INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, e-ISSN 1841-9844, 14(5), 660-671, October 2019.

Intrusion Detection for Mobile Ad Hoc Networks Based on Node Reputation

T. Lin, P. Wu, F.M. Gao, T.S. Wu

Tao Lin
1. School of Automation, Chongqing University, Chongqing 400044, China
2. Chongqing College of Electronic Engineering, Chongqing 401331, China
lintaoemail@126.com

Peng Wu*
1. School of Automation, Chongqing University, Chongqing 400044, China
2. Chongqing Chuanyi Automation Co., Ltd., Chongqing 401121, China
*Corresponding author: pwu@cqu.edu.cn

Fengmei Gao
Chongqing College of Electronic Engineering, Chongqing 401331, China
gfmemail@126.com

Tianshu Wu
College of Computer Science, Chongqing University, Chongqing 400044, China
723412117@qq.com

Abstract: The mobile ad hoc network (MANET) is more vulnerable to attacks than traditional networks, due to the high mobility of nodes, the weakness of transmission media and the absence of central node. To overcome the vulnerability, this paper mainly studies the way to detect selfish nodes in the MANET, and thus prevent network intrusion. Specifically, a data-driven reputation evaluation model was proposed to detect selfish nodes using a new reputation mechanism. The mechanism consists of a monitoring module, a reputation evaluation module, penalty module and a response module. The MANET integrated with our reputation mechanism was compared with the traditional MANET through simulation. The results show that the addition of reputation mechanism can suppress the selfish behavior of network nodes and enhance network security.
Keywords: Mobile ad hoc network (MANET), intrusion detection, reputation mechanism, node reputation.

1 Introduction

A mobile ad hoc network (MANET) is self-organized through the collaboration between numerous dynamic nodes, eliminating the need of fixed infrastructure or manual intervention [2] [3] [13]. In the MANET, multiple intelligent nodes are dynamically connected within a limited range. Each node at once serves as host and router, and can send and receive data. Thus, there is no central entity in the network.

The communication in the MANET is completed through the cooperation among network nodes. However, the cooperation failure may occur if the MANET is intruded. In this case, the

nodes will cease to route, send or receive data packets, which undermines the network performance.

Network intrusion cannot be prevented effectively by traditional security mechanisms, because such mechanisms are unable to eliminate the selfish, non-cooperative behavior of MANET nodes. This calls for new security mechanisms to protect network security. In the absence of pre-agreed trust relationship, reputation mechanism is a promising way to prevent network intrusion and non-cooperation of selfish nodes [5]. If the nodes in the network can't cooperate with each other, they can't route, send and receive data packets. It will seriously affect the performance of the network, and result in a great threat to the security of the network.

To suppress the selfish behavior of MANET nodes, this paper mainly calculates the reputation value, constructs a reputation mechanism, and applies the model to detect selfish nodes. The research results show that the proposed reputation mechanism can detect and deal with selfish behavior of nodes in time, and enhance the security performance of MANET. The most innovative point of this paper is to propose a data-driven reputation evaluation model to evaluate the reputation of nodes, and to detect selfish nodes through a new reputation mechanism.

2 Literature review

The security of ad hoc network has become a research hotspot in recent years. Many security mechanisms have been developed for ad hoc network. However, these mechanisms cannot be directly applied to the MANET. Thus, it is necessary to design a unique security mechanism that fits in with the MANET. Intrusion detection refers to identifying behaviors like the misuse of or attempt to exploit the vulnerabilities in preventive mechanism through persistent monitoring of events in the network. For the MANET, intrusion detection can be non-cooperative or cooperative [1]. Network intrusion is often accompanied by the selfish behavior of nodes. So far, the selfish behavior of MANET nodes has been deeply explored, giving birth to various solution. These solutions mainly rely on credibility, reputation or game.

