INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 12(5), 612-630, October 2017.

Benchmarking of Recommendation Trust Computation for Trust/Trustworthiness Estimation in HDNs

H. El-Sayed, S. Sankar, H. Yu, G. Thandavarayan

Hesham El-Sayed*, Heng Yu, Gokulnath Thandavarayan
College of Information Technology,
UAE University,
Al Ain-15551, United Arab Emirates
*Corresponding author: helsayed@uaeu.ac.ae
heng.yu@uaeu.ac.ae, gokul@uaeu.ac.ae

Sharmi Sankar
Department of Information Technology,
Ibri College of Applied Sciences (MoHE),
Sultanate of Oman
sharmisankar41@gmail.com.

Abstract: In the recent years, Heterogeneous Distributed Networks (HDNs) is a predominant technology implemented to enable various application in different fields like transportation, medicine, war zone, etc. Due to its arbitrary self-organizing nature and temporary topologies in the spatial-temporal region, distributed systems are vulnerable with a few security issues and demands high security countermeasures. Unlike other static networks, the unique characteristics of HDNs demands cutting edge security policies. Numerous cryptographic techniques have been proposed by different researchers to address the security issues in HDNs. These techniques utilize too many resources, resulting in higher network overheads. This being classified under light weight security scheme, the Trust Management System (TMS) tends to be one of the most promising technology, featured with more efficiency in terms of availability, scalability and simplicity. It advocates both the node level validation and data level verification enhancing trust between the attributes. Further, it thwarts a wide range of security attacks by incorporating various statistical techniques and integrated security services. In this paper, we present a literature survey on different TMS that highlights reliable techniques adapted across the entire HDNs. We then comprehensively study the existing distributed trust computations and benchmark them in accordance to their effectiveness. Further, performance analysis is applied on the existing computation techniques and the benchmarked outcome delivered by Recommendation Trust Computations (RTC) is discussed. A Receiver Operating Characteristics (ROC) curve illustrates better accuracy for Recommendation Trust Computations (RTC), in comparison with Direct Trust Computations (DTC) and Hybrid Trust Computations (HTC). Finally, we propose the future directions for research and highlight reliable techniques to build an efficient TMS in HDNs.
Keywords: direct trust computations, hybrid trust computations (HTC), heterogeneous distributed networks (HDNs), receiver operating characteristics, recommendation trust computations (RTC).

1 Introduction

Heterogeneous Distributed Networks have become increasingly popular in the recent years, expanding its contribution across different computing fields with promising results. In wireless networks, the nodes are equipped with On Board Units (OBU) that creates a dynamic communication between different agents without the need for any network infra-structure. Based on

the user demands and network behavior, the HDNs can be classified into Mobile Ad-Hoc Network (MANET), Vehicular Ad-Hoc Network (VANET) and Wireless Sensor Network (WSN), featured with unique characteristics to serve a particular environment. Many researchers have rendered incredible contribution in all these domains and have developed standards and protocols to serve the domain [3, 13]. Certain vital operations like sensing [16], routing [14, 17, 23] and event monitoring [22] are some of the major research topics carried out by the researchers, rendering prodigious contributions and problem-solving techniques in every domain.

Nowadays, the networks are loaded with built-in reliable standards and protocols, despite this the security and privacy concerns are still some of the major issues [15], degrading the efficiency and reliability of the application. Owing to the openness of the wireless network and uncontrollability of the nodes without a Central Authority (CA), the availability of compromising nodes and unauthorized access becomes inevitable in the network. Many researchers have worked on this issue and proposed various schemes that can be broadly classified as hard and soft security schemes [29,30]. In the hard security scheme, cryptographic algorithms are implemented to ensure confidentiality on information exchange and authentication of participation nodes. It demands more resource utilization to perform these actions and consumes more power and processing capabilities that are scarcely available in these networks. Moreover, the reputation of the participating nodes and the trustworthiness of the received message cannot be verified using these schemes/techniques. Therefore, establishing a behavior analysis on these nodes and the verification and validation of the message exchange is implemented using the soft security scheme called Trust Management Systems (TMS). Using trust systems, the behavior analysis is performed for the participating nodes and the selfish acts are reported by computing the trust metrics.

In general, attributes like trustworthiness, reputation, belief and confidence impose uncertain behavior in HDNs. Imprecise information floating around HDNs is unavoidable due to their limitations in wireless communications [8]. HDNs demands an efficient technique to calibrate the opinions and recommendations derived from direct and indirect communications. For this purpose, trust computation (TC) is an important element in TMS, which will enable to compute a trust metric between the trustor and trustee with the available information. Computing and verifying the trust metric in unsupervised environment is challenging and demands an efficient technique to handle it. Also during trust computations, the probability level of acceptance rate in trust metric will change periodically due to the spatial-temporal factors. The probability levels on trustworthiness can be estimated dynamically by monitoring the risk factors involved. Risk analysis (RA) [11] is an important framework to measure trust metric in HDN and will be used to adjust the acceptance rate of the trust metric based on the current requirement as shown in Figure 1. Many technologies have been evolved for RA which primarily focuses on data driven and node driven risk analysis. Decision making in HDNs is adapted to refine the obtained trust metric using aggregated information. Due to the presence of uncertainty and imprecisions in the trust computation logic, a reliable aggregation technique will help the requestor to estimate a reliable trust metric of the enquiring node.

Implementing TMS for a fixed network is simple and direct, easily computing the trustworthiness of a participating node. But, establishing a TMS in HDNs is highly challenging due to the uncertain behavior in the environment. The following key points are some of the major issues in establishing TMS in distributed networks.

- The spatial and temporal dimensions of the participating nodes are ever changing in the dynamic networks making the node observation more challenging. Decisions made from interactions may further provide futile results as the location and time cannot be referenced in the environment which may increase the selfish behavior [10].

