-TOPSIS method, *Sustainability*, 9(12), 2329, 2017.
- [43] Zak, J.; Kruszynski, M. (2015). Application of AHP and ELECTRE III/IV methods to multiple level, multiple criteria evaluation of urban transportation projects, *Transportation Research Procedia*, 10, 820-830, 2015.
- [44] Zhao, H.; Guo, S.; Zhao, H. (2018). Comprehensive performance assessment on various battery energy storage systems, *Energies*, 11(10), 2841, 2018.
- [45] Zhao, H.; Zhao, H.; Guo, S. (2018). Comprehensive Performance Evaluation of Electricity Grid Corporations Employing a Novel MCDM Model, *Sustainability*, 10(7), 2130, 2018.

Wearable System for Daily Activity Recognition Using Inertial and Pressure Sensors of a Smart Band and Smart Shoes

P.H. Truong, S. You, S.-H. Ji, G.-M. Jeong



Phuc Huu Truong

Korean Institute of Industrial Technology, Korea
phtruong@kitech.re.kr

Sujeong You

Korean Institute of Industrial Technology, Korea
sjyou21@kitech.re.kr

Sang-Hoon Ji

Korean Institute of Industrial Technology, Korea
robot91@kitech.re.kr

Gu-Min Jeong*

School of Electrical Engineering, Kookmin University, Jeongneung-dong, Seongbuk-gu, 02707 Korea
*Corresponding author: gm1004@kookmin.ac.kr

Abstract: Human Activity Recognition (HAR) is a challenging task in the field of human-related signal processing. Owing to the development of wearable sensing technology, an emerging research approach in HAR is to identify user-performed tasks by using data collected from wearable sensors. In this paper, we propose a novel system for monitoring and recognizing daily living activities using an off-the-shelf smart band and two smart shoes. The system aims at providing a useful tool for solving problems regarding body part placement, fusion of multimodal sensors and feature selection for a specific set of activities. The system collects inertial and plantar pressure data at wrist and foot to analyze and then, extract, select important features for recognition. We construct and compare two predictive models of classifying activities from the reduced feature set. A comparison of the classification for each wearable device and a fusion scheme is provided to identify the best body part for activity recognition: either the wrist or the feet. This comparison also demonstrated the effective HAR performance of the proposed system.

Keywords: Human Activity Recognition (HAR); Daily Activity Recognition (DAR); Daily Living Activity (DLA); Feature Selection; Smart-Band; Smart-Shoes.

1 Introduction

Human Activity Recognition (HAR) is an emerging research area in human-machine interaction [5, 16, 19]. HAR is also an essential aspect of other fields, especially localization [21, 26], health monitoring [28], medical diagnostics and rehabilitation [14, 33]. HAR has challenges that are common with those in other recognition areas, such as face recognition and speech recognition. Some of these challenges include the determination of which attributes to measure, the design of feature-extraction algorithms, and the development of efficient computational techniques. Nevertheless, HAR exhibits higher complexity because human activities are more various to formulate

its structure compared with face or speech. Additionally, HAR requires different sensing systems for different applications. The recognition of some certain periodic activities, such as walking, is clear [20,37]. However, the recognition of other activities is challenged because people performs a lot of activities a day. Moreover, people occasionally perform many activities at the same time.

Recently, the development of sensor technologies, especially wearable sensors, has advanced numerous design for activity recognition [4,8,18,22]. Wang et al. [35] used a single waist-worn tri-axial accelerometer to recognize six activities based on a hidden Markov model. Banos et al. [2] presented a mobile system based on wearable inertial and electromyography sensors to measure trunk postures and muscle signals. Their evaluation proved that the system can be acceptable for use in measuring trunk endurance. Laudanski et al. [17] mounted two inertial measurement units (IMU) consisting of accelerometer and gyroscope sensors onto user's shanks to classify gait activities. After deriving frequency features, a k-nearest neighbor (KNN) algorithm was used to classify the activities. Najafi et al. [23] developed an ambulatory system using accelerometer and gyroscope sensors, and attached it onto human chest to recognize daily activities. Storm et al. [32] utilized commercial instruments to examine step detection and HAR using triaxial accelerometers. In their study, HAR was performed using a DynaPort move-monitor worn on the lower back and an ActivPAL kit attached to the shanks of users. Their method performed well in terms of recognizing five basic ambulatory activities.

HAR systems based on smartphones have also been developed [26,27,29,30]. Pei et al. [26] constructed a Least Square SVM-based model to classify six activities using sensors from a smartphone. Using the smartphone's inertial data, a HAR dataset was created and published as a benchmark for human activity recognition [27]. On this database, San-Segundo et al. [30] created frequency features and developed a Gaussian Mixture model to segment the activities. Another approach used for HAR systems is based on smart watches [11,24,29]. Gyorbiri et al. [11] used a smart watch connected to a smartphone via Bluetooth to collect acceleration, magnetic, and angular speed data of six activities at the wrist, hip, and ankle. A neural network model was then applied to classify these activities. Moreover, convolution neural network (CNN) have been previously applied to recognize human activities using inertial data from smartphones [29].

HAR systems based on smart shoes have also been presented [13,38]. In a previous publication, we used two smart shoes to classify three ambulatory activities based on a new pressure-based feature. Zhang et al. utilized foot-force sensors and derived basic statistical features to classify five mobile activities. Fusing the aforementioned sensing approaches, different models have been presented to solve the HAR problem [3,9,20]. Bao et al. [3] classified twenty activities using five biaxial accelerometers on the arm, hip, thigh, wrist, and ankle with an accuracy of 84.26% using decision tree classifiers. Huynh et al. [12] placed totally 12 accelerometers on the shoulders, wrists, elbows, knees, ankles and both sides of the hip and then combined multiple eigenspaces with Support Vector Machine (SVM) to recognize eight daily activities. In summary, in the approaches focused on wearable sensors, researchers commonly addressed HAR by identifying tasks performed by users using inertial sensors, particularly accelerometers.

Many features derived from acceleration data have been presented for addressing HAR problems. These features are essentially based on statistical computations such as the mean, median, [1,26,34,36], or correlation between the axes of acceleration [6,10,36]. Features have also been created based on signal-magnitude processing [6,11]. Another category of acceleration-derived features is frequency-based features [3,7]. Several researchers have summarized the presented features and tested them with particular sensor setups [1,10]. Gonzalez et al. [10] used two smart watches to record accelerations at the wrists of users during three activities, namely walking, standing and resting, and then derived a list of common statistical features. A filter feature selection (FS) and a wrapper feature selection were then applied sequentially to select important feature sets for classification. A Genetic Fuzzy Finite State Machine (GFFSM) model

was presented to classify activities based on the selected feature sets.

Although advances in wearable sensors have facilitated the design and deployment of HAR systems, developing HAR applications with high accuracy remains a challenging task. It is because human activity is highly diverse, and therefore, HAR requires effective selection and efficient incorporation of sensors to obtain an accurate classification. In this paper, we aim at addressing some of the important issues in wearable-sensors-based HAR regarding sensor placement, sensor fusion, and feature selection from inertial and plantar-based data. These issues are evaluated in a user-dependent approach for daily activity recognition using a smart band and two smart shoes. We design a wearable monitoring system using a smart band, a pair of smart shoes and a smartphone to synchronously gather data from two users. The wearable monitoring system gathers inertial data at the user's wrist using built-in accelerometer and gyroscope sensors of the smart band. Using the sensors integrated into the smart shoes, the system collects acceleration, angular speed, and plantar pressure from the left and right feet. The plantar pressure consists of eight sensing data from eight metatarsal areas on each foot. The collected data are used to analyze and recognize the daily activities. The contribution of the paper includes: *presenting a wearable monitoring system that can synchronously track human activities; exploring the optimal body part between the wrist and feet to attach sensors for the best HAR; evaluating activity classification using a data-fusion platform; examining state-of-the-art features derived from inertial data to determine the useful features for activities; comparing predictive models for classifying daily activities.*

The remainder of this paper is organized as follows. Section 2 provides the details of the wearable monitoring system that is used to collect data from the daily activities. Section 3 describes the nine aforementioned activities, summarizes the state-of-the-art features, and explains the feature-selection method and the predictive models for recognizing these activities. The experimental results are presented in Section 4. Finally, we conclude and identify future works in Section 5.

2 Wearable sensing system for daily activity monitoring

In this section, we describe the design of the proposed wearable sensing system and the techniques used to synchronously collect inertial and plantar-pressure data from the wearable devices. To recognize human activities, we created a wearable sensing system to acquire the motion data of user activities based on a smart band and two smart shoes. We used the smart band to obtain triaxial acceleration and triaxial angular speed data from the participants' wrist, whereas, the smart shoes were utilized to collect triaxial acceleration and eight pressure values from the insoles of shoes. These devices were connected to a smartphone via Bluetooth to control and synchronize data acquisition. Figure 1 shows the architecture of the proposed sensing system.

Gao et al. [9] stated that recognition accuracy does not vary more than 1% when the sampling rate is increased above 50Hz. In [31], authors concluded that using a low sampling rate (25Hz) for accelerometers and pressure sensors possibly produces high accuracy for posture and activity recognition. Therefore, to save energy and facilitate implementation, we set the sampling rate of the wearable system to 50Hz. We required the user to wear the smart shoes and smart band and to hold the smartphone in his pocket during experimentation. The participants conducted each separate activity for a specific duration. The collected data are continuously saved into a SQL database that can be uploaded to cloud for remote processing. The database is also used for offline analysis and classification to evaluate the performance in terms of the mentioned issues.

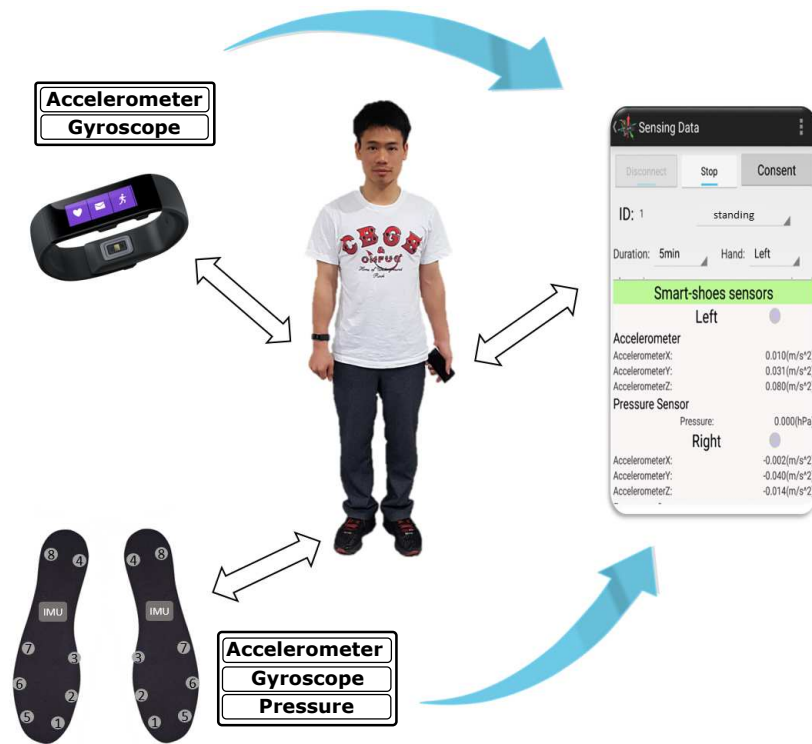


Figure 1: Wearable sensing system

3 Daily activity recognition

This section describes the activities of interest and the experimental setup in the study. We depict and analyze the corresponding inertial and plantar-pressure data of these activities obtained from the right wrist and both feet. In particular, we consider nine daily activities that require movement of both hands and feet. Figure 2 shows the activities studied in the paper.

The nine conducted activities were formed from three groups of similar activities, as described in Table 1. Group 1 represents ambulatory activities, which are closely related to foot movement. Group 2 represents activities that are dominated by hand movement. Finally, group 3 represents activities that include a balanced mixture of hand and foot movement. The combination of these activity groups is used to evaluate the importance of the relationship between the sensor placement and the activities.

Table 1: Groups of daily activities.

Group	Activity (Denotation)		
1	Standing (A1)	Walking (A2)	Jogging (A3)
2	Window cleaning (A4)	Tooth brushing (A5)	PC using (A6)
3	Door opening (A7)	Floor mopping (A8)	Book carrying (A9)

To recognize activities, the sensory data from different sensors in the three devices are first smoothed using a low-pass Butterworth filter. The filtered data are then merged sequentially to evaluate their importance in activity recognition. Then, we derive all possible features from these data based on statistics, customization, and energy computation. Finally, we analyze and rank all of the features derived from the sensory data, and select subsets of important features for classification. This process is described in Figure 3.

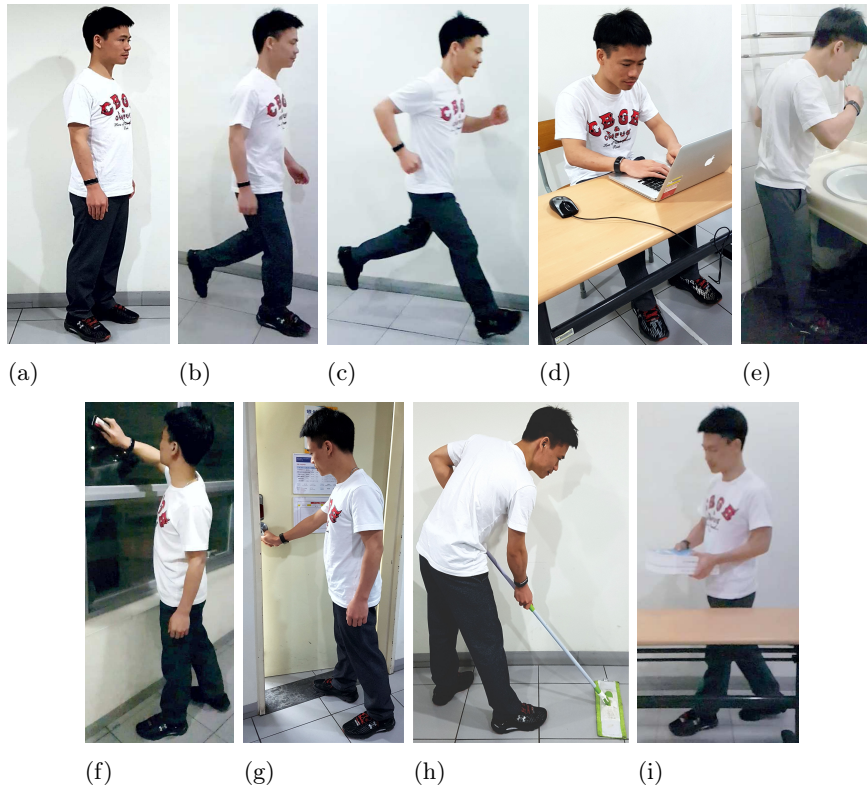


Figure 2: Descriptions of the experimental activities: (a) Standing; (b) Walking; (c) Jogging; (d) PC Using; (e) Tooth Brushing; (f) Window Cleaning; (g) Door Opening; (h) Floor Mopping; (i) Book Carrying

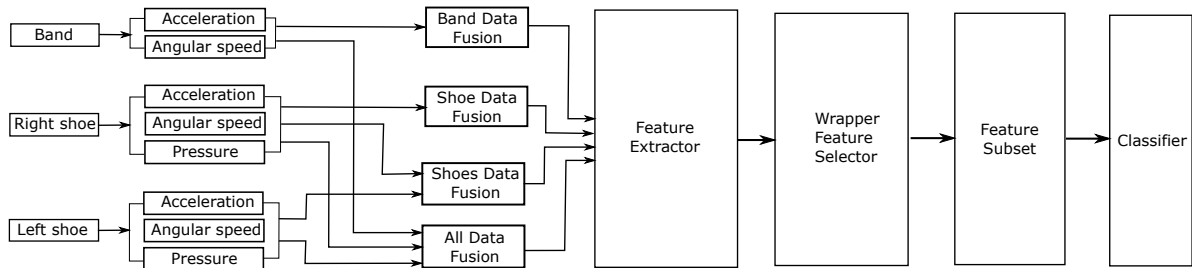


Figure 3: Architecture of activity recognition

3.1 Experimental configuration

Users wear the sensor devices and run the wearable system while conducting the activities. The wearable sensing system continuously records all sensory data and saves data in a SQL-formatted dictionary for offline processing. Figure 4 and 5 depict the acceleration and angular speed, respectively, obtained at a user's wrist for the nine activities. The angular speed data of the activities on the right shoe are shown in Figure 6.