Credibility-based solutions use virtual or real money to pay the network nodes for forwarding data to other nodes [11]. Camp et al. [4] designed a credibility-based system, which incentives nodes to forward data packets with virtual currency. Sun et al. [14] proposed a system that encourages mobile nodes to cooperate honestly, without needing to install tamper-proof hardware in any node. Patel et al. [10] pointed out the defects of credibility-based systems: the complete path from the source to the destination must be known in advance, i.e. adopting the source routing protocol.

Reputation-based solutions evaluate the reputation of each node according to its communication behavior. Each node uses the monitoring module to observe whether its neighbors forward packets from other nodes, and uses the response module to change or update the reputation table. The most famous reputation-based solution is the watchdog scheme [7], which detects whether a node is anomalous based on the packet forwarding of its neighbors. Pan et al. [9] presented a secure and objective credit-based incentive mechanism that encourages network nodes to transmit data packets and act more altruistically.

Game-based solutions draw on the features of the credibility- and reputation-based solutions, and take root in game theory model. Jaramillo et al. [6] modelled various interactions in wireless ad hoc networks as credibility- and reputation-based games, and analyzed the forwarding behavior of selfish nodes. Tang et al. [15] designed a self-learning repetitive game framework, in which each distributed node obeys research cooperation and development protocols. Umar et al. [16] created a coalition game-based method, in which the boundary nodes help the backbone nodes in the network to transmit information. Subramaniyan et al. [12] put forward a new

game theory solution to detect selfish nodes, and thus realized secure transmission of data in the network with a low cost and minimal idle time.

3 Data-driven reputation evaluation model

The distributed control structure is very suitable for the MANET. There are two types of distributed control structures, namely, fully distributed control structure (plane structure) and hierarchical distributed control structure (hierarchical structure) [8]. The plane structure and hierarchical structures of the MANET are shown in Figures 1 and 2, respectively.

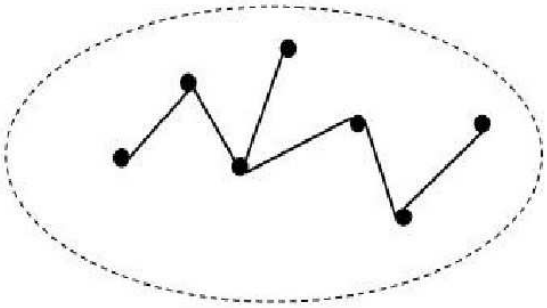

Figure 1: Plane structure of the MANET

In the plane structure, the network is rather simple and each node has equal status. This structure has high robustness and virtually no bottleneck. The network nodes are linked up via multiple paths, laying the basis for optimal routing and load balancing. However, the plane structure should not have too many nodes. Otherwise, the control overhead will increase markedly and the routing will be easily terminated. Hence, a plane structure with relatively few nodes is safe and suitable for small-scale MANETs.

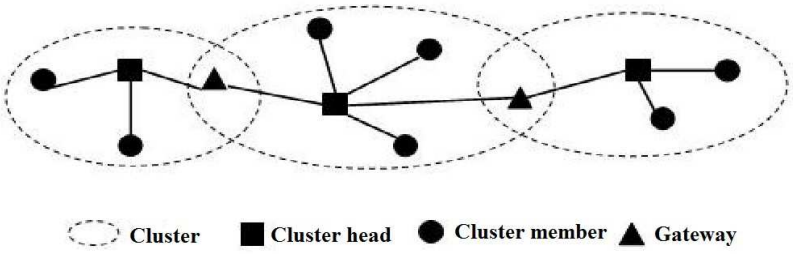

Figure 2: Hierarchical structure of the MANET

In the hierarchical structure, the MANET can be divided into multiple clusters, each of which consists of many members and one head node. The head node is mainly responsible for forwarding data between clusters, and can be set in advance or selected by algorithm. Unlike the head node, the member nodes do not need to save or update routing information, and thus enjoy high extensibility. Since the head node can be selected at any time, the hierarchical structure boasts a strong ability against destruction. Therefore, the hierarchical structure is appropriate for large-scale MANETs.