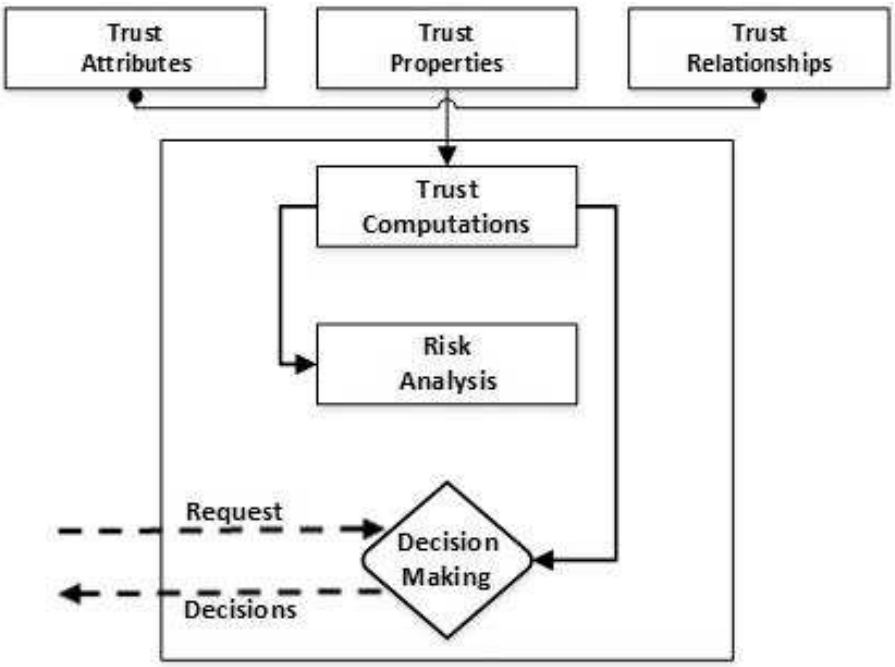

Figure 1: A general view on trust supported models

- As every network follows a particular mobility model [25], handshaking between nodes increases overhead due to the limitations in wireless network.
- Also the network does not follow a master-slave relationship, hence the decision making on a recommendation message from a neighbor node necessitates further verification to strengthen the result. It also limits the trust chain to be intact which cannot be forwarded further.

In the recent years, TMS has contributed numerous models for the HDN and enormous contributions from researchers has led to the development of an efficient model. However, a detailed survey and benchmarking of these models is required for the entire HDN. Some researchers have published survey papers on TMS which highlights the trust computing techniques only for a particular network domain [9, 33]. Also, benchmarking the existing techniques and comparing the techniques for an effective study, is still a major shortfall in these survey papers.

Therefore, a cohesive survey is still in high demand for the entire distributed networks to understand the accomplishment of the existing TMS models and requires benchmarking techniques to explore the best models for the entire domain of HDN. In this paper, we have made a thorough survey on TMS on a broader spectrum, highlighting the best practicing techniques in every HDN domain. Further, the existing techniques are tested with statistical models and the effectiveness is measured. The outcome of the performance measure presented in the paper highlights the best techniques for TMS which addresses the security and privacy issues effectively. Also, the paper conclusively recommends future research trends for a holistic TMS in HDN.

2 Trust dimensions

Trust is a relationship between two or more agents demonstrating the belief with one another, with more reliability and trustworthiness. In HDN, the agent can be a vehicle node, Road-Side Unit (RSU), mobile node or sensor node. Trust relationships are formed between agents to

compute the trust relationship between trusting agents and trusted agents. In this section, we introduce the trust dimensions which help to understand the basic entities of trust.

2.1 Trust environments

A node can analyze the trust relationship and compute the trust metrics based on the network environment in which the participant nodes exist. The trust computation in the environment can be broadly classified as physical and virtual trust. In physical trust, the trust is established between nodes based on direct interactions. In this environment, the trust evaluation is restricted to single hop interaction; whereas, in the virtual trust a trust metric can be computed from nodes which are connected by intermediate nodes. In this environment, the nodes are virtually connected and share recommendations to derive a trust metric.

2.2 Trust definition in literature

The importance of trust is widely accepted and acknowledged across different arenas in a multifaceted vision and connotations. In the field of sociology, trust is referred to as a basic fact of social life that involves both emotional and cognitive dimensions, sprouted from the past as well as from the present activity. In Philosophy, trust is determined as plausible that concedes to form relationships among people. It attributes to be an inevitable trait of our societal life and determines our relationship with the environment, despite the fact that it always carries the risk of being unwarranted. Likewise, in the Economics domain, trust can be conceptualized by bounded rational and subjective probabilities. It make decisions on the business activities to reduce the cost price and thereby discerned as an economic lubricant. In the field of Computer Science and technology, trust is employed as a medium to provide a high-end security, privacy, reliability and integrity in different computing group that ranges from network application to internal system computations. In computing, trust is the firm vision and belief to authorize an entity to act dependably secure and reliable within a specific context. It is to be kept in mind that both the trustor and trustee should be validated equally to enhance the contextual factor of expectancy.

2.3 Trust attributes

The three main properties of trust on a network are asymmetry, transitivity and composability. Asymmetry trust is assured as two nodes trust each other on the same level. Transitivity trust is an inferred trust. Composability trust, receives information from all available sources and compose an opinion value.

2.4 Trust metrics

Trust evaluation metrics are classified into three categories: Trust on scale, trust by facets, and trust upon logic. Trust on scale scheme measures the level of trust using discrete or continuous series. Trust through facets measure rely on three attributes; the belief, the disbelief and uncertainty. The trust is represented as a triplet phase. Trust upon logic uses a probability approach to determine the trust. The ratio upon the number of packets forwarded and received is one trust measure.