Herein, we accounted for the issues in offline-segmented activity recognition, by starting the system immediately before the activities began and stopping it immediately after the activities concluded, which ensured that only the motion data from the activities were obtained. Then, in the offline database, we divided the data into equal-time segments for all activities. We used both the event-defined and the sliding windows for segmentation. We allowed the users

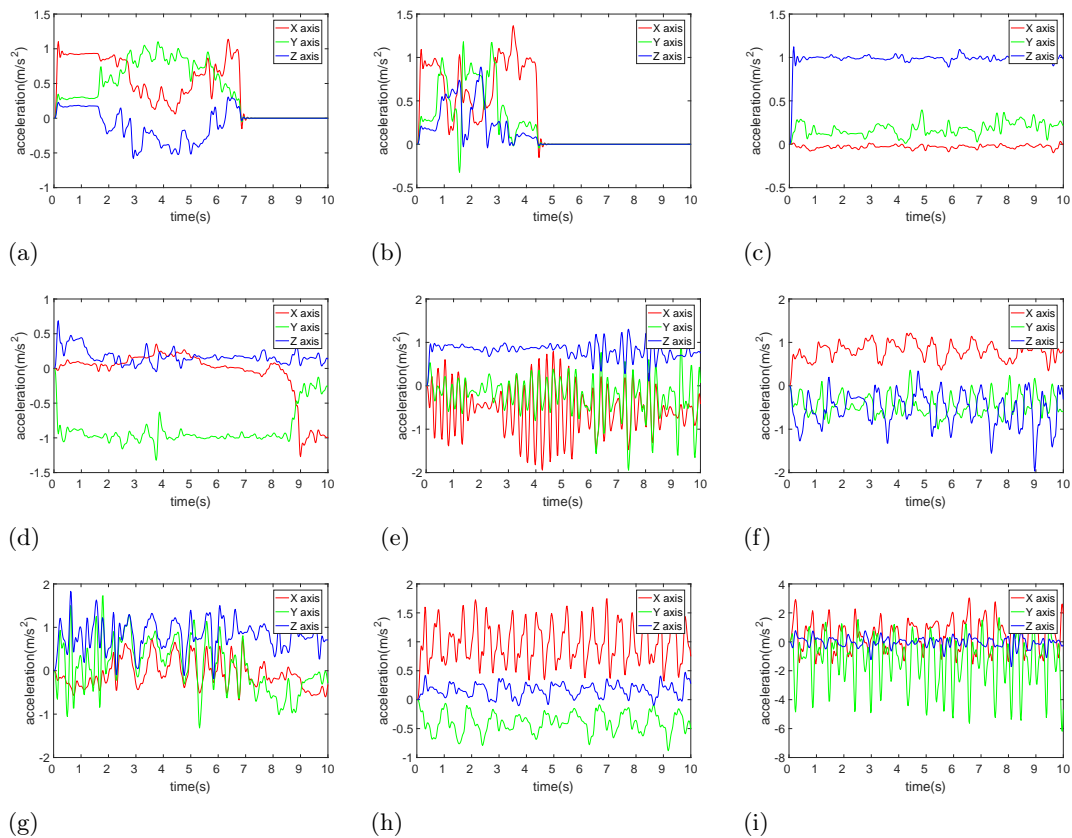


Figure 4: Wrist acceleration for the nine studied activities: (a) Book Carrying; (b) Door Opening; (c) Floor Mopping; (d) PC Using; (e) Jogging; (f) Standing; (g) Tooth Brushing; (h) Walking; (i) Window Cleaning

to separately conduct the "Door Opening" and "Book Carrying" activities, which are distinct actions, and collected the data for each action. For the other activities, the users performed the corresponding actions continuously for 5-10 minutes. We recorded all sensory data and equally segmented the data offline into 10-second samples.

3.2 Feature extraction

From the collected data for each segmented activity, we extracted significant motion features to recognize each activity. Specifically, we considered features based on statistics, correlation, frequency, and magnitude. The following features, derived from the inertial data, were taken into accounts:

(1) The statistic features comprised the mean, median, mode, range, skewness, kurtosis, 4-th and 5-th central moment, standard deviation, variance, mean absolute deviation, and sum of absolute values. The description of these features are as follows:

- Mean [1, 6, 10, 26, 34, 36]: the average of the data segmentation X

$$\mu = \frac{1}{n} \sum_{i=1}^n x_i \quad (1)$$

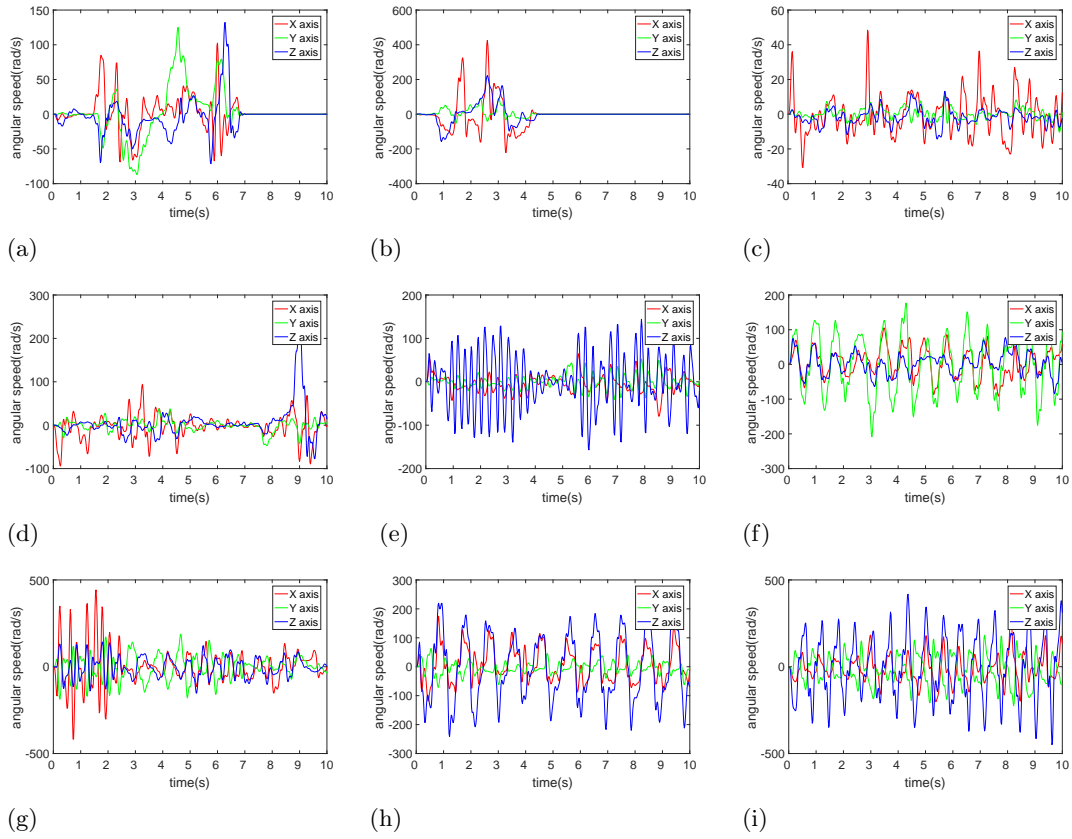


Figure 5: Wrist angular speeds for the nine studied activities: (a) Book Carrying; (b) Door Opening; (c) Floor Mopping; (d) PC Using; (e) Jogging; (f) Standing; (g) Tooth Brushing; (h) Walking; (i) Window Cleaning

- Median [1, 7, 26]: the middle value of the data segmentation X

$$\tilde{\mu} = \begin{cases} X(\frac{n+1}{2}) & n : \text{oddvalue} \\ \frac{X(\frac{n}{2}) + X(\frac{n}{2} + 1)}{2} & n : \text{evenvalue} \end{cases} \quad (2)$$

- Mode [1, 26]: the most frequently occurring value $\hat{\mu}$ in the data segment X - Range [1]: the maximum difference between the values within the sliding window

$$r = \max_{i=1}^n(x_i) - \min_{i=1}^n(x_i) \quad (3)$$

- Skewness [1, 26]:

$$\gamma_1 = \frac{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^3}{(\sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2})^3} \quad (4)$$

- Kurtosis [1, 26]:

$$\gamma_2 = \frac{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^4}{(\sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2})^2} \quad (5)$$

- Moment [1, 10, 34, 36]: we selected the 4-th and 5-th moments of the data segment as derived

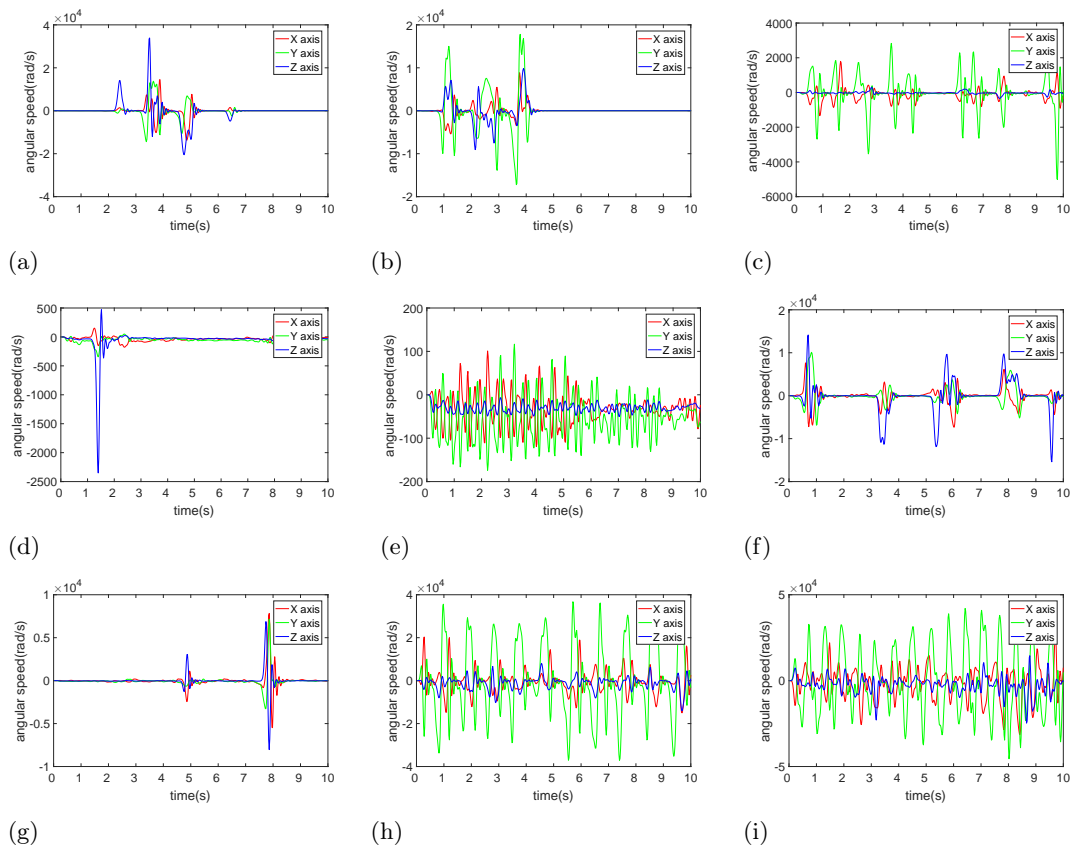


Figure 6: Angular speeds measured at the (g) Tooth Brushing; (h) Walking; (i) Window Cleaning features.

$$\mu_4 = \frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^4 \quad (6)$$

$$\mu_5 = \frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^5 \quad (7)$$

- Standard deviation [6, 7, 10, 34, 36]:

$$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \mu)^2} \quad (8)$$

- Variance [1, 6, 26]:

$$\sigma^2 = \frac{1}{n} \sum_{i=1}^n (x_i - \mu)^2 \quad (9)$$

(2) Magnitude-based features comprised the mean absolute deviation (MAD), signal magnitude area (SMA), root mean square (RMS), intensity of movement (IM), sum of absolute values (SAV). The description of these features are as follows:

- Mean absolute deviation [6, 10]:

$$MAD = \frac{1}{n} \sum_{i=1}^n |x_i - \mu| \quad (10)$$

- Signal Magnitude Area [7, 10, 34, 36]:

$$SMA = \frac{1}{n} \sum_{i=1}^n |x_i - \bar{x}| \quad (11)$$

- Root mean square [6, 10]:

$$RMS = \sqrt{\frac{1}{n} \sum_{i=1}^n x_i^2} \quad (12)$$

- Intensity of movement [10, 11]:

$$IM = \frac{1}{n} \sum_{i=1}^n |x_{n-i+1} - x_{n-i}| \quad (13)$$

- Sum of absolute values [10]:

$$SA = \frac{1}{n} \sum_{i=1}^n |x_i - \bar{x}| \quad (14)$$

(3) Correlation-based features comprised the correlation-between-axes values. The description of these features are as follows:

- Correlation between axes [6, 10, 36]: the Pearson correlation coefficient between two data segments $X = x_1, x_2, \dots, x_n$ and $Y = y_1, y_2, \dots, y_n$ is defined as:

$$\rho_{XY} = \frac{n (\sum_{i=1}^n x_i y_i) - \sum_{i=1}^n x_i \sum_{i=1}^n y_i}{(n \sum_{i=1}^n x_i^2 - (\sum_{i=1}^n x_i)^2) (n \sum_{i=1}^n y_i^2 - (\sum_{i=1}^n y_i)^2)} \quad (15)$$

(4) Frequency-domain features comprised the average energy (AE), dominant frequency (DF), and amplitude values. The description of these features are as follows:

- Average energy [1, 3, 6, 10, 34, 36]: the average of the energies in three axes of the triaxial sensors. The energy is calculated by summing all squared discrete fast Fourier transform (FFT) component magnitudes of the signal.

- Dominant frequency [7, 26]: the frequency determined in the FFT-domain at which the discrete FFT component magnitude is the largest.

- Amplitude [1, 7, 26]: the amplitude at the dominant frequency in the FFT-domain.

To extract the indicators from the plantar-pressure data obtained from the eight pressure sensors, we derived the following features:

◦ Statistical features [38]: these features comprised the mean, max, and standard deviation of the pressure data. The formulas for these functions are the same as those described above.

◦ Correlation between the counterpart sensors from both feet [38]: we calculated the correlation of the plantar-pressure data collected from counterpart sensors that are placed correspondingly under two feet. The correlation computation is as described in Eq. 15.

◦ Pressure area [13]: this feature is computed as the integral of the pressure data. In an earlier study [13], we used this feature for each step to classify three ambulatory activities with an accuracy rate of 95.2%. The formula to calculate this feature for a segment of k -th pressure, $P_k = \{P_k(1), P_k(2), \dots, P_k(n)\}$, is described as follows:

$$S_{P_k} = \sum_{i=1}^n P_k(i). \quad (16)$$

We applied different approaches to the acceleration, angular speed and plantar-pressure data to obtain features for classification. Table 2 summarizes the list of derived features. Here, (x, y, z) and (b, rs, ls) represent the (X, Y, Z) axes and (band, right shoe, left shoe), respectively. The second column of the table denotes the notations of the corresponding feature names in the first column. The third column contains the listed segmented data that are employed to extract the corresponding feature groups in the first column. The last four rows, i.e., mean, max, standard deviation, and pressure area, are the four features that are extracted from the plantar-pressure data.

Table 2: List of derived features.

Feature Name	Notation	Applied Data
mean	μ	
mode	$\hat{\mu}$	
median	$\tilde{\mu}$	
range	r	
skewness	γ_1	$a_x^b, a_y^b, a_z^b, \omega_x^b, \omega_y^b, \omega_z^b, a_x^{rs}, a_y^{rs}, a_z^{rs}, \omega_x^{rs}, \omega_y^{rs}, \omega_z^{rs}, a_x^{ls}, a_y^{ls}, a_z^{ls}, \omega_x^{ls}, \omega_y^{ls}, \omega_z^{ls}$
kurtosis	γ_2	
4-th moment	μ_4	
5-th moment	μ_5	
standard deviation	σ	
variance	σ^2	
mean absolute deviation	MAD	
signal magnitude area	SMA	
root mean square	RMS	$a_x^b, a_y^b, a_z^b, \omega_x^b, \omega_y^b, \omega_z^b, a_x^{rs}, a_y^{rs}, a_z^{rs}, \omega_x^{rs}, \omega_y^{rs}, \omega_z^{rs}, a_x^{ls}, a_y^{ls}, a_z^{ls}, \omega_x^{ls}, \omega_y^{ls}, \omega_z^{ls}$
intensity of movement	IM	
sum of absolute values	SA	
correlation	ρ	$(a_x^b, a_y^b), (a_y^b, a_z^b), (a_z^b, a_x^b), (\omega_x^b, \omega_y^b), (\omega_y^b, \omega_z^b), (\omega_z^b, \omega_x^b), (a_x^{rs}, a_y^{rs}), (a_y^{rs}, a_z^{rs}), (a_z^{rs}, a_x^{rs}), (\omega_x^{rs}, \omega_y^{rs}), (\omega_y^{rs}, \omega_z^{rs}), (\omega_z^{rs}, \omega_x^{rs}), (a_x^{ls}, a_y^{ls}), (a_y^{ls}, a_z^{ls}), (a_z^{ls}, a_x^{ls}), (\omega_x^{ls}, \omega_y^{ls}), (\omega_y^{ls}, \omega_z^{ls}), (\omega_z^{ls}, \omega_x^{ls})$
average energy	AE	$(a_x^b, a_y^b, a_z^b), (\omega_x^b, \omega_y^b, \omega_z^b), (a_x^{rs}, a_y^{rs}, a_z^{rs}), (\omega_x^{rs}, \omega_y^{rs}, \omega_z^{rs}), (a_x^{ls}, a_y^{ls}, a_z^{ls}), (\omega_x^{ls}, \omega_y^{ls}, \omega_z^{ls})$
dominant frequency	f_d	$a_x^b, a_y^b, a_z^b, \omega_x^b, \omega_y^b, \omega_z^b, a_x^{rs}, a_y^{rs}, a_z^{rs}, \omega_x^{rs}, \omega_y^{rs}, \omega_z^{rs}, a_x^{ls}, a_y^{ls}, a_z^{ls}, \omega_x^{ls}, \omega_y^{ls}, \omega_z^{ls}$
amplitude	A_{fd}	$a_x^b, a_y^b, a_z^b, \omega_x^b, \omega_y^b, \omega_z^b, a_x^{rs}, a_y^{rs}, a_z^{rs}, \omega_x^{rs}, \omega_y^{rs}, \omega_z^{rs}, a_x^{ls}, a_y^{ls}, a_z^{ls}, \omega_x^{ls}, \omega_y^{ls}, \omega_z^{ls}$
mean	μ	
max	max	$P_1^{rs}, P_2^{rs}, P_3^{rs}, P_4^{rs}, P_5^{rs}, P_6^{rs}, P_7^{rs}, P_8^{rs}, P_1^{ls}, P_2^{ls}, P_3^{ls}, P_4^{ls}, P_5^{ls}, P_6^{ls}, P_7^{ls}, P_8^{ls}$
standard deviation	σ	
pressure area	S	$P_1^{rs}, P_2^{rs}, P_3^{rs}, P_4^{rs}, P_5^{rs}, P_6^{rs}, P_7^{rs}, P_8^{rs}, P_1^{ls}, P_2^{ls}, P_3^{ls}, P_4^{ls}, P_5^{ls}, P_6^{ls}, P_7^{ls}, P_8^{ls}$

3.3 Feature selection

In this paper, we used the filter technique to reduce the computational complexity and accelerate feature selection. Specifically, we applied the RELIEF-F method [15] to score the extracted features. The RELIEF-F method is based on the average of the K near misses from each class. We analyzed and ranked all features derived from the sensory data, and then, selected subsets of important features for classification. Here, sensory data from each device are independently passed into the feature extractor to derive the features. The feature selector scores and ranks these features to form an effective subset of feature for classification. We also merged the corresponding features from the devices to assess activity recognition with sensor fusion schemes.