The special structure of the MANET makes the network vulnerable to multiple attacks. The attacks may come from the inside or outside of the network. The internal attacks may

occur when malicious network nodes attack the routing information or selfish nodes refuse to participate in routing. If the MANET is attacked by selfish nodes, the attacking nodes should be identified and disposed of rapidly, such as to protect network security and prevent outage.

As mentioned before, each node in the MANET has two roles: host and router. Due to the resource constraints, a MANET node may commit selfish behaviors to maximize its own interests. For example, the selfish node may refuse to participate in routing or forward data to other nodes. The selfish behaviors pose a serious threat to network performance.

The reputation mechanism can effectively suppress the selfish behavior of MANET nodes. To detect network intrusions, the reputation mechanism requires accurate evaluation of the reputation of network nodes. In this paper, a data-driven reputation evaluation model is proposed to compute, share, judge and update the reputation of each node.

In this model, when a normal node is requested to communicate with other nodes, it will firstly determine if the node requesting communication is trustworthy, and then choose a neighbor with high reputation value for routing communication, while updating its reputation table according to the situation of network communication; when a selfish node is requested to communicate with other nodes, it will forward data selectively without evaluate the reputation of the requester, which seriously undermines the network performance. Figure 3 explains the basic flow of communication two nodes in the proposed model.

In this paper, the calculation of node reputation is data-driven, i.e. the data were collected and processed, and updated iteratively for reputation calculation. In each iteration, the reputation value of a node was computed based on the real-time data being collected and classified. After time t, the node reputation was re-evaluated based on the reputation value in the previous iteration.

Suppose S is the source node of the communication request and D is the destination node of the communication request. If D is a normal node, node D calculates the reputation of S node according to the reputation evaluation process shown in Figure 3, and determines whether to communicate with it based on the S reputation value.

The features of ad hoc network determine that it takes more energy for a node to transmit data packets than to transmit routing packets. Thus, the reputation value of a node was calculated considering the number of data packets transmitted by the node. The classified data were computed directly to yield the reputation value of a node forwarding data packets (h_1), that of a node forwarding routing packets (r_1), that of a node receiving data packets (h_2) and that of a node receiving routing packets from other nodes (r_2). The four reputation values can be calculated by:

$$h_1 = \frac{N_{Tdata-others}}{N_{Tdata-self} + N_{Tdata-others}} \tag{1}$$

$$r_1 = \frac{N_{Tctrl-others}}{N_{Tctrl-self} + N_{Tctrl-others}} \tag{2}$$

$$h_2 = \frac{N_{Rdata-others}}{N_{Rdata-self} + N_{Rdata-others}} \tag{3}$$

$$r_2 = \frac{N_{Rctrl-others}}{N_{Rctrl-self} + N_{Rctrl-others}} \tag{4}$$

where $N_{Tdata-self}$ and $N_{Tdata-others}$ are the total number of packets generated by a node forwarding itself and forwarding other nodes, respectively; $N_{Tctrl-self}$ and $N_{Tctrl-others}$ are the total number of routing packets generated by a node forwarding itself and forwarding other nodes, respectively; $N_{Rdata-self}$ and $N_{Rdata-others}$ are the total number of packets a node receives from