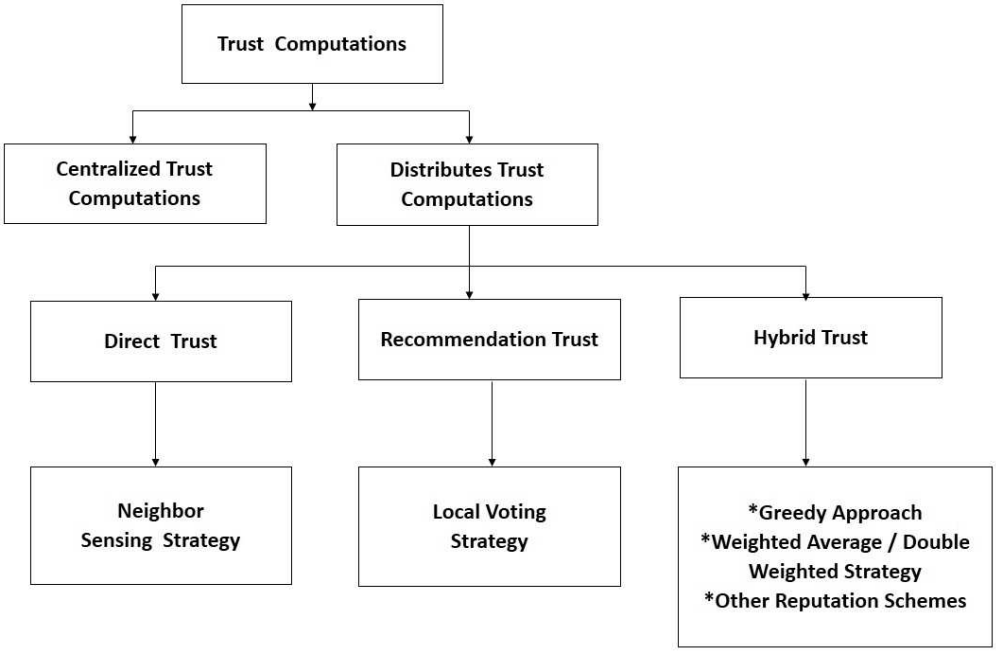

Figure 2: Taxonomy of trust computations

3 Trust computing approaches : an overview

As the HDNs is utilized by life-saving applications, the verification and validation of both data and node is necessary to ensure the authenticity of the incoming data. Therefore, trust management systems have an immense contribution in establishing the trustworthiness in the self-organized HDN. TMS ensures the network to be safe from selfish and malicious nodes. In order to enable trustworthiness between entities, measuring the trustworthy is an essential task. With the uncertainties existing in the environment, the trustworthiness of a node or message has to be ascertained. Additionally, a security system has to be in place to thwart any attacks and to detect vulnerabilities. Adapting a reliable TMS model in HDN is the most effective way to have a secure and reliable service in the environment. Enormous efforts using different statistical and learning techniques have been built into TMS enabling seamless service.

Trust on a node can be ensured with subjective assessment on reliability and accuracy, as they traverse along the node in a given context. Trust computations are measured upon experience, recommendation and knowledge. The experience is measured at regular intervals in a trust table using direct trust strategy. Recommendation on trust sets its path as the values in the trust table are propagated to the other nodes. Knowledge of the total trust is evaluated based on the previous trust computations. The strategies used to measure the trust at various situations differ based on the environment and applicable mode of trust, the taxonomy is illustrated in Figure 2.

Based on the TMS schemes, trust computations are considered as an essential module to verify and validate both node and data. In all the trust computation techniques, a trust metric will be derived from the information shared by the peers. The reliability and credibility of the trust metric is based on the completeness of the chosen factors that are taken into account. In general, trust computations can be broadly classified into two categories based on the network compatibility, (i) centralized trust computations and (ii) distributed trust computations.

In centralized trust computations, a Central Authority (CA) will manage the behavior of the participating nodes and the trustworthiness is derived from the recommendations of CA. The

TMS based on this scheme will follow a master-slave property and the scheme will provide a reliable service to the nodes. However, there are limitations in these schemes, the entire system access can be denied when the CA is under attack or compromised. Also, having centralized servers in the distributed environment is not highly recommended as it could impact the dynamicity of the nodes. Summarizing, in order to have a reliable service in the HDN environment, the node has to follow the peer-to-peer communication and has to be equally distributed in terms of receiving, maintaining and distributing the trust metric. For this purpose, a distributed trust computation offers a reliable service to the node and dynamically manages the trust metric in the HDN environment.

In distributed trust schemes, the nodes are capable of managing themselves and the trust metric is computed based on the input from the participating nodes alone. This paper discusses only the schemes related to the distributed trusted models. Further, trust computation in the distributed trust models follow three different strategies to compute the trust metric; (i) direct trust, (ii) indirect trust and (iii) hybrid trust.

In direct trust computations (DTC), the trustworthiness of a node will be computed from the direct experience. Based on the interactions with a single-hop node, the evidences are collected and stored from the direct input relay node. When a node wants to participate in the network for data exchange, a trust score for the node is computed from the direct interactions with the trustee node and the experiences are shared from the single-hop nodes.

In indirect trust computations (ITC), the node trustworthiness will be computed from the recommendations provided from the surrounding nodes. The nodes will constantly collect evidence and monitor the neighboring nodes behavior. The opinions collected are based on the past and present interaction with the node. If a trustee node wants to know about the trustworthiness of a participating node, it can request other nodes to share their opinions and the other nodes which have opinion on the participating node will share its information as recommendations based on their previous experience. Using this information, the trustee node can compute the trust metric for the participating node and can evaluate the nodes trustworthiness.

In hybrid trust computations (HTC), the results from DTC and ITC are utilized. The trust metric is computed using both the direct experience and recommendations from surrounding nodes are aggregated together. The basic idea in this scheme is to evaluate the trust metric using direct experience and verify the same using the opinions obtained from the ITC. Using this scheme, the selfish behavior nodes can be easily determined from the opinions provided by the surrounding nodes.

The existing methodologies in distributed trust computations with maximum reliability and efficiency are taken into consideration and a detailed comparison on different trust computations are discussed in Table 1-3. In this tables, the selected schemes are evaluated based on the system context, trust metrics, system merits, complexity and limitations of the system.

Based on the comparison, a brief discussion on the classifications of different networks with incorporated trust schemes are highlighted in Table 4. Heterogeneous networks are incorporated with different trust schemes to fulfill and improve the performance. The schemes are listed in table 4 with a brief explanation provided for VANETs, MANETs and wireless sensor networks (WSN). The schemes in Direct Trust Computations (DTC) category computes the trustworthiness of a node based on its own experience, as well as on the opinions obtained from the single-hop neighbor nodes.