3.4 Classification

To classify nine daily living activities, we constructed two classifiers, i.e., KNN and CART. Using the results from the feature selector, we passed the selected features subset into the classifiers and compared the performance of the predictive models. Given a feature subset of m training samples $\{x^{(i)}, y^{(i)}\}_{i=1}^m$, the KNN classifier classifies each test sample $x^{(k)}$ based on the Euclidean distance of the test sample $x^{(k)}$ to each training sample $x^{(i)}$. The Euclidean distance is calculated as follows:

$$d(x^{(k)}, x^{(i)}) = \sqrt{\sum_{j=1}^N (x_j^{(i)} - x_j^{(k)})^2}. \quad (17)$$

The k training samples corresponding to the k shortest distances are used to categorize the test sample. We utilize the bagging approach for KNN classification. Specifically, the k training samples that have the shortest distances to the test sample are bagged in a group G . Then, the labels of these k samples are considered. The test sample is classified into the class that has the highest occurrence probability in the group G . The decision tree classifier is constructed based on a flowchart-like structure. At each internal node, a value test is conducted on an attribute of the selected feature subset to split the outcome into two groups. In other words, at each node, the tree divides the data into two branches. This splitting process is recursively repeated until either the groups at a node belong to the same class or the groups have the same attribute values.

4 Experimental results

In the experiments, we set the sampling rate of the system to 50Hz and required two participants to wear smart band and smart shoes and perform each segmented activity for 10 seconds to collect data. We used a separate sliding window to divide the data series into equal segments of recorded data. Each segment was used as a sample of an activity for recognition. In total, there were 363 samples of nine activities. We applied the proposed method presented to each sample to recognize its corresponding activity label. First, we removed noise in the signal by applying a low-pass Butterworth filter with the order of $N = 6$ and cut-off frequency $f_c = 10Hz$. Then, we create feature sets using a feature extractor with the operations listed in Table 2. Finally, applying the feature selection scheme RELIEF-F with $K=10$ on the feature sets, we identified the most important features for classifying activities on each device and fusion of devices.

Figure 7a and 7b depict results of feature selection for the features derived at the right smart-shoe and the corporation of both shoes in the descending order of their importance, respectively. Figure 7c depicts the 20 most important features derived at the band using the feature selection scheme in the descending order of their importance. Fusing all features created from all sensors of all devices and evaluating their importance, we obtain a set of 20 most important features as shown in Figure 7d. From this evaluation, we can see that the features derived from inertial data at the foot contribute a more important impact on recognition of the 9 activities than the features derived from inertial data at the wrist because the first 20 most important features in Figure 7b and 7a are all selected from data collected on the smart-shoes. Furthermore, it can be observed from Figure 7b and 7a that the two smart-shoes have a similarly influence on the recognition. From Figure 7a, 7b and 7c, we can draw a statement that using gyroscope sensors in the smart-shoes provides a better performance of recognizing the nine activities than using accelerometers at the feet because the all 20 first features in these figures are related to the smart-shoes. From the feature subsets, we applied 2 classifiers, i.e., KNN and CART, to recognize the activity of each sample. We examined the prediction on various feature sets to evaluate the

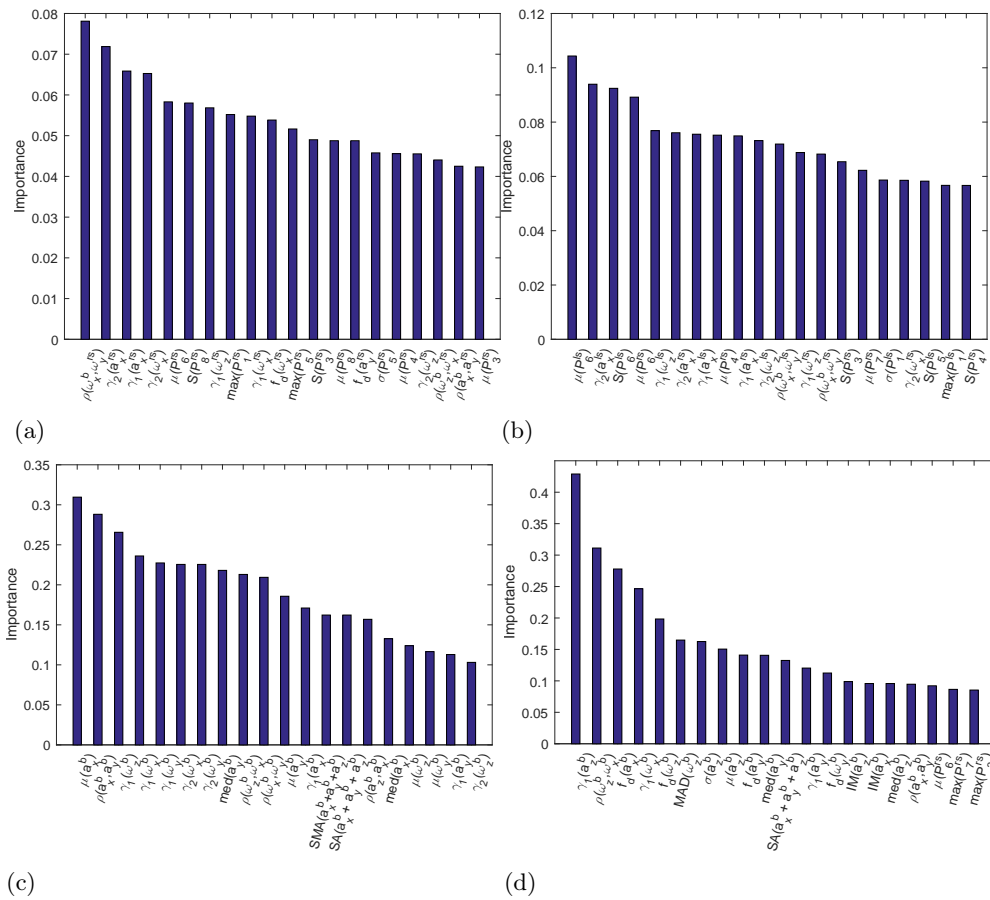


Figure 7: List of most important features for all activity classification: (a) Important features of a smart shoe; (b) Important features of two smart shoes; (c) Important features of smart band; (d) Important features of the sensor fusion

ability of each classifier. It should be noted that we do not need to test all features in the feature sets. Because the importance values of the features in each set have been measured in FS step, we sequentially selected features from the evaluated set according to descending importance. Herein, we examined sets of 1-40 features for each case. Figure 8 shows the accuracy rates of different classifiers with respect to the number of features for each case.

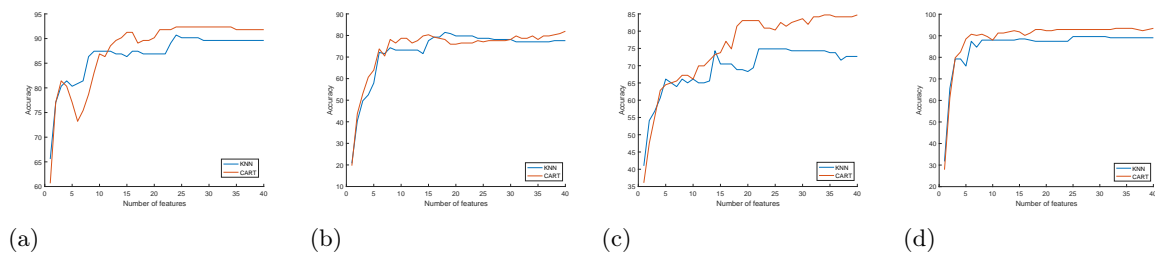


Figure 8: Accuracy of all activity classification versus the number of selected features: (a) A smart band; (b) A smart shoe; (c) A pair of smart shoes; (d) Sensor fusion

It can be seen that in overall, the KNN classifier exhibits a better performance than the CART classifier for recognizing the nine studied activities. Using the KNN classifier, the maximal

result (89.1%) for recognition is obtained with 21 features for the smart band case. For features derived from a smart shoe, the KNN-based recognition exhibits the optimal performance at 39 features. More features are required for the best recognition when using the smart shoe than when using the smart band, but the result is much lower (77%). Merging two smart shoes can improve the recognition up to 80% with 33 features. Finally, the data fusion scheme provides the best result (90.7%) with the fewest features used, i.e., 18 features. Therefore, we recommend the use of the data fusion scheme and application of the KNN classifier to recognize the nine studied activities with the 18 features depicted in Figure 7d.

Table 3 shows the details of the recognition results for all nine activities. The smart band was effective in recognizing the *Door Opening* and *PC Using* activities, which are significantly dependent on the hand movement. Particularly, the precision, recall and f1-score values of the recognition for *Door Opening* and *PC Using* using the smart band's sensors were all higher than the recognition values using the total combination of sensors. The f1-scores when using the smart band's sensors were 3.6% and 2.1% higher than the f1-scores when using the total combination of sensors for *Door Opening* and *PC Using*, respectively. The smart shoes can recognize the *Walking* and *Jogging* activities better than the smart band. The shoes-based recognition of these activities yielded an f1-score improvement of 2.2% and 2.0% compared with that of the smart band-based recognition. For the remain activities, the smart band-based recognition clearly surpasses the smart-shoes-based recognition. Combining all sensors provided the best recognition ability for all nine activities. Using the sensor fusion approach, the f1-score of all activities was 1.6% and 11.3% better than when using the smart-band and smart-shoe approaches, respectively.

Table 3: Classification metrics of each activity with different approaches

Sensing method	Smart-band sensors			Smart-shoe sensors			Combination of sensors		
Activity	precision	recall	f1-score	precision	recall	f1-score	precision	recall	f1-score
BookLoading	88.2%	93.8%	90.9%	73.3%	68.8%	71.0%	88.2%	93.8%	90.9%
DoorOpening	87.5%	93.3%	90.3%	68.4%	86.7%	76.5%	86.7%	86.7%	86.7%
PCUsing	100.0%	95.7%	97.8%	95.7%	95.7%	95.7%	95.7%	95.7%	95.7%
Standing	94.1%	80.0%	86.5%	71.4%	75.0%	73.2%	94.1%	80.0%	86.5%
ToothBrushing	89.3%	96.2%	92.6%	83.3%	57.7%	68.2%	92.6%	96.2%	94.3%
Mopping	95.8%	95.8%	95.8%	82.1%	95.8%	88.5%	96.0%	100.0%	98.0%
WindowsCleaning	90.9%	87.0%	88.9%	77.3%	73.9%	75.6%	95.7%	95.7%	95.7%
Walking	86.4%	95.0%	90.5%	90.5%	95.0%	92.7%	95.0%	95.0%	95.0%
Jogging	90.0%	93.8%	91.8%	93.8%	93.8%	93.8%	100.0%	93.8%	96.8%
Mean	91.4%	92.3%	91.7%	81.8%	82.5%	81.7%	93.8%	93.0%	93.0%

Figure 9 shows the average value of the performance metrics of the smart band-smart shoes fusion (B-S Fusion) and the reference methods. The multi-sensor method [9] yielded the best recognition result by fusing data from the accelerometers on the chest waist, thigh, and side; then, extracting the *mean* and *var* features; and, finally, using a decision tree classifier to recognize the activities. We utilized this approach on the collected database by applying the presented feature extractor on acceleration data from all devices and use a decision tree on the extracted feature set to evaluate the method performance. The RF+KNN method [25] extracted 12 features for each sample of acceleration collected at the wrist based on the mean, energy, frequency entropy, correlation between axes. Then, a variety of classifiers was applied to classify activities. Among these classifiers, a combination of random forest (RF) and KNN using the average of probabilities approach provided the best result.

It is clear that the proposed fusion approach outperformed the reference methods for activity recognition in terms of all four metrics, i.e., precision, recall, f-1 score, and accuracy. In particular, the accuracy rate of the B-S fusion method was 7.9% and 7.1% higher on average than the

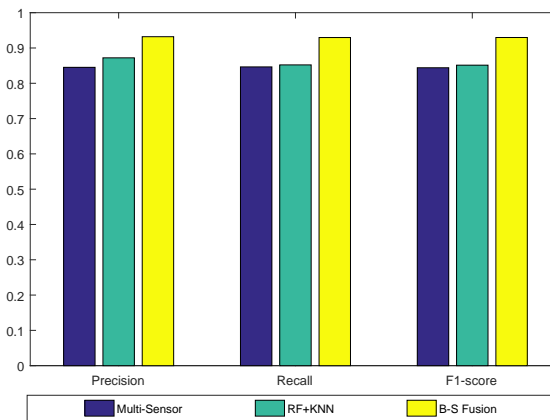


Figure 9: Performance comparison of the proposed method and the reference methods

mMulti-sensor [9] and RF + KNN [25] in accuracy rate, respectively. The B-S fusion method recognized activities better than the RF + KNN method because the B-S fusion method utilized more sensors in different locations, which in turn can better track the motion of different body parts during daily activities. This result confirms once again the results shown in Figure 8 and Table 3. In particular, when applying the same technique, the results of using the B-S fusion data surpassed the results of using only wrist-related data. Although the multi-sensor method also used a combination of accelerometers at the right wrist and both feet, this method did not utilize gyroscope data. Besides, the original paper for the multi-sensor method [9] dealt with four ambulatory activities, i.e., walking, standing, lying, sitting, and transitional states of these activities. Therefore, their selected features were not well-performed in this study.

5 Conclusion

This paper addressed the issues of sensor placement, feature selection, and classification in daily activity recognition using wearable sensors. A combination of a smart band and a pair of smart shoes was used to collect motion data from users and transfer data to a smartphone for offline activity classification. In our experiments, the participants wore the smart shoes and smart band and then, completed the experiments separately for each activity. Using a separate sliding window, we divided the data series into various segments of recorded data. From the segmented samples, we derived features and applied a filter feature selection algorithm to select important subsets. Two classifiers, i.e, KNN and CART, were employed to recognize the activities. The experimental results showed that the KNN classifier yielded better results than the CART classifier; the smart band outperformed the smart shoes in recognizing all nine activities in terms of accuracy and fewer features; the smart band is the best fit for recognizing the two hand-movement-dominated activities; the smart shoes are the best choice for the two foot-movement-dominated activities; and using a total combination of sensors is the best approach for recognizing all nine daily activities in terms of both accuracy and the number of required features.

Funding

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education

(NRF-2018R1D1A1A09083894). This research was also supported by the National Research Foundation of Korea (NRF) funded by the Korean Government (MSIP) (NRF-2016R1A5A1012966).

Conflict of interest

The authors declare no conflict of interest.

Bibliography

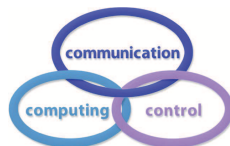
- [1] Banos, O.; Damas, M.; Pomares, H.; Prieto, A.; Rojas, I. (2012). Daily living activity recognition based on statistical feature quality group selection, *Expert Syst. Appl.*, 39, 8013–8021, 2012.
- [2] Banos, O.; Moral-Munoz, J.; Diaz-Reyes, I.; Arroyo-Morales, M.; Damas, M.; Herrera-Viedma, E.; Hong, C.; Lee, S.; Pomares, H.; Rojas, I.; Villalonga, C. (2015). mDurance: A novel mobile health system to support trunk endurance assessment, *Sensors*, 15, 13159–13183, 2015.
- [3] Bao, L.; Intille, S.S. (2004). *Pervasive Computing*; Vol. 3001, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1 – 17, 2004.
- [4] Bruno, B.; Mastrogiovanni, F.; Sgorbissa, A. (2015). Wearable inertial sensors: Applications, challenges, and public test benches, *IEEE Robot. Autom. Mag.*, 22, 116–124, 2015.
- [5] Bulling, A.; Blanke, U.; Schiele, B. (2014). A tutorial on human activity recognition using body-worn inertial sensors, *ACM Comput. Surv.*, 46, 1–33, 2014.
- [6] Chen, Y.P.; Yang, J.Y.; Liou, S.; Lee, G.; Wang, J.S. (2008). Online classifier construction algorithm for human activity detection using a tri-axial accelerometer, *Appl. Math. Comput.*, 205, 849–860, 2008.
- [7] Concepcion., A. D.L.; Morillo, S.; Gonzalez, A.; Ramirez, O. (2014). Discrete techniques applied to low-energy mobile human activity recognition. A new approach, *Expert Syst. Appl.*, 41, 6138–6146, 2014.
- [8] Dzitac, S ; Vesselenyi, T. ; Popper, L. et al. (2010). Fuzzy Algorithm for Human Drowsiness Detection Devices, *Studies in Informatics and Control*, 19(4), 419-426, 2010.
- [9] Gao, L.; Bourke, A.; Nelson, J. (2014). Evaluation of accelerometer based multi-sensor versus single-sensor activity recognition systems, *Med. Eng. Phys.*, 36, 779–785, 2014.
- [10] González, S.; Sedano, J.; Villar, J.R.; Corchado, E.; Herrero, Á.; Baroque, B. (2015). Features and models for human activity recognition, *Neurocomputing*, 167, 52–60, 2015.
- [11] Gyorbiró, N.; Fábíán, Á.; Hományi, G. (2008). An activity recognition system for mobile phones, *Mob. Networks Appl.*, 14, 82–91, 2008.
- [12] Huynh, T.; Schiele, B. (2007). Towards less supervision in activity recognition from wearable sensors. *10th IEEE Int. Symp. Wearable Comput.*, 3–10, 2006.
- [13] Jeong, G.M.; Truong, P.H.; Choi, S.I. (2017). Classification of three types of walking activities regarding stairs using plantar pressure sensors, *IEEE Sens. J.*, 17, 2638–2639, 2017.