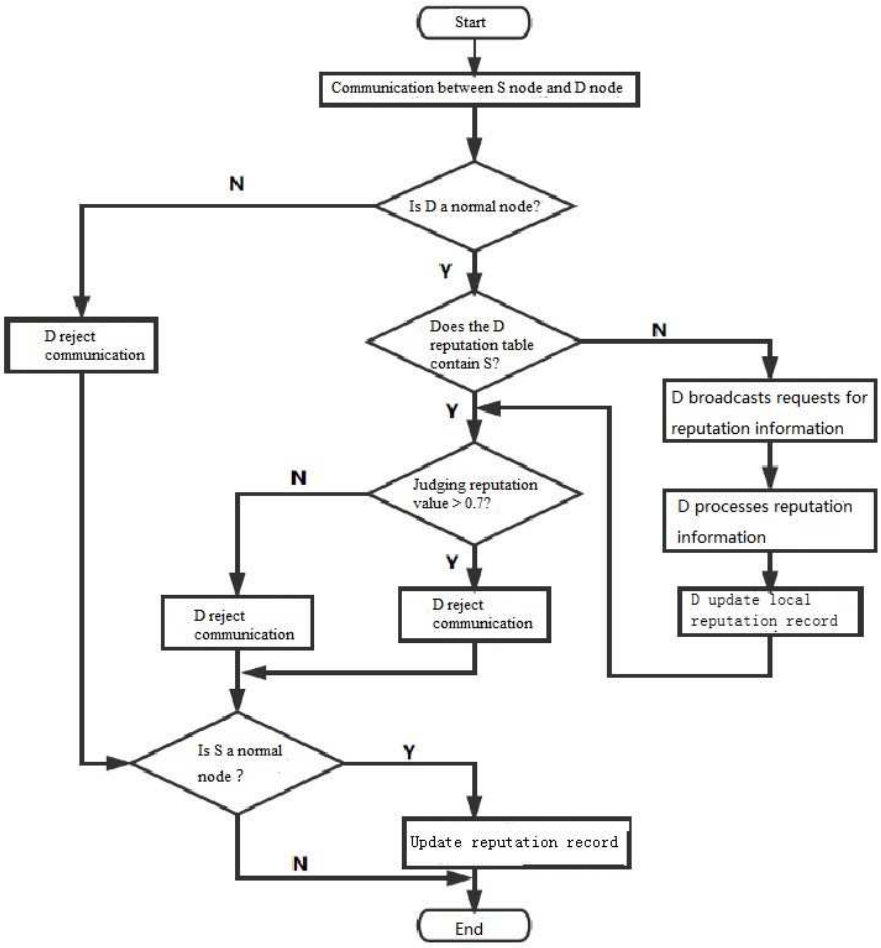

Figure 3: Basic flow of communication between two nodes

itself and from other nodes, respectively; $N_{Rctrl-self}$ and $N_{Rctrl-others}$ are the total number of routing packets a node receives from itself and from other nodes, respectively;

To calculate the reputation value of a node sending and receiving data packets to or from other nodes, h_1 and h_2 were added up to get the reputation value of the node sending and receiving data packets to or from monitored nodes. Similarly, r_1 and r_2 were added up to get the reputation value of the node sending and receiving routing packets to or from monitored nodes. The two reputation values can be defined as:

$$h_{data} = h_1 + h_2 \tag{5}$$

$$r_{control} = r_1 + r_2 \tag{6}$$

The direct reputation value of a node depends on the number of packets and the number of routing packets sent and received to or from other nodes.

Since an ad hoc network node consumes more energy to transmit data packets than to transmit routing packets, the weight factor ρ was introduced:

$$\rho = \frac{N_{Tdata} + N_{Rdata}}{N_{Tdata} + N_{Tctrl} + N_{Rdata} + N_{Rctrl}} \tag{7}$$

where N_{Tdata} and N_{Tctrl} are the total number of packets and routing packets forwarded by the node, respectively; N_{Rdata} and N_{Rctrl} are the total number of packets and routing packets received by the node, respectively. Then, the direct reputation value R_T of the node can be computed by:

$$R_T = \begin{cases} (1-\rho) \times h_{data} + \rho \times r_{control}, & 0 < \rho < 0.5 \\ \rho \times h_{data} + (1-\rho) \times r_{control}, & \rho \geq 0.5 \end{cases} \tag{8}$$

Let R_0 be the default reputation value of all network nodes, that is, the direct reputation value of each network node at time t. For a new node entering the network or each node at the start of network activity, the total direct reputation value of the node equals the default reputation value, i.e. $R_T = R_0$. After time t, the node can compute the reputation values of its neighboring by monitoring their communication behaviors. The new reputation value R_1, which equals R_T, can be computed by:

$$R_1 = \vartheta R_0 + (1-\vartheta) R_{p1} \tag{9}$$

where $\vartheta \in [0,1]$; R_{p1} is the reputation value of neighbors at time t. With the growing amount of information about node activity, the direct reputation value of the node will be updated periodically at a specific time. After time $t+1$, the new reputation value R_2 can be obtained by:

$$R_2 = \vartheta R_1 + (1-\vartheta) R_{p2} \tag{10}$$

The direct reputation value derived from the latest monitoring results can be defined as:

$$R_n = \vartheta^n R_0 + \vartheta^{n-1}(1-\vartheta) R_{p1} + \vartheta^{n-2}(1-\vartheta) R_{p2} + \cdots + \vartheta^{n-i}(1-\vartheta) R_{pi} \tag{11}$$

where n is a positive integer indicating the number of iterations.