Initially, every single node monitors the performance of other directly connected nodes and maintains a precise information table pertaining to the success ratio of the message-forwarding rate, message-strength, message-veracity and transaction rates. Subsequently, when a new target node requests for a participation with a trustee node in the network, the trustee node probes an opinion about the target node from its trustable single-hop neighbor nodes.

Table 1: Direct trust computations

Direct (Experience) Trust Computations						
Ref.	Approach	Context	Trust Metrics	Merits	Complexity	Limitations
[32]	Bayesian Approach	Packet forwarding based	Trust metric [0,1]	*windowing scheme is used*trustworthy route computation	* Route Computation * Opinion Calculation	Vulnerable to colluding and badmouth attack
[33]	Role and Experience Sensing	Cluster based aggregation	Trust value [0,1]	*identity-based aggregation *effective local action decision	*Cluster Head computation	Non-resistivity to selfish cluster-heads
[19]	A multi-faceted trust computing approach	Roles, experience, priority, and majority opinion based	Trust interval [-1,1]	*limits consulting advisors *majority consensus	*Computational complexity	Vulnerable to selfish and spoofing attacks
[20]	Bayesian probabilistic approach	Opinion analytics based	Trust value [0,1]	*beta and Gaussian reputation system *expert Opinion theory	*Computational complexity	Vulnerable to sybil attack
[6]	Markov chain approach	Trust value based	Trust value [0,1]	*secure authentication for group management	*Computational complexity	Trust decay factor not considered
[28]	Recommen-dation exchange approach	Neighbor trust based	Trust value [0,1]	*resistance to false *recommendation attack	*Computational complexity	Not suitable for more complex scenarios
[5]	Perron-Frobenius (PF) theorem	Message behavior analysis	Trust value [0,1]	*generate trust values full or partial data	*Computational complexity	Vulnerable to On-Off and Collusion attack

Table 2: Indirect trust computations

Indirect (recommendation) trust computations						
Ref.	Approach	Context	Trust Metrics	Merits	Complexity	Limitations
[12]	Analytical trust model	Node behavior model	Trust value [0,1]	*Entity and data approach with markov chain *Restrict selfish behavior	*Space Complexity *Computation Complexity	Demands constant monitoring and updating
[7]	Stochastic Petri net (SPN) technique	Trust chain optimization	Trust value [0,1]	*precise trust metric from social and QoS trust	*Computation Complexity	Vulnerable to selfish behavior
[24]	Geographic Hash Table	Consensus technique based	Trust opinion [0,1]	*Identify storage nodes *Decrease storage cost	*Computation Complexity	Susceptible to sophisticated attacks
[18]	Dempster-Shafer Theory(DST)	Attack resistant model	Trust value [0,1]	*Trust evaluation for both data and node	*Space Complexity *Computation Complexity	Vulnerable to sybil and collusion attacks
[21]	Dempster-Shafer theory (DST)	Trust path model	belief map [0,1]	*Detection of malicious nodes and benign nodes	*Computation Complexity	Demands constant monitoring and updating

Table 3: Hybrid trust computations

Hybrid Trust Computations						
Ref.	Approach	Context	Trust Metrics	Merits	Complexity	Limitations
[1]	Geometric mean-based	Node trust model	Trust metric [0,1]	*Estimate node trust level *Reliable routing	*Computation Complexity	Requires constant monitoring and updating
[2]	Stochastic Petri nets technique	Subjective trust Validation	Trust value [0,1]	*Resilient to black-/sink hole, slandering and bad-mouthing attacks	*Space Complexity *Computation Complexity	System overhead and Cluster head failure
[4]	Dempster-Shafer theory (DST)	User centric privacy based	Trust value [0,1]	*Estimate trust event messages	*Computation Complexity	Vulnerable to selfish behavior
[26]	Bayesian statistical approach	Dynamic cluster based	Trust value [0,1]	*Filter dishonest recommendations	*Computation Complexity	Non-resistance to time and location dependent attacks
[27]	Fuzzy logic and graph theory	Node trust model	Trust value [0,1]	*Filtering algorithm for node *Decay method for routing	*Computation Complexity	Vulnerable to trust based attacks

Table 4: Trust in heterogeneous distributed networks

Heterogeneous distributed networks			
Trust schemes	VANET	MANET	WSN
Trust agent based scheme	*Effective decision making using agents on routing	*Manage reputation score for agents	*Estimate node trust level using agents and provides reliable routing
Hybrid trust scheme	*Estimate trust event messages *Helps to extricate malicious and selfish nodes *Detect inside attackers	*Distinguish trust nodes Decay method for routing	*Identify malicious sensor data
Recommendation trust scheme	*Enhance trustworthiness estimation *Detect fraudulent servers	*Precise trust metric from social and QoS trust	*Resistance to false attacks on sensor nodes
Direct trust scheme	*Generate trust values with full or partial data	*Secure authentication for group management	*Behavior analysis of nodes and computes trust score

The neighbor nodes which has previous experience with the target node, share its opinion about the target node. After collecting the opinions, the trustee node computes the trust metric for the target node and evaluates its trustworthiness.

In order to serve this purpose, techniques like Bayesian approach, Markov chain modelling and Perron-Frobenius (PF) models are employed in computing the trust metric in DTC. As the trustworthiness are computed only from the direct nodes, the derived trust metric is instantaneous and may not be accurate. Additionally, due to the limitations like mobility and connectivity issues that already exists in the HDN environment, the communication between two nodes are short lived and the opinions obtained from the neighbor nodes will be significantly minimal. These lead the trust metric in DTC provide a futile and biased results.

The Recommendation Trust Computations (RTC) category utilizes techniques and computes the trust value from the recommendations relayed from various indirect nodes. Every node follows a transitive path to derive the trustworthiness of other nodes. In order to find the trustworthiness of a target node, the trustee node broadcasts a message to the neighboring nodes, requesting an opinion about the target node. The nodes holding previous handshaking experience with the target node will share their opinions to the trustee node in a multi-hop fashion. Once the trustee node receives the opinions, it validates the received data based on the signal strength, distance, time lapse, similarity, energy level and closeness of the node. For this purpose, techniques like Dempster-Shafer theory (DST), Stochastic Petri Net (SPN) and Geographic Hash Tables are employed to verify the opinions and compute the trust metric for the target node. Due to fact that the recommendations are obtained from unknown and indirect nodes, the recommendations exhibit selfishness that are too hard to identify and validate. Moreover, attacks like Sybil and On-Off attacks would easily compromise the network and malicious nodes remain undetectable due to the indirect connections.