-
- [14] Jia, Y. (2009). Diabetic and exercise therapy against diabetes mellitus, *2009 Second Int. Conf. Intell. Networks Intell. Syst.*, 693–696, 2009.
- [15] Kononenko, I. (1994). Estimating attributes: Analysis and extensions of RELIEF. *Proc. Eur. Conf. Mach. Learn.*, 171–182, 1994.
- [16] Lara, O.; Labrador, M. (2013). A survey on human activity recognition using wearable sensors, *IEEE Commun. Surv. Tutorials*, 15, 1192–1209, 2013.
- [17] Laudanski, A.; Brouwer, B.; Li, Q. (2015). Activity classification in persons with stroke based on frequency features, *Med. Eng. Phys.*, 37, 180–186, 2015.
- [18] Liu, Y.; Nie, L.; Liu, L.; Rosenblum, D. (2016). From action to activity: Sensor-based activity recognition, *Neurocomputing*, 181, 108–115, 2016.
- [19] Lowe, S.; ÓLaighin, G. (2014). Monitoring human health behaviour in one’s living environment: A technological review, *Med. Eng. Phys.*, 36, 147–168, 2014.
- [20] Mannini, A.; Sabatini, A.M. (2010). Machine learning methods for classifying human physical activity from on-body accelerometers, *Sensors*, 10, 1154–1175, 2010.
- [21] Mocanu, I.; Scarlat, G.; Rusu, L.; Pandelica, I.; Cramariuc, B. (2018). Indoor Localisation through Probabilistic Ontologies, *International Journal of Computers Communications & Control*, 13(6), 988-1006, 2018.
- [22] Mukhopadhyay, S.C. (2015). Wearable sensors for human activity monitoring: A review, *IEEE Sens. J.*, 15, 1321–1330, 2015.
- [23] Najafi, B.; Aminian, K.; Paraschiv-Ionescu, A.; Loew, F.; Büla, C.J.; Robert, P. (2003). Ambulatory system for human motion analysis using a kinematic sensor: Monitoring of daily physical activity in the elderly, *IEEE Trans. Biomed. Eng.*, 50, 711–723, 2003.
- [24] Nguyen, L.; Zeng, M.; Tague, P.; Zhang, J. (2015). Recognizing new activities with limited training data, *Proc. 2015 ACM Int. Symp. Wearable Comput. - ISWC '15*, ACM Press: New York, USA, 67–74, 2015.
- [25] Nguyen, M.; Fan, L.; Shahabi, C. (2015). Activity Recognition Using Wrist-Worn Sensors for Human Performance Evaluation, *2015 IEEE Int. Conf. Data Min. Work.*, 164–169, 2015.
- [26] Pei, L.; Guinness, R.; Chen, R.; Liu, J.; Kuusniemi, H.; Chen, Y.; Chen, L.; Kaistinen, J. (2013). Human behavior cognition using smartphone sensors, *Sensors*, 13, 1402–1424, 2013.
- [27] Reyes-Ortiz, J.L.; Oneto, L.; Samà, A.; Parra, X.; Anguita, D. (2016). Transition-aware human activity recognition using smartphones, *Neurocomputing*, 171, 754–767, 2016.
- [28] Rodgers, M.; Pai, V.; Conroy, R. (2015). Recent advances in wearable sensors for health monitoring, *IEEE Sens. J.*, 15, 3119–3126, 2015.
- [29] Ronao, C.A.; Cho, S.b. (2016). Human activity recognition with smartphone sensors using deep learning neural networks, *Expert Syst. Appl.*, 59, 235–244, 2016.
- [30] San-Segundo, R.; Lorenzo-Trueba, J.; Martínez-González, B.; Pardo, J. (2016). Segmenting human activities based on HMMs using smartphone inertial sensors, *Pervasive Mob. Comput.*, 30, 84–96, 2016.

- [31] Sazonov, E.S.; Fulk, G.; Hill, J.; Schutz, Y.; Browning, R. (2011). Monitoring of posture allocations and activities by a shoe-based wearable sensor, *IEEE Trans. Biomed. Eng.*, 58, 983–990, 2011.
- [32] Storm, F.; Heller, B.; Mazzà, C. (2015). Step detection and activity recognition accuracy of seven physical activity monitors, *PLoS One*, 10, e0118723, 2015.
- [33] Sung, M.; Marci, C.; Pentland, A. (2005). Wearable feedback systems for rehabilitation, *J. Neuroeng. Rehabil.*, 2, 17, 2005.
- [34] Suto, J.; Oniga, S. and Sitar, P.P. (2017). Feature analysis to human activity recognition, *Int. J. of Computers Communications & Control*, 12(1), 116-130, 2017.
- [35] Wang, J.; Chen, R.; Sun, X.; She, M.; Wu, Y. (2011). Recognizing human daily activities from accelerometer signal, *Procedia Eng.*, 15, 1780–1786, 2011.
- [36] Yang, J.Y.; Wang, J.S.; Chen, Y.P. (2008). Using acceleration measurements for activity recognition: An effective learning algorithm for constructing neural classifiers, *Pattern Recognit. Lett.*, 29, 2213–2220, 2008.
- [37] Zhang, W.; Thurow, K. and Stoll, R.. (2016). A context-aware mhealth system for on-line physiological monitoring in remote healthcare. *Int. J. Computers Communications & Control*, 11(1), 142-156, 2016.
- [38] Zelun Zhang.; Poslad, S. (2014). Improved use of foot force sensors and mobile phone GPS for mobility activity recognition, *IEEE Sens. J.*, 14, 4340–4347, 2014.

Automated Expert System Knowledge Base Development Method for Information Security Risk Analysis

D. Vitkus, Z. Steckevecius, N. Goranin, D. Kalibatiene, A. Cenys



Donatas Vitkus*

Vilnius Gediminas Technical University, Vilnius, Lithuania

*Corresponding author: d.vitkus@vgtu.lt

Zilvinas Steckevecius

Vilnius Gediminas Technical University, Vilnius, Lithuania

zilvinas.steckevecius@vgtu.lt

Nikolaj Goranin

Vilnius Gediminas Technical University, Vilnius, Lithuania

nikolaj.goranin@vgtu.lt

Diana Kalibatiene

Vilnius Gediminas Technical University, Vilnius, Lithuania

diana.kalibatiene@vgtu.lt

Antanas Cenys

Vilnius Gediminas Technical University, Vilnius, Lithuania

antanas.cenys@vgtu.lt

Abstract: Information security risk analysis is a compulsory requirement both from the side of regulating documents and information security management decision making process. Some researchers propose using expert systems (ES) for process automation, but this approach requires the creation of a high-quality knowledge base. A knowledge base can be formed both from expert knowledge or information collected from other sources of information. The problem of such approach is that experts or good quality knowledge sources are expensive. In this paper we propose the problem solution by providing an automated ES knowledge base development method. The method proposed is novel since unlike other methods it does not integrate ontology directly but utilizes automated transformation of existing information security ontology elements into ES rules: The Web Ontology Rule Language (OWL RL) subset of ontology is segregated into Resource Description Framework (RDF) triplets, that are transformed into Rule Interchange Format (RIF); RIF rules are converted into Java Expert System Shell (JESS) knowledge base rules. The experiments performed have shown the principal method applicability. The created knowledge base was later verified by performing comparative risk analysis in a sample company.

Keywords: information security risk analysis, ontology, knowledge base, expert system, transformation, RIF, JESS.

1 Introduction

Many authors agree that today information is the critical business part despite the size of the enterprise. Companies are adapting to the time changes: growing speed of change and complexity, globalisation [16]. Even the smallest company has any information and information system, which are needed to be secured [35]. However, because of enterprises becoming more complex, integrated and connected to third parties, the security and controls budget quickly reaches its limitations [12].

The protection of information resources from the complex and rapidly evolving security threat landscape is a significant challenge to the modern organisation [46]. The reasons stated above motivate for searching of effective ways to increase information security level in organizations.

According to the importance of assets, it is necessity to analyse the potential risks to do not allow these risks to be converted into events [48]. As [10] said, risk management has proved to be efficient in the frame of the governance system due to its capacity to reduce costs associated with the management of different risks. According to Europe's General Data Protection Regulation, a risk-based approach to data protection is embraced [30]. So, all companies, including small and medium-sized enterprises (SME), have to protect their information systems. Enterprises have two ways of ensuring their information security: to employ a specialist or to outsource the risk analysis service. The problem is that the price of both choices is rather high.

Therefore, there is a need to automate the security risk analysis process by introducing expert systems or decision support systems, which could help enterprises to perform an information security risk analysis without any special knowledge and without hiring security experts and making security risk analysis process faster and cheaper [47]. There were some attempts to use expert systems for automating a particular part of security risk analysis [4, 5], cybersecurity incident prediction [42] and solving other real-world problems also [29]. The main reason of such attempts is to make risk analysis process faster and cheaper [47]. Also, using expert systems helps to optimise asset management and their life cycle according to risk assessment, especially in specific sectors, like electric power transmission [41], power plant projecting [19]. However, it is necessary to mention that the development of an expert system knowledge base is an expensive and complicated process [24], [15]. So, the motivation of the paper is related to the need to automate the security risk analysis knowledge base development to minimize the expenses.

In this paper we propose a novel approach that allows the automatic transformation of existing information security ontologies into the expert system knowledge base rule set. Currently, a lot of information, including security information, like standards, best practices, is collected and presented in the ontologies [7]. Ontology comparing with usual not semantic database has particular advantages that can be used for developing expert systems [14]. Ontology can be expressed in several ways, for example, using graphical software, which makes ontology formation, maintenance, and usage easier [40]. Therefore, ontology presented in a particular software, could be used for its automatic transformation into the expert system knowledge base.

However, a deep understanding of ontology is needed, since any change in the ontology may require a change in the software's source code [27]. Nevertheless, these disadvantages cannot reproduce the expressiveness of ontology, and expert systems have their inference engine which is separate from the knowledge base. The main advantages of the work is that we provide a method for automated knowledge base development for an expert system, that can be used for risk analysis. It can help to provide an information security risk assessment for non-IT specialist cheaper and in a more effective way. The methods of information security risk analysis and the development of reasoning engines for expert systems are out of the scope of this paper.

The paper is organized as follows. Section 1, current section, is an introduction. Section 2

presents related works in security risk analysis and ontology usage for the development of expert systems knowledge base. Section 3 presents an approach of automatic transformation of existing security ontologies into the expert system knowledge base rule set and presents the implementation of the proposed approach of the information security standards ontology transformation into the JESS ES rules which is implemented in several steps with the help of a developed tool. OWL RL subset of ontology elements are segregated into RDF triplets, that are later transformed into RIF format. Then, RIF rules are converted into JESS knowledge bases rules with the help of an external tool. Conversion results are presented in Section 4. Finally, Section 5 concludes the paper.

2 Related work

Expert system is a computer-based system which has several parts. The basic architecture of an expert system is shown in Figure 1.

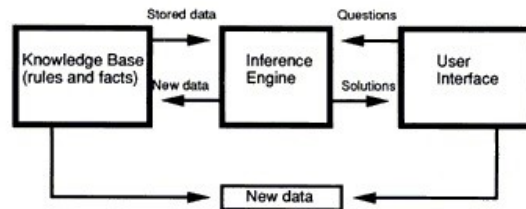


Figure 1: The basic architecture of an expert system [22]

The basic architecture of an expert system includes three main parts: Knowledge Base, Inference Engine and User Interface. One of the biggest problems in expert system usage is to get knowledge base updated [3]. Nevertheless, expert systems are used in nowadays for solving actual problems. For example, it can be successfully used as first-line in IT help-desk [13].

The majority of expert systems are developed using specialized software called a shell, especially when it comes to the rule-based expert systems. Shell allows the user just to create the knowledge base in the form of simple rules and not paying attention to knowledge interpretation engine development, thus minimizing the ES development time [2].

Nevertheless, forming the knowledge base is a complicated process that has a number of unsolved issues and illustrates the problems of this work. One of them is knowledge base integrity that is hard to maintain [24]. Adding new data can destroy existing rules, cause conflicts or endless cycles [25]. In result, it can make expert system work incorrectly.

There are some methods to solve knowledge base integrity problem. One of them is KADS (and its extension - CommonKADS) methodology [44]. The main idea is to design everything with UML diagrams [28]. The main disadvantage of that method is that it needs a lot of time resources, and the user can still make a mistake if a knowledge base is very complicated.

The use of information collected in the form of ontologies for ES knowledge base formation seems useful by many experts, but in practice, current research focus on ontologies and expert systems is separated. The main idea of ontology is to identify specific object classes and relations between them [8]. Ontology can be used in various business areas, but these areas can be divided into two parts: ontology usage as a vocabulary and ontology usage as a content [9].

Ontology usage as vocabulary enabled to develop the second generation of the web [18]. But ontology can be much more than a set of concepts or vocabulary - they have a lot of

applications in artificial intelligence. In this context, ontology can be used as information sources [23]. Ontology provides integrity and can be displayed by various graphical tools, has a common format and can be apprehensible in other systems, which designed to work with ontologies [31]. For example, XP.K (eXtreme Programming of Knowledge-based systems) methodology is based on Agile principles: to start from the simplest model of expert system and grow it with time [26]. Model should include just that what is really needed to solve existing problems. Knowledge base is created from ontology which is created by experts [38]. The main problem of this approach is that it requires a lot of time to develop the ontology from scratch on iteration basis and does not make use of already existing knowledge collected, while it could be valuable to use already existing information security-related ontologies.

Some attempts [34] for ontology use as a source for knowledge base formation, but the approach proposed destroys the idea of ES that knowledge base and inference engine should be separate. DAMLJessKB [21] software was developed to transform DAML (DARPA Agent Markup Language) ontology to the JESS expert system's rules, but it can work only with specific DAML ontology and JESS expert system. Another sample is DLEJena - the software, which transforms the OWL 2 RL profile, compatible with pD semantic, to Jena expert system platform [32]. The main disadvantage of these programs is that they transform only specific ontologies to the specific expert systems format.

On the other hand, there exist a number of information security ontologies that can be used in knowledge base formation of risk-analysis ES. Currently, most of them are used for other purposes. For example, ontology proposed in [39] can be used as a tool to identify the level of system vulnerabilities according to the internal users' accounts configuration and system configuration [33]. As the authors state, all illegal activity in the system is done by human resources and internal users have more privileges than external. This tool is based on taxonomy with users' settings and includes different behavioural motivation, for example, intentional and unintentional activity.

ROPE methodology and the related ontology is used for enterprise IT security evaluation, focuses on business processes and risk management [33]. Ontology encapsulates well-known information security concepts, such as assets, vulnerabilities, threats, and controls. There is a number of ontologies based on external security standards, like ISO 27001/2 that can be used to align external standards with internal procedures [17]. One more security ontology is OntoSec [33] that can be used by security engineers can to set configuration effectively, according to the existing security events.

In [36] the new exhaustive ontology was proposed, which increased coverage of security standards compared to the existing ontologies and has better branching and depth properties for ontology visualization purposes. It was used for security standards mapping task and was linked with 4 security standards: ISO 27001, PCI DSS, ISSA 5173 and NISTIR 7621.

Summarasing it can be said that there are a lot of information security ontologies and our work allows transforming the selected ontology into expert system rules set in an automated and novel way.

3 Automated approach of ontology transformation into ES knowledge base

In order not to spend time resources for developing knowledge bases from scratch and to solve the limitations specific to earlier research in ontology transformation to knowledge base rule-sets we propose new method that allows transformation of existing information security ontologies into expert system rule-set via universal RIF format, that is later converted to the

format of a specific expert system. In fact, the method can be applied for any ontology type transformation to any ES knowledge base with some additional modifications, related to the syntax of ES rule defining language.

The method proposed is that it uses the RIF (Rule Interchange Format) format, which was presented by the W3C consortium in 2010. The primary purpose of this format is to transfer rules from one system to another [49]. Unlike other standards of Semantic Web (RDF, OWL, SPARQL), RIF was developed not for defining rules, but as a standard for rule transfer from one system to another, which became extremely important with the increase of standards for rule definition [43].

RIF has two dialects: based on logic and based on rules. Dialects based on logic include logical languages, like Horn logic and others. Dialects based on rules include productive rules. The same rules are used in expert systems [37]. RIF PRD (Production Rule Dialect) is a dialect based on production rules. Production rules semantic have format "IF condition THEN activity". Figure 2 shows an example of RIF PRD.

```
Document (
  Prefix(rdfs <http://www.w3.org/2000/01/rdf-schema#>)
  Prefix(imdbrelf
<http://example.com/fauximdbrelations#>)
  Prefix(dbpediaf
<http://example.com/fauxibdbrelations>)
  Prefix(ibdbrelf
<http://example.com/fauxibdbrelations#>)

  Group(
    Forall ?Actor (
      If Or(Exists ?Film
(imdbrelf:winAward(?Actor ?Film))
      Exists ?Play
(ibdbrelf:winAward(?Actor ?Play)) )
      Then assert(dbpediaf:awardWinner(?Actor))
    )
    imdbrelf:winAward(RobertoBenigni LifeIsBeautiful)
  )
)
```

Figure 2: Example of RIF PRD

RIF was created in a way to be compatible with other W3C standards. That means that it can be compatible with RDF and OWL ontology languages [1]. Transferring these ontology languages into RIF can be done not only in the form rule-sets, but also in RDF triplets (subject, predicate, object) and OWL axioms with RIF rules, e.g. RDF data: S(Subject), P(Predicate) and O(Object) are transferred to the RIF format in a form: [(P->O)].

For example:

ex:Peter ex:isBrother ex:John;

ex:John ex:isFather ex:Paul;

states that Peter is the brother of John, and John is the father of Paul.