This formula lays the basis for node reputation calculation in the MANET. In our model, each node stores the reputation values of other nodes in the local reputation table. The values recorded in the table are known as the local reputation values.

4 MANET intrusion detection based on node reputation

Based on the above reputation evaluation model, a novel reputation mechanism was developed to detect selfish nodes in the MANET and thus identify network intrusions. A penalty module and a response module were introduced to deal with abnormal nodes, and improve the evaluation of reputation values. The penalty module mainly compares the evaluated reputation values against the penalty rules, while the response module executes commands and deals with selfish nodes according to the message from penalty module and reputation evaluation. The workflow of the reputation mechanism after the addition of the two modules is described in Figure 4.

In the MANET, all the nodes are of equal status. There is no reliable third-party authentication authority, or preset trust relationship between the nodes. Therefore, the reputation value of a node can only be evaluated based on its communication status in the network. In our reputation mechanism, the reputation evaluation module is mainly composed of four processes: reputation calculation, sharing, judgment and updating. As shown in Figure 5, the module firstly processes data by data-driven method, then identifies the selfish network nodes, and finally submits the results to the penalty module.

The reputation evaluation module stores the evaluated reputation value in the reputation table, and regularly transmits the latest table to the penalty module. Next, the penalty module will process the message from the reputation evaluation module, get the corresponding evaluation results, and evaluate the trustworthiness of the node.

The reputation evaluation module also stores the total direct reputation value in the reputation table and updates the table regularly. If the target node forwards data and routing information to other nodes, its total reputation value will increase. Once a node is marked as an intrusive node, it will be blacklisted at once, and its information will be sent to the response module.

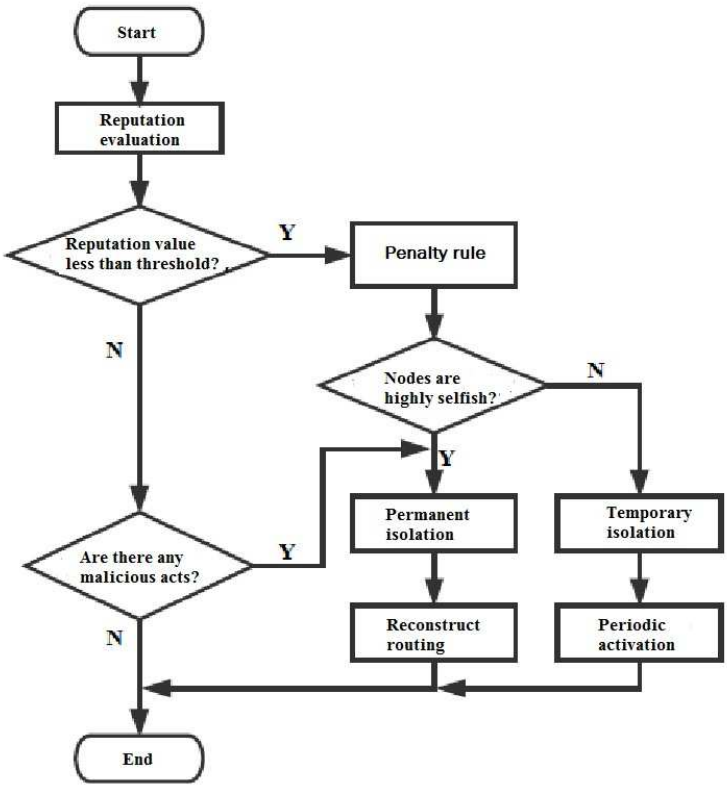

Figure 4: Workflow of the reputation mechanism after the addition of the two modules