Consequently, in such above mentioned cases, the Hybrid Trust Computations (HTC) can be employed as a reliable technique that involves both the functionalities of direct and recommenda-

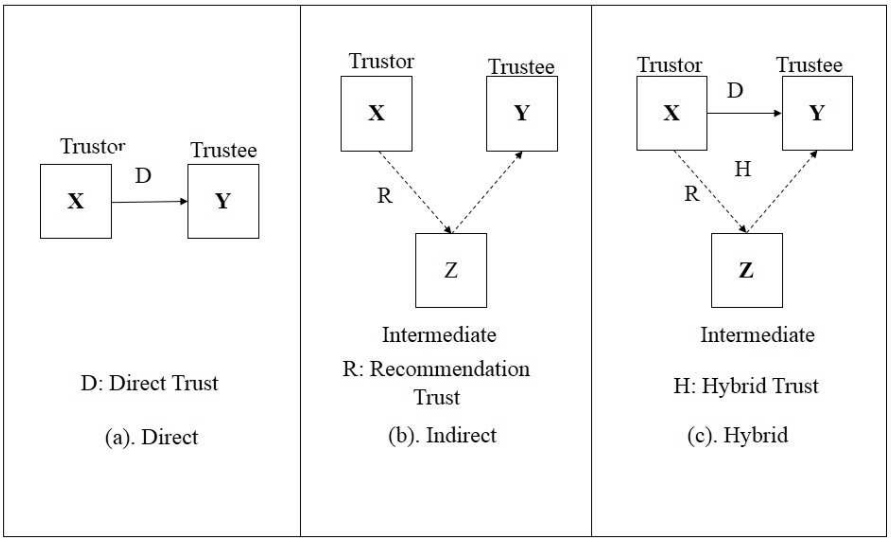

Figure 3: Taxonomy of trust computations

tion trust computation schemes. Along the lines of HTC technique, the trustee node computes the trustworthiness of a target node, procures opinions from the neighbor node without any limitations. Both direct referrals and indirect recommendations are utilized to derive the trust metric for the target node. Using this technique, the trustworthiness of both data and node could be verified.

Generally, the trustee node combines the recommendations from indirect vehicles and aggregates it to a single opinion. This aggregated metric will be further validated by the direct referrals that are in close proximity to the trustee node. In this technique, the derived trust metric for the target node is verified and validated by both the direct and the indirect nodes. Thereby, this multifaceted computation strategy efficiently computes and validates the trust metric, providing more resistance to the selfish behavior and thwarts the trust related attacks in the HDN environment.

4 Estimation of trust computations

Trust is computed based on two varieties of trust between the trustor and trustee nodes. They are direct trust and recommendation trust. In direct trust, the trust value is authenticated by a directed path between the trustor and the trustee. Whereas, in recommendation trust, the trust value is authenticated by third parties. In hybrid computation, both directed path trust value and third party recommended trust values are considered and the trust computation models are shown in Figure 3.

4.1 Direct trust computation (DTC)

Direct-trust computations are estimated with trust values ranging between +1 and -1. A tangent-hyperbolic function is used to estimate the trust value (a) built on the experience of trustor node (b), as shown in Equation (1). The equation is generalized, as a trustor node en-

Table 5: Trust elements and their properties

Element	Property
P_i	Path directed trust value
W_i	Prioritizes the level of importance on trust
τ_i	Node directed trust value; +1 for positive experience; -1 for negative experience
N	Unlimited, varies with environment
R_i	Recommended trust value range between +1 and -1

counters many trustee nodes and affect the evaluation of trust. The trust value will be computed using Equation (2), where P_i represents the direct-path experience with i^{th} trustee node, n is the total number of trustee nodes that participate with the trustor node, W_i represents the weight for the directed path prioritizing the experience and τ_i is +1 for a positive trust with the i^{th} trustee node and -1 for distrust. The trust element properties are listed in Table 5.

$$a = \frac{sinh(b)}{cosh(b)} = tanh(b) \tag{1}$$

$$T_{DTC} = tanh(\sum_{i=1}^{n} \tau_i \times P_i W_i) \tag{2}$$

The reason behind the choice of tangent hyperbolic function in comparison to the other identity activation function and logistic sigmoidal function being, the identity function maps output values range between $-\infty$ to ∞, logistic sigmoidal function maps output range lies between 0 and 1, whereas tangent hyperbolic function maps output values range from -1 to 1. Summarizing these, the trust values calculated in DTC use hyperbolic tangent function, to return trust values between -1 and $+1$. The corresponding hyperbolic tangents values ratio over hyperbolic sine represented as sinh() function and hyperbolic cosine represented as cosh() function.

4.2 Recommendation trust computation (RTC)

The trustor node has no directed path of experience with the trustee, therefore, it enquires a third node otherwise called the recommender node. When nodes do not encounter directed path experiences, they rely on third party recommendations. In this situation, to justify reasonable recommendation, the trustor always initiates multiple recommendation path experiences. The path experiences are not limited. The recommended trust values depend on the trustworthiness of the third party nodes with the trustor itself. Multiple trust recommendations from multiple third party nodes to the trustor widens the vision of the trustor in fixing the trust value for the trustee.

$$T_R = \sum_{i=1}^{n} (R_i \times T_{DTC_i}) \tag{3}$$

The recommender node when enquired delivers a trust value R_i on the i^{th} trustee node. The trustor holds T_{DTC} the direct trust value for the recommender node, as shown in Equation (3). The recommender nodes trust values reasonability is crosschecked by the trustor by inquiring/investigating several third party recommendation nodes.