In the RIF transferring to:

ex:Peter [ex:isBrother -> ex:John];

ex:John [ex:isFather -> ex:Paul];

RIF rule, that uncle is the brother of father:

Forall ?x ?y ?z (?x[ex:isUncle -> ?z] :- And(?x[ex:isBrother -> ?y] ?y[ex:isFather -> ?z]))

states, that if x is the brother of y and y is the father of z , then x is the uncle of z . In our experiments we were using OWL RL profile as a source. OWL RL rules can be divided into four categories (which may overlap):

Triplet structure rules: RDF triplets. Transformation to RIF is trivial.

Listing rules: RDF lists. Transforming in two ways - transforming into a recursive set of rules or transforming into triple structure rules.

Inconsistent rules: RDF graph inconsistencies, which are expressed in first-order rules. There are several ways how to perform transformation.

Data type rules: type's comparison and verification. OWL and RIF supported types are transformed directly.

I.e. OWL RL can be transformed into RIF rules. However, some limitations still exist. These limitations were introduced by OWL founders to provide maximum flexibility without sacrificing the reliability of the calculations. So it can be said that the violation of at least one limitation affects the results of the expert system. The method proposed in Figure 3 was implemented using C# language. During the first step, the tool developed converts the information security ontology into RIF standard. At the second step (RIF transforming into expert system production rules) the RIF PRD profile was used, which is already included in the RIF Core profile. The obtained RIF rules can later be transformed into the syntax supported by the ES or used directly if ES supports the RIF format, like XSB, JESS, and ASP.

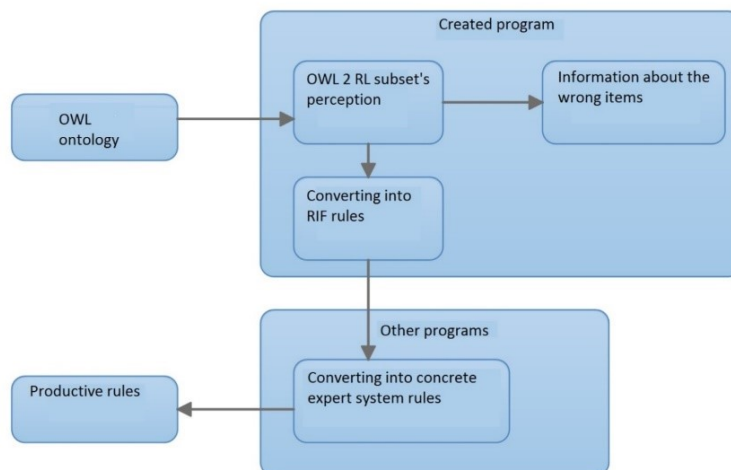


Figure 3: General view of the method proposed

The detailed method activity diagram is shown in Figure 4. The yellow border depicts actions that were proposed and implemented by the paper authors, while actions outside the yellow border are performed with the help of already existing methods and tools.

Model consists of primary data - ontology (OWL). Transformation of RIF rules is performed in several steps:

Scan ontology. OWL\XML ontology is scanned and checked, if the ontology is in OWL\XML format, since the developed tool supports only the most popular OWL\XML format. If ontology is stored in other formats, external tools should be used first to convert it into OWL\XML.

Check if the element is OWL RL. Only OWL RL subset is converted, but it covers the big part of OWL Full. Elements not belonging to OWL RL will be skipped and should be converted into ES rules if needed manually or using other methods.

Collect non-OWL RL subset & Collect OWL RL subset. After successful scanning of OWL\XML ontology OWL RL elements are extracted for further processing. Non-OWL RL elements are separated for manual processing

Transform to RDF triplets. The identified OWL RL elements are saved in the form of

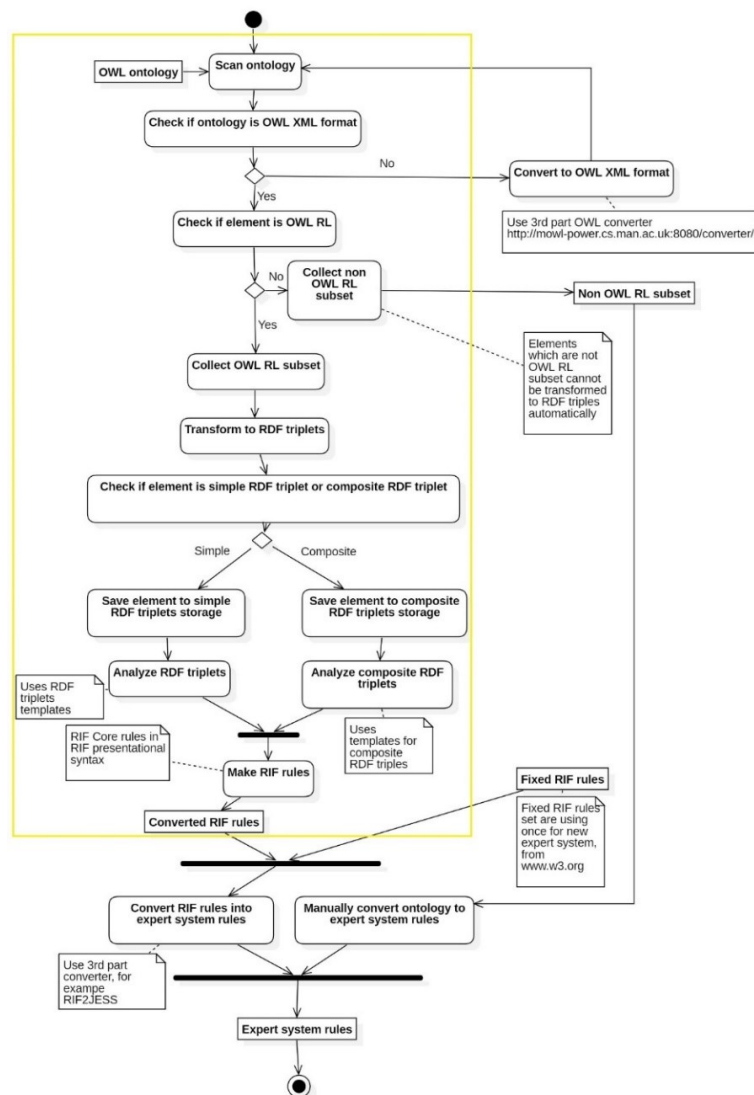


Figure 4: The detailed method activity diagram

RDF triplet format (subject, predicate, object). Check if the element is a simple RDF triplet or composite RDF triplet. Evaluation is performed if RDF triplet can be unlinked from other RDF triplets.

Save element to simple RDF triplet storage. RDF storage stores RDS triplets that can be unlinked from other RDF triplets, e.g. attribute type "symmetrical" is saved in the form of RDF triplet (*?p rdf:type owl:FunctionalProperty*), where ?p is attribute name. Such kind of data is stored in the form of text registry, having 3 fields.

Save element to composite RDF triplet storage. Elements that cannot be unlinked are stored in a storage for composite RDF triplets. for example the ontology statement that all attributes *?p of object ?x are of ?y type: (?x owl:allValuesFrom ?y) (?x owl:onProperty ?p)*. Up to 3 linked RDF triplets can be stored.

Analyze RDF triplets & Analyze composite RDF triplets. In this step, RDF triplets are transformed according to the conversion table, i.e. RDF triplet conversion templates. The main part of the RDF triplet is predicate, which can acquire values from a finite set of possible

values because of ontology formality feature. The remaining two triplet elements - subject and object are specific concepts or attributes, defined in the ontology, that are used to fill in the conversion template. In several specific cases (e.g. *owl:maxCardinality*) the template is modified.

Make RIF rules. Templates are applied for RDF triplet conversion into RIF rules.

The formal algorithm in the form of pseudocode of OWL RL transformation into RIF rules is provided in Fig. 5

```

READ selected_owl_file;
WHILE NOT End_of_xml_tokens DO
  GET xml_nodes
END DO
FOREACH xml_node in document_element DO //analyze each XML node
  IF node_name=="Declaration" THEN DO node_Declaration(node) //next step by the node_name
  IF node_name=="DisjointClasses" THEN DO node_DisjointClasses(node)
  //similar actions for other types of nodes. At all 18 types of nodes are used.
  ELSE DO collect_non_RL_elements //if XML node aren't OWL 2 RL element, collect them separately
END DO

PROCEDURE node_Declaration (XmlNode node) //example of procedure by node_name;
  IF childNode_Name == "Class" THEN
    MAKE rdf_Triplet(attr.Value, "rdf:type", "owl:Class")
  IF childNode_Name == "NamedIndividual" then
    MAKE rdf_Triplet(attr.Value, "rdf:type", "owl:NamedIndividual")
  //making RDF triplets by childNode names, at all 5 types of RDF triplets for this class in this example
END

DO rdf_to_rif //RDF triplets are converting to RIF rules, using patterns

PROCEDURE rdf_to_rif(IN rdf_triplets; OUT rule_1; OUT rule_2)
  READ rdf_triplet
  IF rdf_triplet_item2 == "rdf:type"
    THEN DO templateType(item, out rule1); //choose RIF pattern by the RDF triplet type
  IF rdf_triplet_item2 == "owl:equivalentProperty"
    THEN DO templateEquivalentProperty(item, out rule1, out rule2);
  //the similar for all RDF triplet item types,
END

PROCEDURE templateType(IN item, OUT string ans) //example of RIF rule pattern
  IF item == "owl:FunctionalProperty"
    THEN return rule ("forall ?y2 ?x ?y1 (?y1[owl:sameAs->?y2] :- And(?x[{}->?y1] ?x[{}->?y2]))", item.s1);
  //at all 20 similar RIF rules patterns
END

```

Figure 5: Pseudocode for OWL RL transformation into RIF rules

While analyzing XML nodes, RDF triplets are segregated. RDF triples are created according to the predefined patterns:

IF	THEN
T (s ₁ , p ₁ , o ₁)	T (sr ₁ , pr ₁ , or ₁)
...	...
T (s _n , p _n , o _n)	T (sr _m , pr _m , or _m)

where each argument to the T predicate may be a variable or literal value. RDF triplets created in such a way are later transformed into RIF rules.

Group (

Forall ?v₁₁ ... ?v₁_o (

sr₁[pr₁->or₁] :- And(s₁[p₁->o₁] ... s_n[p_n->o_n]))

...

Forall ?v_m₁ ... ?v_m_o (

sr_m[pr_m->or_m] :- And(s₁[p₁->o₁] ... s_n[p_n->o_n]))

)

where ?v₁₁ ... ?v₁_o are the variables which occur in the rule.

Below the sample transformation is provided.

Two following RDF triplets are extracted from the ontology:

atributte_1 rdf:type owl:SymmetricProperty

atributte_2 rdf:type owl:SymmetricProperty,

the template of symmetrical attributes is applied:

```
Forall ?x ?y (
  ?y[?p->?x] :- And(
    ?x[?p->?y] ))
```

the following RIF rules are obtained:

```
Forall ?x ?y (
  ?y[atributte_1->?x] :- And(
    ?x[atributte_1->?y] ))
Forall ?x ?y (
  ?y[atributte_2->?x] :- And(
    ?x[atributte_2->?y] ))
```

The transformation process is composed of two parts: transformation of fixed rules and ontology rules, obtained from its T-Box axioms. In OWL 2 RL profile both ontology axioms and additional logical rules can be stored [45], but in this research, only the subset of axioms is used as a suitable source for ES knowledge base rules.

Although ontology typically has a very sophisticated structure, it can be easily represented in the form of RDF triplets as was shown earlier.

Another issue of ontology transformation - correctness of ontology that cannot be evaluated by the conversion program. Evaluation of ontology composition correctness is out of scope of this paper. It is assumed that ontologies used for experiments were correct and verified by other methods during their development process.

Some RIF rules (Fixed RIF rules) are obtained without analysis of ontology, since their perception is a part of ES. Such rules are transformed into ES production rules only once and are loaded into the knowledge base. The sample of a fixed rule:

```
Forall ?c1 ?c2 (
  ?c1[rdfs:subClassOf->?c2] :- ?c1[owl:equivalentClass->?c2])
Forall ?x ?z ?y (
  ?x[owl:sameAs->?z] :- And(
    ?x[owl:sameAs->?y]
    ?y[owl:sameAs->?z] ))
Forall ?x ?y (
  rif:error() :- And(
    ?x[owl:sameAs->?y]
    ?x[owl:differentFrom->?y] ))
```

ES knowledge base rules are obtained by conversion of RIF rules, that are automatically generated from the ontology as described earlier. As also stated earlier, some ontology elements, that were not converted automatically, can be converted manually if they store some valuable information.

The final set of rules can be expressed by equation:

$$R(RDF(O)) = Fixed_rules \cup Ontology_rules(RDF(O)),$$

where O is ontology, $RDF(O)$ RDF triplets of ontology O , $R(RDF(O))$ - RIF is a set of rules, imported into ES knowledge base.

4 Results and discussion

The created program has five main parts: user interface; ontology scanning engine; analysis engine; ontology alignment to RDF triplet engine; transformation (into RIF rules) engine. The program class diagram is shown in Figure 6.

Program is composed of 6 main classes:

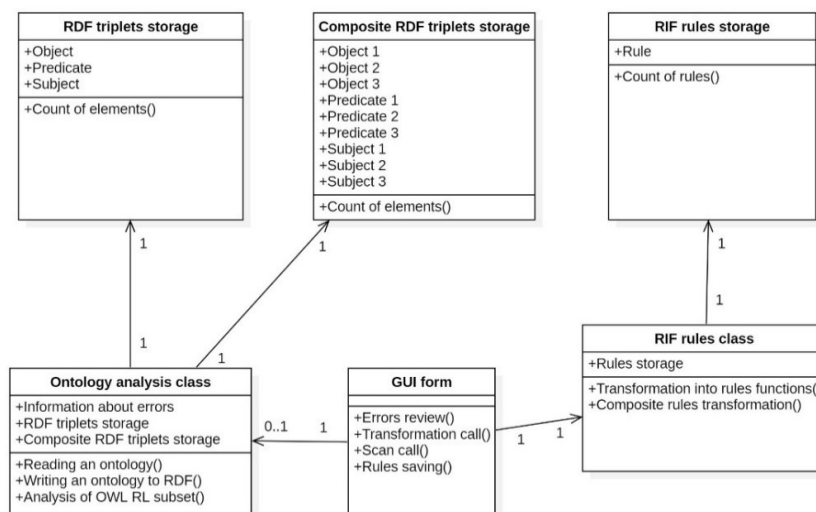


Figure 6: Program class diagram

GUI form. Program management. User can call ontology scanning, conversions into RIF rules, error review and rules saving functions.

Ontology analysis class. Responsible for XML/OWL ontology scanning, identification of extractable elements and their saving in the form of RDF triplets.

RDF triplets storage. Stores RDF triplets that can be unlinked from other RDF triplets.

Composite RDF triplets storage. Stores up to 3 linked together complex RDF triplets that can not be unlinked.

RIF rules class. Converts RDF triplets into RIF rules as defined. **RIF rules storage.** Stores RIF rules in the form of presentational syntax that is later used for transformation into ES knowledge base rules.

All functionality is available from the main program window (Figure 7). The user has to press the "Scan ontology" button and specify the path to the ontology file.

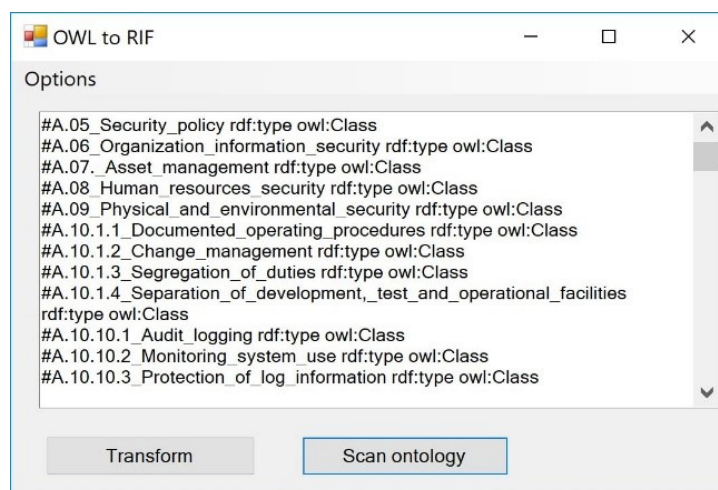


Figure 7: The program user interface

Ontology scanning engine imports (Figure 6) the ontology from the external .xml file of OWL/XML format. The program later performs the automatic scanning of elements, extraction

of OWL RL subset and performs conversion to RDF triplets. The results are shown in the main window. User, after reviewing the intermedium data and the list of errors, can press the "Transform" button. After that, RDF triplets are transformed to RIF rules and presented for user review. User can copy them or to save via program interface into the specified file.

User interaction is needed to initiate ontology imports and transformation processes. Program was tested with several ontologies: W3C consortium test ontologies [51], cloud security ontology [20] which is used in practice and information security standards ontology [36]. While W3C and Cloud security ontologies were developed by external parties, the Information security standards ontology was developed at Vilnius Gediminas Technical University in accordance with the formal OWL 2 RL rules defined in [11] and OWL 2 Full defined in [50]. Its presentation and in-depth description with verification was provided in [36].

All tested ontologies were relatively small (up to 1000 elements). The proportional size of the RL subset in ontologies used in tests was equal to 100% in case of W3C testing ontologies, and 65% - in case of Information security standards ontology. The proportion of the OWL RL subset in the case of Cloud security ontology was not analyzed. Execution time has not exceeded 50 ms (test platform: Intel Core i7-4710HQ 2.50 GHz, 8 CPU, 16GB RAM, Windows 8.1 OS). There were 15 ontologies at all. Results are shown in Table 1.

Table 1: Transformation results

Ontology	The part of successfully transf. rules
W3C testing ontologies, compatible OWL RL	90%
Cloud computing security ontology	64%
Information security standards ontology	60%

As can be seen from the transformation results, not all ontology elements were transformed. Some elements cannot be transformed into separate rules because they are just a part of other element or additional information. The best transformation result was achieved with test ontologies, that are based on the OWL RL profile. Specific security ontologies had shown worse results. In the case of the Information security standards ontology data types *xsd.real* and *xsd.rational* have caused 15% of unsuccessful conversion, 20% were caused by *SubClassOf* elements and 5% by other *xsd* data types. General method applicability was approved, since the transformation of even 60% can drastically decrease the knowledge base creation time.