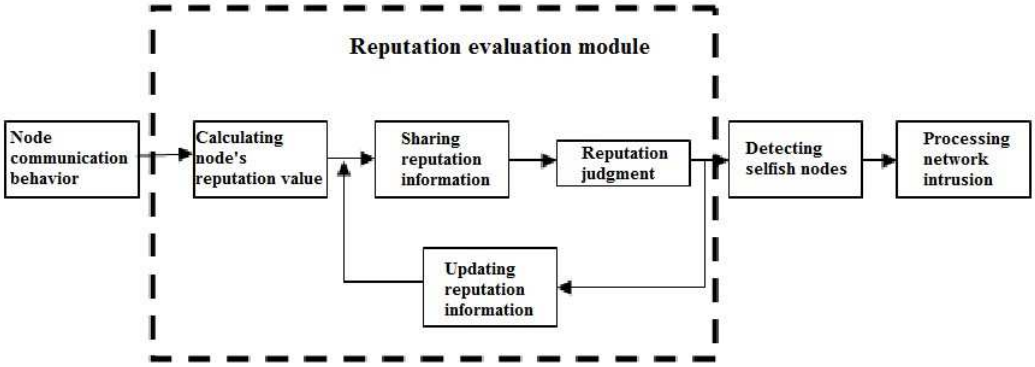

Figure 5: Workflow of reputation evaluation module

The response module mainly takes actions according to the messages from reputation eval-

uation module and penalty module. Once a node is judged as selfish, it will be added into the observation table of the penalty module, and then be processed by the response module. In general, the selfish nodes can be permanently isolated from the network or temporarily banned from the network. In this paper, it is proposed that a selfish node can join the network again but with limited times, that is, the node cannot enter the network beyond the set limit on the number of entries. The workflow of the response module is given in Figure 6 below.

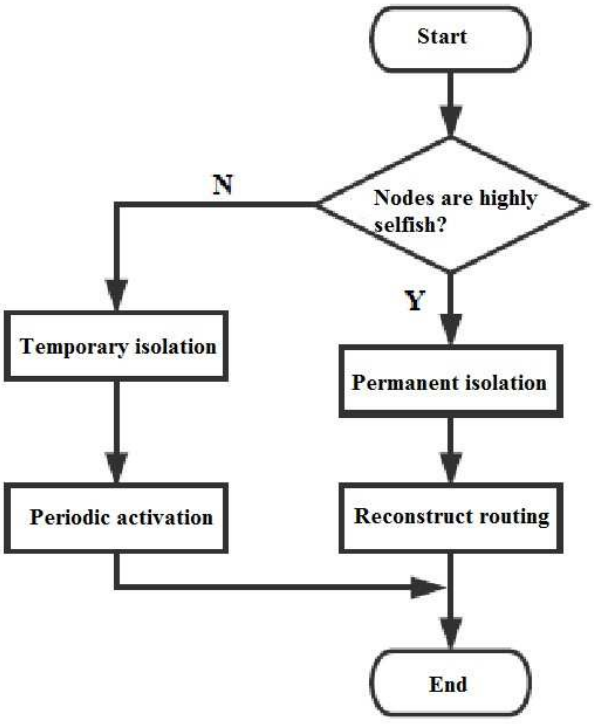

Figure 6: Workflow of the response module

5 Simulation experiment and performance analysis

To validate our reputation mechanism in Linux, the MANET was simulated on Network Simulator 2 (NS2), taking the dynamic source routing (DSR) as the routing protocol. The DSR protocol was simulated with and without reputation mechanism, both in the absence of selfish nodes and the presence of different number of selfish nodes. The parameters of the simulation environment are listed in Table 1 below.

As shown in Figure 7, the traditional DSR network delivered packets basically at the same rate with the DSR network integrated with reputation mechanism, in the absence of selfish nodes. This means the addition of the reputation mechanism has little effect on the delivery rate of packets.