Table 6: Trust computation (TC) summary

Trustee-id	Trustor-id	W_i	P_i	τ_i	TC (Expected) DTC	RTC	HTC	Actual Trust
166497924	725979012	4	1	1	0.999329	0.999329	0.999329	+1
166497924	258110	5	1	1	0.999909	0.999909	0.999909	+1
166497924	334400	5	1	1	0.999909	0.999909	0.999909	+1
166497924	492685	4	1	1	0.999329	0.999329	0.999329	+1
166497924	396581	4	1	1	0.999329	0.999329	0.999329	+1
166497924	328049	4	0.5	-1	0.995055	-0.99505	-0.59703	-1
166497924	534929	4	1	-1	0.995055	-0.99505	-0.59703	-1
166497924	768446340	4	1	-1	0.999329	-0.99933	-0.59960	-1
166497924	223418	3	0.5	-1	0.964028	-0.96403	-0.57842	-1
166563460	379568	5	1	1	0.999909	0.999909	0.999909	+1

4.3 Hybrid trust computation (HTC)

The trustor acquires direct trust values and recommendation trust values for the trustee node. The equations (3) and (2) are combined together in Equation (4) to arrive at hybrid computation trust value T_H. If T_{DTC} value is high and T_R value is low, then considerations on T_{DTC} is more when compared with T_R, or vice versa.

$$T_H = \{T_{DTC} = +\}, (1 \times |T_{DTC}| \times T_R)(-1 \leq T_{DTC} \leq 1)(-1 \leq T_R \leq 1) \tag{4}$$

In particular instances, when $T_{DTC} = 1$ and the trustor is assured complete certainty on the trust value, then the trustor will no longer consider the third party nodes recommendations. Otherwise, as $T_{DTC} = 0$ and the trustor is not assured complete certainty on the trust value, then the trustor will rely on the recommendations that are relayed from the third party nodes. In addition, the consideration of recommendations trust depends on the percentage of certainty values of direct trust.

5 Empirical results

The dataset from www.trustlet.org is explored and the trust values are computed using all the three computation strategies DTC, RTC, and HTC which are listed in Table 6. The expected/actual trust values are computed and plotted for visual illustration as shown in Figure 4.

6 Receiver operating characteristics (ROC) benchmarking trust computations

The operating characteristics are classified for the actual and estimated trust values with true positive (TP), true negative (TN) along with false positive (FP) and false negative (FN) accordingly in Table 7. The dataset from www.trustlet.org is being used to plot the ROC for 1000 instances, with equally distributed trust and distrust values (500 instances each). The characteristic of true positive denotes the proportion of trusted trust values correctly classified as +1, true negative is the proportion of distrust trust values correctly classified as -1, false positive

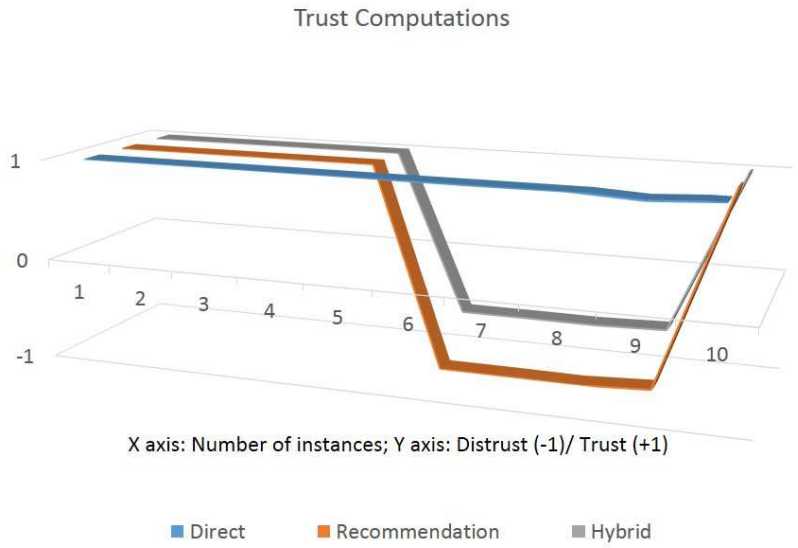

Figure 4: Trust computation summary (Direct, Recommendation, and Hybrid)

Table 7: Actual vs Estimated trust values

	Actual Trust value		Estimated Trust value	
1 / -1	Trust	Distrust	Trust	Distrust
Trust TP	FP	TP	FN	
Distrust	FN	TN	FP	TN

shows the proportion of distrust trust values incorrectly classified as +1 and false negative as the proportion of trusted trust values incorrectly as -1.

The sensitivity or true positive rate (TPR) on trust values are calculated by dividing the true positive values by the summed up value of true positive and false negative. Later, specificity or true negative rate (TNR) on trust values are calculated by dividing the true negative values by the summed up value of true negative and false positive. The estimations on true positive/negative and false positive/negative for expected and actual trust/distrust values as shown in Figure 5(a) moving ahead further graph is plotted on sensitivity and specificity as shown in Figure 5(b). The values estimated for sensitivity and specificity are presented in table 8.

The true positive rates will be plotted along the Y axis and false positive rates will be plotted along the X axis. Hence, an ROC is defined by TRP and FPR. The ROC curve shown in Figure 6, illustrates no false negatives and no false positives on the left upper coordinate (0, 1).