For further verification purposes, the generated rules were integrated into the JESS-based prototype risk analysis ES, adapted for SMEs (enterprise size definition is adopted by EU recommendation 2003\361). This part of ES knowledge base was developed using traditional knowledge base development methods and included rules for identification of appropriate assets, calculating impact and probabilities based on the environment of a specific company (infrastructure, maturity level, environment, sector, etc.), while rules generated automatically from the ontology mainly included information on appropriate security controls.

According to ISO 27001, information security risk is defined as a potential that some threat exploits an asset or assets group vulnerability and thus undermine the enterprise. Risks management process's purpose is to identify such risks, assess the likelihood of their occurrence and then take actions to reduce them to the acceptable level. Almost all risk analysis processes use the same method: identifying assets; identifying problems, threats, vulnerabilities; assessing risk likelihood and impact for assets [6]. After the risk analysis process, the user has to decide how to reduce risks; therefore, ES should not only evaluate risks, but also give some recommendations based on the acceptable risk level.

5 Conclusions and future work

The increasing demand for information security compliance and overall understanding of information security management importance leads a modern company to a need of a systematic risk management process. The use of expert systems for risk analysis is seen by many authors as a possible solution. Still, the development of expert systems is also a complicated and expensive task, and we indicate it as unsolved problem. Advantage of our method is that development of knowledge base can be partially simplified by using already available knowledge sources. Some earlier attempts by other authors were made to perform direct integration of security ontologies, that can be seen as a valuable source of information for expert systems knowledge base, with expert systems, but they lacked flexibility.

In this paper the new method was proposed that allows automatic transformation of existing information security ontologies into the expert system knowledge base ruleset. Information security standards ontology transformation into the JESS ES was implemented in several steps with the help of a developed tool: OWL RL subset of ontology elements are segregated into RDF triplets, that are later transformed into RIF format that can be easily converted into JESS knowledge bases rules with the help of external tool. The method supports the most popular OWL/XML format. Both simple (unlined) and complex (linked) OWL RL elements can be transformed. The biggest method advantage is that although ontology typically has a very sophisticated structure, it can be easily represented in the form of RDF triplets. The conversion test with different ontologies (W3C testing ontologies, "Cloud computing security ontology" and "Information security standards ontology" [36]) have shown 60-90% conversion success rate, that proves general method applicability, since automatic generation of even part of expert system knowledge base can decrease the general expert system development price. Verification of generated rules was performed by their integration with the knowledge base of a developed JESS-based expert system for risk analysis in SME. The obtained results have shown high correlation rate, but what is more important is that the generated rules were successfully integrated into the ES knowledge base.

Later research should be concentrated on tuning the conversion templates for achieving higher conversion success rates of ontologies and finding other sources for automatic filling of the ES knowledge base. Currently, we see the CVE (Common Vulnerabilities and Exposures) and attack trees as the next perspective sources for technical risk evaluation. Combination of these two structured sources should provide information on relevant threats as well as probabilities of different attack scenarios.

Funding

This research received no external funding.

Author contributions. Conflict of interest

The authors contributed equally to this work. The authors declare no conflict of interest.

Bibliography

- [1] Abbas, A.; Privat, G. (2018). Bridging Property Graphs and RDF for IoT Information Management, *SSWS@ ISWC*, 77–92, 2018.
- [2] Abraham, A. (2005). *Rule-Based expert systems. Handbook of measuring system design*, John Wiley and Sons, New York, USA, 2005.

-
- [3] Akerkar, R.A.; Sajja, P.S. (2010). *Knowledge-based systems*, Jones & Bartlett Publishers: Toronto, Canada, 2010.
- [4] Atymtayeva L.; Kozhakhmet K.; Bortsova G. (2014). Building a Knowledge Base for Expert System in Information Security, *Soft Computing in Artificial Intelligence. Advances in Intelligent Systems and Computing*, Springer, Cham, 57-76, 2014.
- [5] Benta, D.; Rusu, L.; Manolescu, M.J. (2017). Workflow Automation in a Risk Management Framework for Pavement Maintenance Projects, *International Journal of Computers Communications & Control*, 12(2), 155-165, 2017.
- [6] Blackley, J.; Peltier. (2015). *Information Security Risk Analysis*, CRC Press: New York, USA, 2015.
- [7] Blanco, C.; Lasheras, J.; Valencia-García, R.; Fernandez-Medina, E.; Toval, A.; Piattini, M. (2008). A systematic review and comparison of security ontologies, *Availability, Reliability and Security, ARES 08. Third International Conference on IEEE*, 813-820, 2008.
- [8] Bova, V.V.; Kureichik, V.V.; Lezhebokov, A. (2014). The integrated model of representation of problem-oriented knowledge in information systems, *2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT)*, 1-4, 2014.
- [9] Brank, J.; Grobelnik, M.; Mladenic, D. (2005). A survey of ontology evaluation techniques, *Proceedings of the conference on data mining and data warehouses (SiKDD 2005)*, 166-170, 2005.
- [10] Butaci, C.; Dzitac, S; Dzitac, I; Bologa, G. (2017). Prudent decisions to estimate the risk of loss in insurance, *Technological and Economic Development of Economy*, 23(2), 428-440, 2017.
- [11] Cao, S. T.; Nguyen, L. A.; Szalas, A. (2011). On the Web ontology rule language OWL 2 RL, *International Conference on Computational Collective Intelligence*, Springer, 254-264, 2011.
- [12] Classically, I. (2010). Performing a Security Risk Assessment, *ISACA Journal*, 1, 1-7, 2010.
- [13] Dahouk, A. W.; Abu-Naser, S. S. (2018). A Proposed Knowledge Based System for Desktop PC Troubleshooting, *International Journal of Academic Pedagogical Research*, 2(6), 1-8, 2018.
- [14] Daraio, C.; Lenzerini, M.; Leporelli, C.; Naggari, P.; Bonaccorsi, A.; Bartolucci, A. (2016). The advantages of an Ontology-Based Data Management approach: openness, interoperability and data quality, *Scientometrics*, 108(1), 441-455, 2016.
- [15] de Rosa, F.; De Gloria, A.; Jousselme, A. L. (2019). Analytical games for knowledge engineering of expert systems in support to Situational Awareness: The Reliability Game case study, *Expert Systems with Applications*, 138, 112800, 2019.
- [16] Dzitac, I.; Barbat, B. E. (2009). Artificial intelligence+ distributed systems= agents, *International Journal of Computers Communications & Control*, 4(1), 17-26, 2009.
- [17] Fenz, S.; Plieschnegger, S.; Hobel, H. (2016). Mapping information security standard ISO 27002 to an ontological structure, *Information & Computer Security*, 24(5), 452-473, 2016.

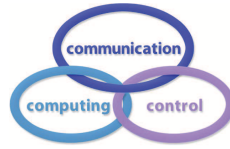
- [18] Gruber, T. (2008). Collective knowledge systems: Where the social web meets the semantic web, *Web semantics: science, services and agents on the World Wide Web*, 6(1), 4-13, 2018.
- [19] Islam, M. S.; Nepal, M. P.; Skitmore, M.; Kabir, G. (2019). A Knowledge-based Expert System to Assess Power Plant Project Cost Overrun Risks, *Expert Systems with Applications*, 138, 12-32, 2019.
- [20] Janulevicius, J.; Marozas, L.; Cenys, A.; Goranin, N.; Ramanauskaite, S. (2017). Enterprise architecture modeling based on cloud computing security ontology as a reference model, *2017 Open Conference of Electrical, Electronic and Information Sciences (eStream)*, IEEE, 1-6, 2017.
- [21] Joseph, K.; William, R. (2003). DAMLJessKB: A Tool for Reasoning with the Semantic Web, *IEEE Intelligent Systems*, 18, 74-77, 2003.
- [22] Kaminski, J. (2014). *Nursing Decision Support and Expert Systems & Artificial Intelligence*, [Online]. Available: <http://www.nursing-informatics.com/>, Accessed on 03 March 2019.
- [23] Katz, Y.; Grau, B.C. (2005). Representing qualitative spatial information in OWL DL, *Proceedings of the First International Workshop: OWL Experiences and Directions*, Galway, Ireland, 2005.
- [24] Kidd, A. (1987). Knowledge Acquisition - An Introductory Framework, *Knowledge acquisition for expert systems: A practical handbook*, Plenum Press: New York, USA, 5 - 15, 1987.
- [25] Kim, S.K.; Lim, S.; Mitchell, R.B. (2008). A method for knowledge modeling with unified modeling language (UML): Building a blueprint for knowledge management, *Current Issues in Knowledge Management*, IGI Global: Paris, France, 228-242, 2008.
- [26] Knublauch H. (2002). *A method for knowledge modeling with unified modeling language (UML): Building a blueprint for knowledge management*, PhD thesis, University of Ulm, 2002.
- [27] Kontopoulos, E.; Martinopoulos, G.; Lazarou, D.; Bassiliades (2016). An ontology-based decision support tool for optimizing domestic solar hot water system selection, *Journal of Cleaner Production*, 112, 4636-4646, 2016.
- [28] Kozhakhmet, K.; Bortsova, G.; Inoue, A.; Atymtayeva, L. (2016). Expert System for Security Audit Using Fuzzy Logic, *Proceedings of the 23rd Midwest Artificial Intelligence and Cognitive Science Conference (MAICS2012)*, 146-151, 2016.
- [29] Ma, X.; Zhan, J.; Ali, M. I.; Mehmood, N. (2018). A survey of decision making methods based on two classes of hybrid soft set models, *Artificial Intelligence Review*, 49(4), 511-529, 2018.
- [30] Maldoff G. (2017). *The Risk-Based Approach in the GDPR: Interpretation and Implications*, [Online]. Available: https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf, Accessed on 03 March 2019.
- [31] Mas, S.; Wang, F.; Reinhardt, W. (2005). Using ontologies for integrity constraint definition, *Proceedings of the 4th international symposium on spatial data quality*, 25-26, 2005.

- [32] Meditskos, G.; Bassiliades, N. (2008). Combining a DL Reasoner and a Rule Engine for Improving Entailment-Based OWL Reasoning, *International Semantic Web Conference*, Karlsruhe, Germany, 277-292, 2008.
- [33] Obrst, L.; Chase, P. (2012). On Developing an Ontology of the Cyber Security Domain, *Proc. of the 7-th International Conference on Semantic Technologies for Intelligence, Defense and Security*, Fairfax, USA, 49-56, 2012.
- [34] Otero-Cerdeira, L.; Rodriguez-Martinez, F.J.; Gomez-Rodriguez, A. (2015). Ontology matching: A literature review, *Expert Systems with Applications*, 42.2, 949-971, 2015.
- [35] Rainer, R.K.; Cegielski, C.G.; Splettstoesser-Hogeterp, I.; Sanchez-Rodriguez, C. (2014). Information Systems within the Organization, *Introduction to information systems. Supporting and Transforming Business*, 3rd ed., John Wiley & Sons: Toronto, Canada, 2014; 227-228, 2014.
- [36] Ramanauskaite, S.; Olifer, D.; Goranin, N.; Cenys, A. (2013). Security ontology for adaptive mapping of security standards, *International Journal of Computers Communications & Control*, 8(6), 878-890, 2013.
- [37] Reynolds, D. (2010). OWL 2 RL in RIF, *W3C Working Group Note*.
- [38] Rick, U.; Vossen, R.; Richert, A.; Henning, K. (2010). Designing agile processes in information management, *2010 2nd IEEE International Conference on Information Management and Engineering*, 156-160, 2010.
- [39] Sicilia, M.A.; Garcia-Barriocanal, E.; Bermejo-Higuera, J.; Sanchez-Alonso, S. (2015). What are information security ontologies useful for?, *Research Conference on Metadata and Semantics Research*, Springer, Cham, 51-61, 2015.
- [40] Slimani, T. (2015). Ontology development: A comparing study on tools, languages and formalisms, *Indian Journal of Science and Technology*, 8(24), 1-12, 2015.
- [41] Spatti, D. H., Liboni, L., Flauzino, R. A., Bossolan, R. P., Vitti, B. C. (2019). Expert System for an Optimized Asset Management in Electric Power Transmission Systems, *Journal of Control, Automation and Electrical Systems*, 30(3), 434-440, 2019.
- [42] Sun, N.; Zhang, J.; Rimba, P.; Gao, S.; Zhang, L. Y.; Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey, *IEEE Communications Surveys & Tutorials*, 21(2), 1744-1772, 2018.
- [43] Tommasini, R.; Bonte, P.; Della Valle, E.; Ongenaes, F.; De Turck, F. (2018). A Query Model for Ontology-Based Event Processing over RDF Streams, *European Knowledge Acquisition Workshop*, Springer, Cham, 439-453, 2018.
- [44] Tsudik, G.; Summers, R. C. (1990). AudES-An Expert System for Security Auditing, *IAAI*, 221-232, 1990.
- [45] Van Woensel, W.; Abidi, S. S. R. (2018). Optimizing semantic reasoning on memory-constrained platforms using the RETE algorithm, *European Semantic Web Conference*, Springer, Cham, 682-696, 2018.
- [46] Webb, J.; Ahmad, A.; Maynard, S.B.; Shanks, G. (2014). A situation awareness model for information security risk management, *Computers & security*, 44, 1-15, 2014.

- [47] Willcocks, L. (1994). *Information management: the evaluation of information systems investments*, 1st ed. Springer Science & Business Media: Oxford University, United Kingdom, 219-225, 1994.
- [48] Yazdani, M.; Alidoosti, A.; Zavadskas, E.K (2011). Risk analysis of critical infrastructures using fuzzy COPRAS, *Economic research-Ekonomska istrazivanja*, 24(4), 27-40, 2011.
- [49] Yu, L. (2011). *A developer's guide to the semantic Web*, Springer Science & Business Media: Oxford University, United Kingdom, 2011.
- [50] *OWL 2 Web Ontology Language Structural Specification and Functional-Style Syntax (Second Edition)*, [Online]. Available: <https://www.w3.org/TR/owl2-syntax/>, Accessed on 03 March 2019.
- [51] *W3C OWL 2 Web Ontology Language Conformance (Second Edition)*, [Online]. Available online: https://www.w3.org/TR/owl2-conformance/#Test_Cases, Accessed on 03 March 2019.

Identification of Opinion Spammers using Reviewer Reputation and Clustering Analysis

M.J. Zhong, L.Tan, X.L. Qu



Minjuan Zhong*

School of Information Technology
Hunan University of Finance and Economics
Changsha 410205, China
*Corresponding author: lucyzmj@sina.com

Liang Tan

School of Information Management
Jiangxi University of Finance and Economics
Nanchang 33013, China
ghosticy@foxmail.com

Xilong Qu

School of Information Technology
Hunan University of Finance and Economics
Changsha 410205, China
quxilong@126.com

Abstract: Online reviews have increasingly become a very important resource before making a purchasing decisions. Unfortunately, malicious sellers try to game the system by hiring a person or team (which is called spammers) to fabricate fake reviews to improve their reputation. Existing methods mainly take the problem as a general binary classification or focus on some heuristic rules. However, supervised learning methods relies heavily on a large number of labeled examples of deceptive and truthful opinions by domain experts, and most of features mentioned in the heuristic strategy ignore the characteristic of the group organization among spammers.

In this paper, an effective method of identifying opinion spammers is proposed. Firstly, suspected spammers are detected by means of unsupervised learning based on reviewer's reputation. We believe that the reviewer's reputation has a direct relation with the quality of reviews. Generally, review written by user with lower reputation, shows lower quality and higher possibility to be fake. Therefore, the model assigns reputation score to each reviewer wherein the content based factors and activeness of reviewers are employed efficiently. On basis of all suspected spammers, k-center clustering algorithm is performed to further spot the spammers based on the observation of burst of review release time.

Experimental results on Amazon's dataset are encouraging and indicate that our approach poses high accuracy and recall, and good performance is achieved.

Keywords: opinion spammer, fake review, reviewer reputation, clustering analysis.

1 Introduction

The rapid development of online shopping has led to a large number of user reviews for various products or services. More and more potential consumers tend to rely on them to assess

the quality of goods or services before buying. Therefore, driven by the desire for profit or competition, producer and retailers generate motivations and behaviors to manipulate reviews, maliciously posting deceptive or fake reviews to deliberately mislead potential consumers and make their risky purchasing decisions. Moreover, for the purpose of high satisfaction rate and reputation, manufactures may hire a person (known as an individual spammer) or team (known as spammer group) to post glamorized positive on their product or harmful negative reviews on their competitor as consumers. Hu Nan et al. [7] conducted research on the website reviews of two major US bookstores, Amazon.com and Barnes & Noble, and found that a large number of comments on the website were manipulated by publishers and vendors; Michael Luca and Georgios Zervas analyzed [14] that 16% of the comments on the Yelp website are deceptive; China's e-commerce websites, such as Taobao and Jingdong Mall also acknowledge that there are a large number of fake reviews on their e-commerce platforms.

Studies have shown that the discrimination of such deceptive reviews by ordinary consumers is relatively low and the task of opinion spam or spammers detection is a very challenging problem. For example, consider figure 1 (a) and (b), which illustrates two reviews written by two users for a product from Amazon.

If we only look at the two reviewers individually, they all appear genuine. However, when we collect them together, we could find easily that both reviews are duplicated. From the publication time of the review, it seems likely that the first user copies the review made by the second user. Remarkably, there are ten other users to read and make feedback on this review written by the first user, and two people thought it was a useful review. Obviously, genuine users are unable to judge whether a review is a fake review or not, and whether a reviewer is a spammer or not.