A probability threshold has been used to classify the trust/distrust values. The values are classified based on probability. When the probability shoots the threshold it gets into class 1 (trust) and as it becomes low, class 0 (distrust). The group discrimination can also point some errors in certain cases. A ROC graph is constructed for all the three trust computation techniques described above. The computations are done for many varying thresholds. The ROC curve in Figure 6 showcases the area under curve (AUC) for all DTC, RTC and HTC. The graph with the highest AUC portion is the best recommended trust computation model. Hence, RTC

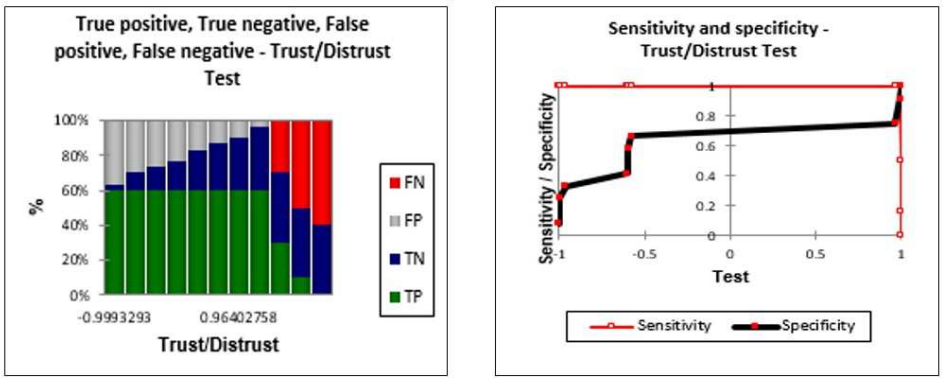

Figure 5: Benchmarking results

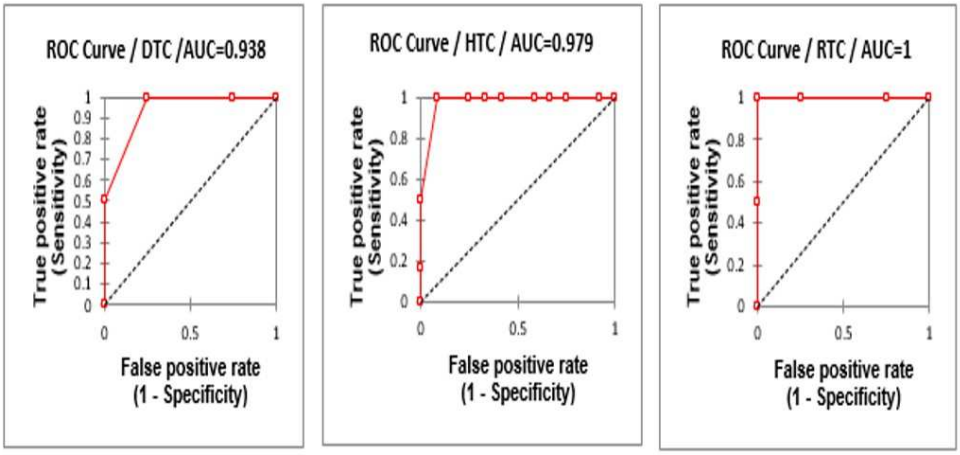

Figure 6: ROC Curve benchmarked on trust computations

Table 8: ROC analysis (Sensitivity vs Specificity)

Trust/Distrust	Sensitivity	Low (95%)	Up (95%)	Specificity	Low (95%)	Up (95%)
-0.999	1.000	0.789	1.000	0.083	0.000	0.379
-0.995	1.000	0.789	1.000	0.250	0.085	0.540
-0.964	1.000	0.789	1.000	0.333	0.138	0.612
-0.600	1.000	0.789	1.000	0.417	0.194	0.681
-0.597	1.000	0.789	1.000	0.583	0.319	0.806
-0.578	1.000	0.789	1.000	0.667	0.388	0.862
0.964	1.000	0.789	1.000	0.750	0.460	0.915
0.995	1.000	0.789	1.000	0.917	0.621	1.000
0.999	0.500	0.291	0.709	1.000	0.713	1.000
1.000	0.167	0.052	0.402	1.000	0.713	1.000

is pronounced as the best recommended trust computation to be adopted for trust management and is benchmarked with experimental results.

The complete ROC analysis is highlighted in Table 8, where the upper bound and lower bound of the sensitivity, specificity are specified. The negative/positive trust values are mapped towards both FPR and TPR. The upper/lower bounds ensure the trustworthiness for the received trust values between the nodes.

7 Conclusion and future enhancements

In this research, we have quantified the trust metrics between nodes in heterogeneous distributed network. We have defined three possible distributed trust computation strategies, we make an effort to zero-in on the best one and describe its performance by substantiating with highly accurate trustworthiness. The nodes in HDNs demonstrate trustworthiness among the participating nodes using DTC, RTC or HTC. The trust evaluation is performed and trust metrics are shared and recommended among the participating nodes. The trust values are measured using discrete/continuous series. The dataset from www.trustlet.org when computed with DTC, HTC and RTC delivers appropriate values for TP, TN, FP and FN. When the computed values of TPR and FPR are plotted on a ROC, the AUC presents itself. The AUC (area under curve) values are 0.938, 0.979 and 1.000 for DTC, HTC and RTC respectively. Interpreting the ROC graph with respective AUC regions, we conclude that the Recommendation Trust Computation (RTC) delivers a highly accurate trustworthiness score when compared with the other two trust computations. Hence, the RTC techniques trust computation performance is benchmarked with appropriate experimental results and we declare that RTC delivers promising trustworthiness and is more reliable over DTC and HTC. In future, we plan to extend recommendation trust computation (RTC) in VANETs to eliminate malicious entries and secure the vehicular network appropriately. The next step is to extend our research further ahead to include more efficient and dynamic approaches for trust computing, ensuring a high degree of trustworthiness.

Acknowledgments

This research was supported by the Roadway, Transportation, and Traffic Safety Research Center (RTTSRC) of the United Arab Emirates University (grant number 31R058).
Data for this study comes from www.trustlet.org. The dataset holds 841,372 trust observations

with 717,667 trusts and 123,705 distrusts, which is archived at
$http://www.trustlet.org/datasets/extended_epinions/userrating.txt.gz$.

The Trustlet, open research datasets on trust metrics has been cited by some researchers. Reference: P. Massa, K. Souren, M. Salvetti, D. Tomasoni. Scalable Computing: Practice and Experience.

Bibliography

[1] Babu S.S., Raha A., Naskar M.K. (2011); Geometric mean based trust management system for WSNs (GMTMS), *Information and Communication Technologies (WICT)*, 444-449, 2011.

[2] Bao F., Chen R., Chang M., Cho J.H. (2012); Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, *IEEE Transactions on Network and Service Management*, 9(2), 69-83, 2012.