[A2HP9COIPKXQ1I][August 20, 2003][2][10][1.0][Not as good as the Scorpions.] Yanni fans and others have come to expect from him "music" that provokes landscape images, religious symbolism, and cultural...ZZZZZ ZZZZZZZZZZ. Anyway, the fact is his music has never been the same since his departure from german rock band, the Scorpions. His presence was felt on a few early recordings and fans may have noticed the difference upon its absence. Yanni has completely left behind all previous styles and taken on a new identity in the world music genre. The Album is over the top and over long and will definitely take you into another realm - one in which you may not want to be - So Yanni heads will appreciate it. The only really unique aspect of Acropolis is the out of place appearance of Rob Halford (Judas Priest). I would really like to know how he agreed to appear on it. The unknown Twisted Sister cover song is absent once again - It may not even exist on bootleg. Yanni fans will like this but if you know his metal roots its a little hard to take in. ↵

(a) The first candidate fake reviews

[AOCJ3A12C91U5][May 23, 2001][1][7][1.0][Not as good as the Scorpions.] Yanni fans and others have come to expect from him "music" that provokes landscape images, religious symbolism, and cultural...ZZZZZ ZZZZZZZZZZ. Anyway, the fact is his music has never been the same since his departure from german rock band, the Scorpions. His presence was felt on a few early recordings and fans may have noticed the difference upon its absence. Yanni has completely left behind all previous styles and taken on a new identity in the world music genre. The Album is over the top and over long and will definitely take you into another realm - one in which you may not want to be - So Yanni heads will appreciate it. The only really unique aspect of Acropolis is the out of place appearance of Rob Halford (Judas Priest). I would really like to know how he agreed to appear on it. The unknown Twisted Sister cover song is absent once again - It may not even exist on bootleg. Yanni fans will like this but if you know his metal roots its a little hard to take in. ↵

(b) The second candidate fake reviews

Figure 1: Two product reviews from Amazon.com

In fact, the opinion spam and spammers are closely related. The reviews written by the

spammers are fake reviews to a large extent, and correspondingly, the author of a fake review must be a spammer. Therefore, many researchers have developed detection techniques combination the fake reviews with spammers together and solved them by means of binary classification problem(spam vs. non-spam, spammer vs non-spammer). As we all known, the classification algorithm is a supervised learning method that requires large sets of pre-labeling instances. However, the task of pre-labeling both classes, deceptive and truthful opinions is difficult and time-consuming. The biggest problem is the authenticity of the labeled opinions.

In this paper, we propose an unsupervised method for detecting opinion spammers. This research makes the following main contributions:

(1)It introduces the concept of reputation and proposes a reviewers' reputation model to detecting spammers. The model can capture the suspected spammers with low reputation value by analyzing both content-based characteristics(context similarity, opinion sentiment, review length and helpful feedback) and behavior-based characteristics (authors' activeness, review deviation and rating) without requiring a large sets of labeled instances.

(2)Clustering technique is further performed to spot accurately spammers. Generally, spammers will post their reviews intensively. This behavior shows the characteristics of abruptness in posting time interval. Consequently, users' posting time interval is proposed to measure the similarity and on basis of all suspected spammers, k-center clustering algorithm is implemented to filter spammers.

(3)We conduce the experiments on the Amazon review dataset. The experimental results are encouraging and indicate that our approach poses high accuracy and recall, and good performance is achieved.

The rest of the paper is organized as follows: the next section discusses some relevant literature on opinion spammers detection. Section 3 describes our user reputation model to the task of suspected spammers detection. Section 4 presents the clustering algorithm for the spammers spotting. Experimental results and analysis are discussed in section 5. Finally, section 6 presents our conclusions and discusses some future work directions.

2 Related work

Detection of opinion spam was first introduced by Jindal N. and Liu B. They conduced a series of studies for automatically detecting review spam [8], spammers [11] and spammer group [15] by machine learning, pattern recognition, graph theory and other techniques.Yuanchao [13] summarized previous detection approach as supervised or unsupervised learning.

Most existing supervised learning methods, which is mainly based on text content, regard the detection of opinion spam as classification process. Combing psychology and computational linguistics to extract the linguistic content cues of the reviews, supervised learning methods applied neural network [16], decision tree [4] and other classifiers to establish a statistical model and then predict the unknown reviews [6].

In text content, repeated review is considered to be important clue for the identification of fake review. In order to find duplicate and near duplicate reviews, Lin et al. [12] defined three similarities, including similarity of reviews written by the same reviewer, similarity between reviews in the target product, and similarity of reviews between different categories of products.

Lau [9] established language model to identify conceptual duplicate reviews.

However, this kind of opinion spam only represents a small percentage of the opinion spam. So, other linguistic features have also received much attention [2].

Rupesh et al. [3] proposed new lexical and syntactic features including type of punctuation mark, Part-of-Speech (POS) etc and applying supervised algorithms,such as SMO, Decision

Tree, and Naive Bayes for performing classification on fake reviews dataset. The final results give promising accuracy 91.51% for detecting fake reviews.

Banerjee and Chua [1] distinguished between deceptive and genuine reviews from following aspects: the readability of a review, the richness of describing the objective information in review, the writing style of reviews, and review genre. On basis of these features, they built logistic regression model to detect opinion spams.

Wen et al. [19] proposed a two-view collaborative filtering approach based on SVM benchmark to identify opinion spams. In their work, two different expressions are used for each review. One is the lexical terms derived from the textual content of the reviews and the other is the PCFG rules derived from a deep syntax analysis of the reviews. The statistical differences between deceptive and truthful opinions are observed from above two different perspectives. On basis of them, CoSpa-C and CoSpa-U strategies are proposed for classifier training to identify fake and true reviews.

The challenge for the existing supervised classification algorithms is that manually marking massive ground truth spam reviews is difficult and time-consuming. Therefore, another detection approach, unsupervised learning, has been proposed and tended to focus on the opinion spammers or group by relying on behavioral reviewers features. For example, Savage Z. et al [17] find that the reviews of opinion spammers tend to give extreme evaluation scores.

Vlad and Martin [18] conducted detection on Singletons reviewers in fake reviews, who registered multiple names deliberately, posting each review under a different name. They made an important assumption: singleton reviewers is lack of complete imagination and are not able to rewrite each review completely. They prefer to rephrasing, switching some synonyms, and keeping the sentiment consistency to all reviews. So, semantic similarity has been measured from the perspective of terms and topic distribution, and meanwhile singleton reviewers have been identified indirectly.

In Atefeh Heydari et al.'s work [5], suspicious time intervals are captured from the sudden rapid increase in the number of the reviews. The reviews in suspicious time are analyzed combining the rating deviation, content similarity and activeness of reviewers, which is beneficial to the time efficiency due to narrowing the detection range.

David S. et al. [?] used binomial regression to identify those reviewers with an abnormal rating for products. The proposed method stemmed from overarching assumption that the majority of reviews are posted by truthful reviewers. Therefore, the method does not pay attention to the text-based features, but focused merely on the rating differences between spammers and the majority of truthful reviewers.

With an in-depth study on features of fake reviews, Lijing et al. [10] introduced the concept of user-credibility and shop-credibility, and established a fake review identification model, which integrated the reviewer's behaviour characteristics, businesses characteristics and review texts.

In the above method, the supervised learning technique focuses on analyzing the review text, and uses the natural language processing technology to extract the part of speech, grammar, sentiment and other features of the review text to distinguish the authenticity of the content. However, this method heavily depends on a large number of labeled examples of fake and truthful opinions by domain experts, which is a time-consuming and costly endeavour. The unsupervised recognition method does not need to mark a large amount of training corpus, but the problem of low recognition rate is generally found. Furthermore, most of the heuristic features proposed in the existing methods are based on individual opinion spammer, ignoring the characteristics of group review spamming. Therefore, the current identification of opinion spam has not yet formed an effective solution.

3 Feature representation

For detecting the fake reviews, the first thing is defining the features. In this paper, we mainly considered two scopes of features to indicate spamming activities, one is user's review content features and one is user's behavioral features.

Suppose there is a review sequence $R_p = r[1], r[2], \dots, r[n]$ for a product p , where $r[i]$ is a review sorted by time arrival and contains a variety of information, such as user name $r[i].u$, release time $r[i].t$, review rating $r[i].r$, review title $r[i].title$ and review content $r[i].content$ etc.

3.1 Review content features

Spammers usually consider the following factors while writing fake review: first, to generate a review as quickly as possible and second, to express their emotions as strongly as possible to promote or demote a product. Therefore, we employ following criteria to score reviews to detect users with low reputation:

(1) Duplicate of target review

In order to generate more reviews and get more economic benefits as soon as possible, spammers often copy the text of existing reviews or make minor changes for the same or different target products. For example, they posted the same review to express different products, or just changed the product name. We can judge whether the target review is a duplicate review by measuring their similarity with other reviews from dataset. Due to the large number of reviews in dataset, the similarity is based on the following two cases:

- ① Duplicated reviews on the same user id in different products.
- ② Duplicated reviews for different user id of the same product.

Corresponding to above two cases, we consider two copy behaviors separately. One is to copy his/her own previous reviews and the other is to copy the reviews written by other users on the same product.

① Review similarity between the same user id (*User_Similarity*)

Review similarity between the same users is used to determine whether the user of the target review copied his/her own previous reviews. Therefore, the similarity is calculated between the target review and each of his/her own previous reviews, and choose the largest similarity as *User_Similarity*.

$$User_Sim(r[i].u) = Max(Similarity(r[i], r[j])) \quad (1)$$

Where $r[i]$ indicates the target review, $r[j]$ indicates the j th review of his/her own previous reviews. The similarity is calculated by using the cosine formula of vector space model.

② Review similarity between the same product (*Production_Similarity*)

Review similarity between the same product is used to judge whether a target review is a copy of another user's reviews on the same product. Also, we can calculate the similarity of a target review and the rest of reviews for the same product by other users, and choose the largest similarity as *Production_Similarity*.

$$Production_Sim(r[i].u) = Max(Similarity(r[i], r[k])) \quad (2)$$

Where $r[i]$ indicates the target review, $r[k]$ indicates the k th review by other users on the same product. Similarity is calculated by the same cosine formula of vector space model.

Duplicated score of review is determined by the above both user_similarity and production_similarity.

$$Duplicated_Score(r[i].u) = 1 - (0.5 * User_Sim(r[i].u) + 0.5 * Production_Sim(r[i].u)) \quad (3)$$

(2) Review opinion

Generally, spammers tend to express strong emotional tendencies to promote or demote some target product while writing reviews, and their sentiment polarity tends to be closer to the poles, i.e, extremely strong or very weak. Conversely, genuine reviews are more likely to be closer to the middle of variance distributions.

$$O_Score(r[i].u) = \begin{cases} 0, & \text{if } Sen_Value(r[i]) > \tau \text{ or } Sen_Value(r[i]) < -\tau \\ |Sen_Value(r[i])|, & \text{otherwise} \end{cases} \quad (4)$$

Where $O_Score(r[i])$ indicates sentiment tendency of the target review $r[i]$, τ is the threshold value which denotes the emotion polarity beyond which reviews expressed are thought to be suspicious.

The sentiment value of the target review is a challenge work. We firstly extracted the opinion word by using association rule mining. After that, original polarity of the opinion word was obtained based on PageRank model combined with mixture relevance relation. Finally, both the location of the opinion word and the context of modified information were taken into account to complete the task of the sentiment analysis of the target review. Furthermore, a greedy hill climbing search to learn τ is performed and the final estimated value is 0.758.

(3) Personal expression

Through the careful observation of the reviews, we find that the personal expression also has an implicit role for judging whether a user is a spammer. While producing a genuine review, user often express their experiences in the form of the first person to all aspects of the product. For instance, often we see such reviews, "After reading a lot of very negative review on this album, I thought I should hate this album, but I love it and it's hard to say why.", "I love her lyrics and I love the songs and what can I say she has a unique voice which I think is hot and very cool!!!", etc.,. However, there are some sentences that use the "you", "you should...." and others to express, in order to recommendations or guide other consumers how to do. By this, we think such reviews are very suspicious. We can use the proportion of the first-person pronoun appeared in reviews, "I", "my", "me", "we", "us", "our", and the second-person pronouns "you", "your" to examine target reviews.

$$PersonExpre(r[i]) = \frac{FirstPerson_Num(r[i])}{SecondPerson_Num(r[i])} \quad (5)$$

Where $FirstPerson_Num(r[i])$ indicates the number of the first-person pronouns in the target review $r[i]$, $SecondPerson_Num(r[i])$ indicates the number of the second-person pronouns in the target review $r[i]$. To facilitate the comparison, we take a normalized value as the final Personal Expression Feature value ($NormalPersonalExpressionScore, NPE_Score$).

$$NPE_Score(r[i]) = \frac{PersonExpre(r[i])}{Max(PersonExpre(r[i]))} \quad (6)$$

(4) Review length

Users tend to write review of appropriate length to express his/her true feelings about the use of product. Too long or too short are likely to be suspicious. Spammers sometimes deliberately write longer reviews to get more consumers' attention, and thus get more helpful feedback from consumers. Meanwhile, too short reviews often cannot clearly express the user's true feelings. Therefore, spammers sometimes simply use a few simple words to express, such as "good" or "bad" and so on.

$$RL_Score(r[i].u) = \begin{cases} 0, & \text{if } NRLength(r[i]) > \xi_1 \text{ or } NRLength(r[i]) < \xi_2 \\ NRLength(r[i]), & \text{otherwise} \end{cases} \quad (7)$$

Where $NRLength(r[i])$ indicates normalized length of the target reviews (Normal Review Length, NRL), which is calculated as follows:

$$NRLength(r[i]) = \frac{|r[i]|}{Max(|r[k]|)} \quad (8)$$

$|r[i]|$ indicates the number of words in the target review. ξ_1 and ξ_2 are the parameters which denote the length beyond/below which reviews posted are considered to be suspicious. Similarly, a greedy hill climbing search to learn ξ_1 and ξ_2 was performed and in our subsequently experimental environment, the final estimated values were $\xi_1=0.82, \xi_2=0.18$.

(5) Helpful Feedback

Before making a purchase, users tend to look over the reviews from the other customers, and feedback it by marking that whether a review is helpful to their purchase. Naturally, we believe that the more positive feedback on a review is, the higher quality of it, and the lower probability of becoming a fake review, and meanwhile the lower probability of the reviewer becoming spammer. Consequently, helpful feedback could be:

$$HRF_Score(r[i]) = \frac{Helpful_FeedNum(r[i])}{FeedNum(r[i])} \quad (9)$$

Where $Helpful_FeedNum(r[i])$ indicates the number of users who believe the target review $r[i]$ is helpful to their purchase and feedback them after reading. $FeedNum$ represents $(r[i])$ the number of all feedback review for the target $r[i]$.

3.2 Reviewer behavior features

Some of specific behavior of reviewer also has certain relevance with spammers. So, we examine fake reviewers from the following three behavioral characteristics.

(1) User Activity

Spammers usually tend to register multiple different user accounts on multiple forums or websites. When they accept a new task, they may use the newly registered user id to write and publish fake reviews. Until it is completed, they give them up. Accordingly, user's activity will be a critical aspect for detecting spammers. The activity score can be measured by examining whether the user id has release review on other products at other time.

The value could be computed as:

$$UA_Score(r[i].u) = \frac{tf(r[i].u)}{\sum_{j=1}^{tf(r[i].u)} T(r[j].t, r[j+1].t)} \quad (10)$$

Where $tf(r[i].u)$ indicates the number of reviews written by the user $r[i].u$, $r[j].t$ refers to the release time of $r[j]$, $T(x, y)$ is the time interval between the two reviews x and y . It is important to note that when the user id of target review does not submit their review on other products at other time, the interval is considered to be infinite.

(2) Review Deviation

Many e-commerce sites usually provide review ratings of product. Assuming 5-star rating system, 1 star is the lowest level, indicating that the sentiment of customer for the product is the most negative; whereas 5 star represents the highest level, indicating that the product is most satisfactory and the review is belong to the positive reviews. Therefore, the spammers tend to raise or suppress the target product or brand by rating. For example, a user post a negative reviews about a product, while others wrote positive reviews on the same product. In this case, the reviewer is more likely to be spammer.

Or the user's reviews on a series of brand products are positive, representing that the reviewer is highly suspected as spammer. Given a set of *ratings* $\{r[j].r, r[j+1].r, \dots, r[m].r\}$ allocated to a product p by reviews, the deviation of a review is measured between the rating value and the normal value:

$$RD_Score(r[i].u, R_p) = \frac{r[i].r - Avg(r[j].r, r[j+1].r, \dots, r[m].r)_{(j=1,2,\dots,m)\wedge j\neq i}}{Avg([r[j].r, r[j+1].r, \dots, r[m].r])_{(j=1,2,\dots,m)\wedge j\neq i}} \quad (11)$$

Where $r[i].r$ indicates posted rating by the user $r[i].u$, $Avg(\square)$ denote the average of review sequence R_p (not containing the target review $r[i]$ for product p).

(3) Other rating score

According to the 5-star rating systems, ratings can be divided into three levels: ① Good (Rating ≥ 4); ② bad (Rating ≤ 2.5); ③ average ($2.5 \leq \text{Rating} \leq 4$). Therefore, a customer's review ratings for products mainly belong to the following four conditions: ① all good or bad; ② some good and other average; ③ some bad and other average; ④ some good, some bad and some average. If the review ratings for other products are all fallen in the first category, it is the most feasible possibility that the reviewer is a spammer. Using the following formula to calculate the proportion of three levels.

$$\begin{aligned} GoodRatio(r[i].u) &= \frac{ReviewNum_{good}}{TotalNum} \\ BadRatio(r[i].u) &= \frac{ReviewNum_{bad}}{TotalNum} \\ AveRatio(r[i].u) &= \frac{ReviewNum_{average}}{TotalNum} \end{aligned} \quad (12)$$

According to the scale of three levels, the score of the reviewer's behavior is judged by formula (13).

$$OR_Score(r[i].u) = \begin{cases} 0, & \text{if } GoodRatio(r[i].u)=1 \text{ or } BadRatio(r[i].u)=1 \\ Max(GoodRatio(r[i].u), BadRatio(r[i].u), AveRatio(r[i].u)), & \text{otherwise} \end{cases} \quad (13)$$

4 Proposed methodology

4.1 Reviewer reputation model for suspected spammers detection

Reputation refers to the extent of one user access to public trust, favor, and popularity, mainly focusing on qualitative evaluation. In the product reviews, each customer is allowed to present and share their own opinions for product quality, performance and price. We believe that the reviewer's reputation has a direct relation with the quality of reviews.

Consequently, the proposed method for detecting opinion spammers stems from two overarching assumptions regarding reviewer reputation:

(1) Review, written by user with lower reputation, shows lower quality and higher possibility to be fake. Consequently, with higher probability, the reviewer is spammer;

(2) if one customer has high reputation, his/her reviews are high quality, and are more helpful to others. Therefore, the user's reputation could be measured to detect suspicious spammers.

By modeling both the content of reviews and behavior of the reviewer, we propose eight features to describe the reputation of the reviewer and show the likelihood of the reviewer being

spammer from different aspects. Let reviewer's reputation was graded over [0,1]. Values close to 0 signify low reputation for reviewer and greater extent to which user are marked spammers. Similarly, Values close to 1 signify high reputation for reviewer and greater extent to which users are genuine. Therefore, if the eight normalized values of a targeted reviews are lower, the lower reputation value of the reviewer, and the greater the probability of becoming the fake reviewer is. Conversely, the higher the eight normalized values is, the higher the value of reputation of the reviewer, and the greater the likelihood of becoming a real user is. Hence, detection indicators are then used to score each reviewer and the value of reviewer's reputation will be:

$$Reputation_Value(r[i].u) = \alpha_1 * Content_Features(r[i].u) + \alpha_2 * Behavior_Features(r[i].u) \quad (14)$$

Where $Content_Features(r[i])$ indicates content characteristics of the target review $r[i]$ and include various indicators described in section 3.1. Similarly, $Behavior_Features(r[i].u)$ refers to behavioral characteristics of the reviewer who wrote the target review $r[i]$ and is also presented in section 3.2. α_1 and α_2 are both parameters that represent the proportion of content characteristics and the behavioral characteristics in the model.

Ultimately, reviewers with reputation scores lower than the defined threshold are marked as suspected spammers.

$$L_{r[i].u} = \begin{cases} L_{normal} & Reputation_Value(r[i].u) > \tau \\ L_{suspected_spammer} & Reputation_Value(r[i].u) < \tau \\ random & Reputation_Value(r[i].u) = \tau \end{cases} \quad (15)$$

This section construct the reviewer's reputation quantification model by analyzing the target reviews' two sets of such indicators on content and the behavior characteristics of the reviewer which may indicate spamming activities, to find out reviewer with low reputation.

4.2 Spammers identification based on the K-center clustering

After the suspected spammers were detected, we believe that many of them may not all spammers. So, further screening should be need on this basis. In fact, spammer group is a group organization in which they work together to promote or damage their reputations of the target product. To achieving this, they will be close link together. This behavior is represented as a cluster structure on the network structure diagram. Therefore, based on the low-reputation user set, we adopt clustering algorithm to further distinguish between genuine users and spammer group.

The crucial problem in clustering algorithm is how to measure similarity. Different similarity measurement will result in different clustering results. In spamming activities of product reviews, each member of spammer group will publish multiple fake reviews in a short period of time once they received the designed task by the manufactures or the store owners. The purpose of it is to achieve the effect of taking control of sentiment on the target product. Therefore, users' posting time interval is proposed to measure similarity. The shorter the time interval between the two users, the more similar to each other, and the greater probability designed in the same cluster.

The users' posting time interval is calculated as the following formula:

$$TimeInterval_Score(r[i].u, R_p) = \frac{T(r[i].t, r[j].t)}{Max(T_p)} \quad (16)$$

Where, $T(x, y)$ is similar to that defined in equation (10), $Max(T_p)$ indicates the max posting time interval of all reviews pairs for the product $r[i].p$.

Because our ultimate goal is to identify spammers, the clustering results could be reduced two clusters, one for the fake reviewers and the other for genuine users group. Based on the clustering number, the k-center algorithm is used to cluster the user set with low-reputation, and then spammers is identified finally.

5 Experimental analysis

5.1 Dataset construction and labeling

The dataset used in this research is Music product reviews from Amazon.com provided by Hu and Liu. Generally, spammers post fake reviews on a particular product or brand. Therefore, the reputation calculation of reviewer is based on their reviews. This requires us to firstly select a certain type of product reviews from the 7705 products of the Music data set. We counted the number of reviews for each different product and selected the product with the most reviews as the data set of our experiment (product number=B0002GMSC0), which contains 1424 comments.

Moreover, the dataset was marked by seven volunteers for evaluation purpose. They first refer to the methods in the report "30 Ways You Can Spot Fake Online Reviews" which distinguish the reviews as deceptive and truthful opinions, and then make use of the relation between fake reviews and reviewers to achieve a standard annotated corpus. Seven volunteers were from four college students, two postgraduates, and one PHD candidate. In order to be able to complete the labeling task rapidly and accurately, seven volunteers are also divided into two groups and each group contains two undergraduate students and a postgraduate respectively. Undergraduate students are responsible for annotating, while postgraduate is checking. When the two undergraduate students had made different judgments, the postgraduate is responsible for decision. Finally, the PHD candidate checks and confirms the conflict labels from the two groups again and determines the label by referring to the results of two postgraduates. The entire process judges were made to work in isolation to prevent any bias.

5.2 Experiments results and analysis

Experiment1: Impact of parameters for the reputation model

In our method, reputation score of reviewer plays a crucial role in the detection task. However, there are two parameters influencing the accuracy of the detection in the reputation model. In formula(14), α_1 indicates the proportion of the review content, and α_2 corresponds to the proportion of the reviewer behavior. Obviously, the greater the proportion, the greater the role of the corresponding factors in the overall evaluation system, and therefore the effective will be different. Therefore, the purpose of this experiment is to find best configuration for our method.

Based on our experience and actual situation, we firstly tested different parameter values. Then, the stepwise addition method was used to evaluate the effect of different parameters, with step of 0.1, ranging from 0 to 1. The experimental results under precision, recall and the F value criteria are shown in the table below.

Table 1: The impact of parameters

Parameter Value	Precision	Recall	F	Parameter Value	Precision	Recall	F
$\alpha_1 = 0.0, \alpha_2 = 1.0$	0.69	0.87	0.77	$\alpha_1 = 0.6, \alpha_2 = 0.4$	0.81	0.08	0.16
$\alpha_1 = 0.3, \alpha_2 = 0.7$	0.74	0.81	0.77	$\alpha_1 = 0.7, \alpha_2 = 0.3$	0.75	0.05	0.09
$\alpha_1 = 0.4, \alpha_2 = 0.6$	0.85	0.73	0.79	$\alpha_1 = 1.0, \alpha_2 = 0.0$	0.67	0.03	0.06
$\alpha_1 = 0.5, \alpha_2 = 0.5$	0.82	0.14	0.24				

Results from the table 1 clearly indicate that the performance of the model with the two parameters $\alpha_1 = 0.4, \alpha_2 = 0.6$ is superior to other configuration, indicating that comparing to the content-based indicators the behavioral characteristics has a more significant effect on accurately detecting spammer group. Thus, the greatest values are used in the subsequent experiments. Another interesting observation in table 1 is that the recall decreases sharply with the increase proportion of the content-based feature in the entire reputation model. Its poor performance could be attributed to the number of candidate low-reputation users. In the users' reputation model, with the proportion of content-based feature increasing, the number of candidate low-reputation users is greatly reduced. On this basis, the consequently performing clustering results in high precision of detection but low recall. On the contrary, while reducing the proportion of the content-based feature, it results in a substantial growth in the number of candidate low-reputation users, which add to the noise in the clustering, and thereby reduce the accuracy of detection but increase the recall.

Experiment2: Impact of detection metrics

In the second experiment, to further analyze the role of the content-based features and behaviour of reviewers in the spammer detection, eight influence metrics are tested separately. We implemented the experiment with different combination of the metrics, in which feature options refer to the sequence indicators, their values "1" or "0" indicates the corresponding feature work or not work.

Table 2: The impact of the detection metrics

Features Options	Precision	Recall	Features Options	Precision	Recall
01111111	0.52	0.82	11110111	0.82	0.19
10111111	0.74	0.21	11111011	0.12	0.10
11011111	0.62	0.73	11111101	0.75	0.39
11101111	0.73	0.57	11111110	0.75	0.39

From table 2, we can see that the reviewer behavior features could more influence the performance for spammer groups detection compared with the review content, especially the indicator of the user activity. When user activity feature does not work, very few candidate low-reputation users are returned, and most of them are not spammers, so their precision and recall are both very low.

Moreover, according to the results of the experiments, in the reviewer behavior indicators, the review deviation and other rating score of the reviewer are the same impact on spammer group identification. The reason is that both features return the same number of candidate low-reputation users, which lead to consistent identification recall and precision.

Another interesting observation is that among the five review content indicators, the target review's features of duplicate and sentiment have more impact on the spammer group identification than the other three. When the duplicate review indicator does not work, the results show that the excessive candidate low-reputation users are returned, indicating that reputation model does not perform the filtering of low-reputation user well, resulting in the noise increase and lower detection accuracy. Simultaneously, while the review opinion indicator does not work, too few low-reputation users are returned, indicating that a large number of real low-reputation users are filtered out, resulting in a rapid decrease of the recall.

Experiment3: Comparison of the models

In order to further verify the effectiveness of the proposed method, we conduct a comparison experiment with the Lin's work [12]. They proposed an unsupervised learning method for fake review detection. Actually, there exists a close correlation between fake reviews and spammers. A review written by a spammer is a fake review with high probability, and a fake review is almost certainly written by a spammer. Therefore, the experimental results are comparable. The specific experimental data is shown in Table 3.

Table 3: Performance comparison results

	Precision	Recall	F-Score
Our method	0.85	0.73	0.79
Lin's work	0.81	0.70	0.75

As can be seen from the data in Table 3, the model proposed in this paper clearly obtained better performance results. For the reason of analysis, in Lin's work [12], the proposed six characteristics of the review text and the reviewer's behavior are all individual spammers, ignoring the characteristics of group organizations among spammers. Therefore, some normal reviewers are mistaken for spammers. At the same time, the model proposed in this paper has gone through two stages. The first stage is to detect the suspected opinion spammers. The users with low reputation value will be regarded as suspected spammers. They are filtered out through the reputation value combining the review text and the reviewer's behavior. On this basis, the characteristics of the group behavior between the spammers are fully explored, and the clustering analysis is used to identify the spammers. The two-stage joint implementation ensures the accuracy of opinion spammers identification.

6 Conclusion and future work

In this paper, an effective opinion spammers detection approach is put forward. Based on the idea that the reviewer's reputation has a direct relation with the quality of reviews, in this paper, we first propose a reviewer's reputation model which employs the target review's content-based characteristics (context similarity, opinion sentiment, review length and helpful feedback) as well as behavior-based features (authors' activeness, review deviation and rating) to assign reputation scores to each reviewer and distinguish suspected spammers with low-reputation reviewers from ordinary reviewers. On this basis, the k-center clustering algorithm is used to perform for suspected spammers to ultimate identify spammers due to the observation that the spammers' posting time intervals burst.

On Amazon's Music real dataset, we constructed a set of annotated review, and verify the effectiveness of spammers identification method. Besides, we also analyze the effects of the eight kinds of features on identification model. The experimental results are encouraging and indicate that the spammers identification method based on reputation and clustering algorithm poses high accuracy and recall, and good performance is achieved. Furthermore, performance comparison results between the proposed method and Yuming' work show better detection accuracy.

To date, the spammer detection is still open issue. Two suggestions should be worthy attention in the future research direction. The first direction could be a deep exploring and analyzing more features of linguistic, relations, and psycholinguistic of opinion spammers to distinguish from ordinary reviewers. These valuable features could be benefit to improve the performance of detection.

Another suggestion for future work is transformation from detection to analysis social and psychological impact of spamming activities on customers. At present, a lot of work focuses on how to identify the existing spammers or spammer groups. However, harmful spammers activity can affect many potential customers psychology and decision-making. Therefore, analysis the impact of spamming activities on customer participation is our next work.

7 Acknowledgments

This work was supported by the National Science Foundation of China under Grant Numbers 71861014, 71762017 and 61662027, and the Project of Hunan Provincial Education Department(17A113,18A441,17K015) and Hunan Provincial Philosophy and Social Science Fund(16YBA228).

Bibliography

- [1] Banerjee, S.; Chua, A.; Kim, J.(2015). Using Supervised Learning to Classify Authentic and Fake Online Reviews, *Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication*, 938–942, 2015.
- [2] Crawford, M.; Khoshgoftaar, T.M.; Prusa, J.D. et al.(2015). Survey of Review Spam Detection using Machine Learning Technique, *Journal of Big Data*, 2(1), 1–24, 2015.
- [3] Dewang, R.K.; Singh, A. K.(2015). Identification of Fake Reviews using New Set of Lexical and Syntactic Features, *Proceedings of the sixth International Conference on Computer and Communication Technology*, 115–119, 2015.
- [4] Dong, M.; Yao, L.; Wang, X.(2018). Opinion Fraud Detection via Neural Autoencoder Decision Forest, *Pattern Recognition Letters*, 1–9, 2018.
- [5] Heydari, A.; Tavakoli, M.; Salim, N.(2016). Detection of Fake Opinions using Time Series, *Expert Systems with Application*, 58, 83–92, 2016.
- [6] Heydari, A.; Tavakoli, M.; Salim, N. et al. (2015). Detection of Review Spam: A Survey, *Expert Systems with Applications*, 42 (7), 3634–3642, 2015.
- [7] Hua, N.; Boseb, I.; Koh, N. et al.(2012). Manipulation of Online Reviews: An Analysis of Ratings, Readability, and Sentitnents, *Decision Support System*, 52(3), 674–684, 2012.
- [8] Jindal, N.; Liu, B. (2008). Opinion Spam and Analysis, *Proceedings of the First ACM International Conference on Web Search and Data Mining (WSDM)*, 219–229, 2008.
- [9] Lau, R.Y.K.; Liao, S.Y.; Chi-Wai Kwok, R.; Xu, C. et al.(2014). Text Mining and Probabilistic Language Modeling for Online Review Spam Detection, *ACM Transactions on Management Information Systems*, 2(4), 1–30, 2011.
- [10] Li, J.; Wu, G.S.; Xie, F. et al.(2016). Research of Fraud Review Detection Model on O2O Platform, *Journal of ACTA Electronica Sinica*, 44(12), 2855–2860, 2016.
- [11] Lim, E.; Nguyen, V.; Jindal, N. et al.(2010). Detecting Product Review Spammers using Rating Behaviors, *Proceedings of the 19th ACM International Conference on Information and Knowledge Management(CIKM)*, 939–948, 2010.

- [12] Lin, Y.; Zhu, T.; Wang, X. et al.(2014). Towards Online Review Spam Detection, *Proceedings of the companion publication of the 23rd International Conference on World Wide Web Companion*, 341–342, 2014.
- [13] Liu, Y.; Pang, B.(2018). A Unified Framework for Detecting Author Spamicity by Modeling Review Deviation, *Expert Systems With Applications*, 112, 148-155, 2018.
- [14] Luca, M.; Zervas, G. (2016). Fake it Till You Make It: Reputation, Competition, and Yelp Review Fraud, *Harvard Business School Working Paper*, 62, 3412-3427, 2016.
- [15] Mukherjee, A.; Liu, B.; Wang, J. et al.(2011). Detecting Group Review Spam, *Proceedings of the 20th International World Wide Web Conference (WWW)*, 93-94, 2011.
- [16] Ren, Y.; Ji, D.(2017). Neural Networks for Deceptive Opinion Spam Detection: An Empirical Study, *Information Sciences*, 385-386, 213-224, 2017.
- [17] Savage, D.; Zhang, X.; Yu, X. et al.(2015). Detection of Opinion Spam based on Anomalous Rating Deviation, *Expert Systems with Applications*, 42(22), 8650-8657, 2015.
- [18] Vlad, S.; Martin, E.(2015). Detecting Singleton Review Spammers using Semantic Similarity, *Proceedings of 24th International Conference on World Wide Web Companion*, 971-976, 2015.
- [19] Zhang, W.; Bu, C.; Taketoshi, Y. et al.(2016). Cospa: A Co-training Approach for Spam Review Identification with Support Vector Machine, *Information*, 7(12), 1-15, 2016.
- [20] Zhang, D.(2017). High Speed Train Control System Big Data Analysis based on Fuzzy RDF Model and Uncertain Reasoning, *International Journal of Computers Communications & Control*, 12(4), 577-591, 2017.
- [21] Zhang, D.; Sui, J.; Gong, Y. (2017). Large Scales Software Test Data Generation based on Collective Constraint and Weighted Combination Method, *Tehnicki Vjesnik*, 24(4), 1041-1050, 2017.

Author index

Amiri, M., 710
Antucheviciene, J., 710

Cenys, A., 743
Chen, Z., 615
Chen, Z.X., 653

Filip, F.G., 633

Ghahremanloo, M., 710
Goranin, N., 743

Jain, A., 670
Jeong, G.-M., 726
Ji, S.-H., 726
Jiang, J.W., 615

Kalibatiene, D., 743

Li, Y., 633
Liu, F., 653

Nandury, S.V., 691

Peng, T., 615
Peng, Y., 653

Qu, X.L., 759

Shi, L.M., 615
Shi, Y., 653
Singh, A., 670
Siva Prashanth, J., 691
Steckevicius, Z., 743

Tabatabaei, M.H., 710
Tan, Z., 759
Truong, P.H., 726

Vitkus, D., 743

Wang, X.X., 633
Wang, Y.H., 615

Xu, Z.S., 633

You, S., 726

Zavadskas, E.K., 710
Zhong, M.J., 759
Zhu, S.L., 615