[3] Baronti P., Pillai P., Chook V.W., Chessa S., Gotta A., Hu Y.F. (2007); Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards, *Computer communications*, 30(7), 1655-1695, 2007.

[4] Chen Y.M., Wei Y.C. (2013); A beacon-based trust management system for enhancing user centric location privacy in VANETs, *Journal of Communications and Networks*, 15(2), 153-63, 2013.

[5] Chaurasia B.K., Verma S., Tomar G.S. (2013); Trust computation in VANETs, *2013 International Conference on Communication Systems and Network Technologies (CSNT)*, 468-471, 2013.

[6] Chang B.J., Kuo S.L. (2009); Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs, *IEEE Transactions on Vehicular Technology*, 58(4), 1846-63, 2009.

[7] Cho J.H., Swami A., Chen R. (2012); Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks, *Journal of Network and Computer Applications*, 35(3), 1001-12, 2012.

[8] Conti M., Giordano S. (2014); Mobile ad hoc networking: milestones, challenges, and new research directions, *IEEE Communications Magazine*, 52(1), 85-96, 2014.

[9] Cho J.H., Swami A., Chen R. (2011); A survey on trust management for mobile ad hoc networks, *IEEE Communications Surveys and Tutorials*, 13(4), 562-83, 2011.

[10] Dias J.A., Rodrigues J.J., Zhou L. (2014); Cooperation advances on vehicular communications: A survey, *Vehicular Communications*, 1(1), 22-32, 2014.

[11] Earle T.C. (2010); Trust in risk management: a model-based review of empirical research, *Risk Analysis*, 30(4), 541-74, 2010.

[12] Gazdar T., Rachedi A., Benslimane A., Belghith A. (2012); A distributed advanced analytical trust model for VANETs, *Global Communications Conference (GLOBECOM)*, 201-206, 2012.

[13] Hartenstein H., Laberteaux L.P. (2008); A tutorial survey on vehicular ad hoc networks, *IEEE Communications Magazine*, 46(6), 164-171, 2008.

[14] Hanzo L., Tafazolli R. (2007); A survey of QoS routing solutions for mobile ad hoc networks, *IEEE Communications Surveys and Tutorials*, 9(2), 50-70, 2007.

[15] Khan Pathan A.S. (2010); *Security of self-organizing networks: MANET, WSN, WMN, VANET*, Auerbach Publications, 2010.

[16] Lee U., Gerla M. (2010); A survey of urban vehicular sensing platforms, *Computer Networks*, 54(4), 527-44, 2010.

[17] Li F., Wang Y. (2007); Routing in vehicular ad hoc networks: A survey, *IEEE Vehicular Technology Magazine*, 2(2), 12-22, 2007.

[18] Li W., Song H. (2016); ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks, *IEEE Transactions on Intelligent Transportation Systems*, 17(4), 960-9, 2016.

[19] Minhas U.F., Zhang J., Tran T., Cohen R. (2011); A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks, *IEEE Transactions on Systems, Man, and Cybernetics*, 41(3), 407-20, 2011.

[20] Momani M., Aboura K., Challa S. (2007); RBATMWSN: recursive Bayesian approach to trust management in wireless sensor networks, *Intelligent Sensors, Sensor Networks and Information, 2007*, 347-352, 2007.

[21] Mali G., Misra S. (2016); TRAST: Trust-Based Distributed Topology Management for Wireless Multimedia Sensor Networks, *IEEE Transactions on Computers*, 65(6), 1978-91, 2016.

[22] Oliveira L.M, Rodrigues J.J.(2011); Wireless Sensor Networks: A Survey on Environmental Monitoring, *JCM*, 6(2), 143-51, 2011.

[23] Pantazis N.A, Nikolidakis S.A., Vergados D.D. (2013); Energy-efficient routing protocols in wireless sensor networks: A survey, *IEEE Communications Surveys and Tutorials*, 15(2), 551-91, 2013.

[24] Ren Y., Zadorozhny V.I, Oleshchuk VA, Li F.Y. (2014); A novel approach to trust management in unattended wireless sensor networks, *IEEE Transactions on Mobile Computing*, 13(7), 1409-23, 2014.

[25] Rezende C., Boukerche A., Pazzi R.W., Rocha B.P., Loureiro A.A. (2011); The impact of mobility on mobile ad hoc networks through the perspective of complex networks, *Journal of Parallel and Distributed Computing*, 71(9), 1189-200, 2011.

[26] Shabut A.M., Dahal K.P., Bista S.K., Awan I.U. (2015); Recommendation based trust model with an effective defense scheme for MANETs, *IEEE Transactions on Mobile Computing*, 14(10), 2101-15, 2015.

[27] Tan S., Li X., Dong Q. (2016); A Trust Management System for Securing Data Plane of Ad-Hoc Networks, *IEEE Transactions on Vehicular Technology*, 65(9), 7579-92, 2016.

[28] Velloso P.B., Laufer R.P., Cunha D.D., Duarte O.C., Pujolle G. (2010); Trust management in mobile ad hoc networks using a scalable maturity-based model, *IEEE Transactions on Network and Service Management*, 7(3), 172-85, 2010.

[29] Yu H., Shen Z., Miao C., Leung C., Niyato D. (2010); A survey of trust and reputation management systems in wireless communications, *Proceedings of the IEEE*, 98(10), 1755-72, 2010.

[30] Zhao S., Aggarwal A., Frost R., Bai X. (2012); A survey of applications of identity-based cryptography in mobile ad-hoc networks, *IEEE Communications Surveys and Tutorials*, 14(2), 380-400, 2012.

[31] Zhang J. (2011); A survey on trust management for vanets, *Advanced Information Networking and Applications*, 105-112, 2011.

[32] Zouridaki C, Mark B.L, Hejmo M, Thomas R.K. (2005); A quantitative trust establishment framework for reliable data packet delivery in MANETs, *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, DOI: 10.3233/JCS-2007-15102, 1-10, 2005.

[33] Zhang J., Chen C., Cohen R. (2013); Trust modeling for message relay control and local action decision making in VANETs, *Security and Communication Networks*, DOI: 10.1002/sec.519, 6(1), 1-4, 2013.