As shown in Figure 8, with the growth in the number of selfish nodes, the packet delivery rates of both networks exhibited a gradual decline. The decline was steeper in the traditional DSR network, while the packet delivery rate in the network with reputation mechanism remained above 0.6. The possible reasons are as follows. In the traditional network, the selfish nodes only receive packets but do not forward packets, pushing up the resource consumption of normal nodes. Meanwhile, in the network with reputation mechanism, the selfish nodes are effectively

Table 1: Parameters of the simulation environment

Parameters	**Value**
Simulation area	900m*900m
Number of nodes	50
Propagation model	Two-Ray Ground Reflection
Packet size	512 bytes
MAC type	802.11
Signal coverage radius	300m
Maximum number of connections	20
ϑ	0.15

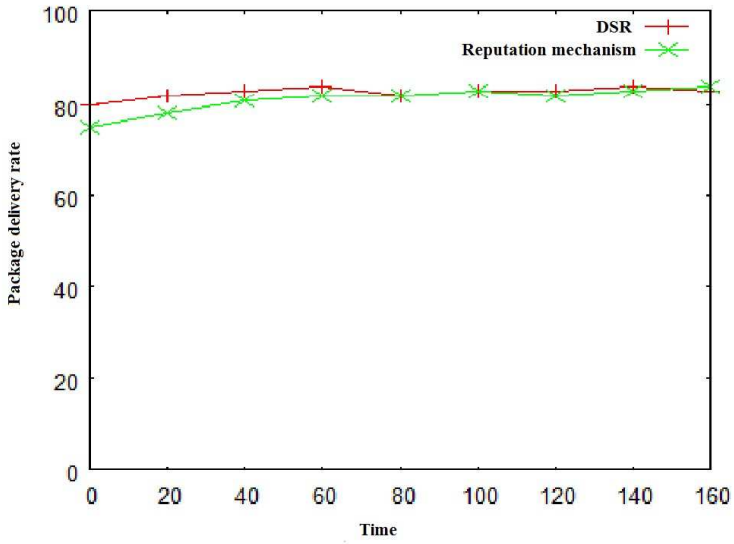

Figure 7: Relationship between packet delivery rate and time

removed and isolated.

As shown in Figure 9, the routing overheads in both networks were gradually falling, with the growth in the number in selfish nodes. The decline of routing overheads can be attributed to the following facts: With the elapse of time, the network nodes will establish routing paths and store routing information with each other, thus reducing the routing overhead. Of course, the network with reputation mechanism had a slightly lower routing overhead than the traditional network.

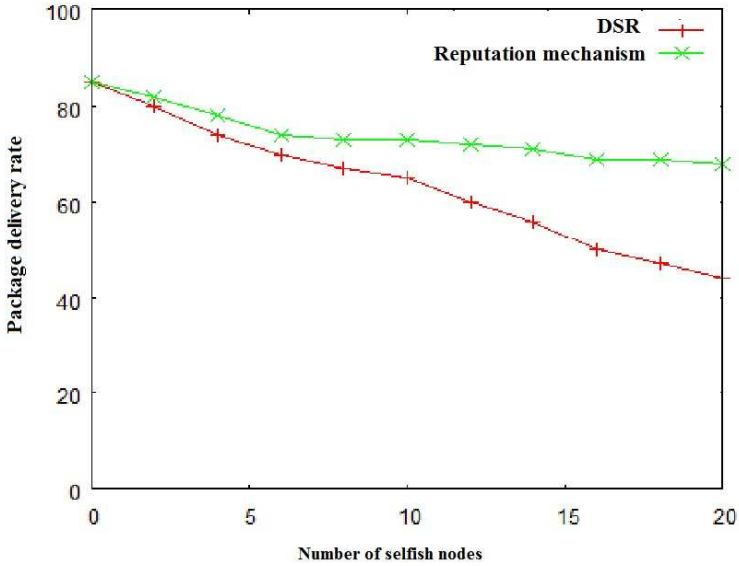

Figure 8: Relationship between packet delivery rate and the number of selfish nodes

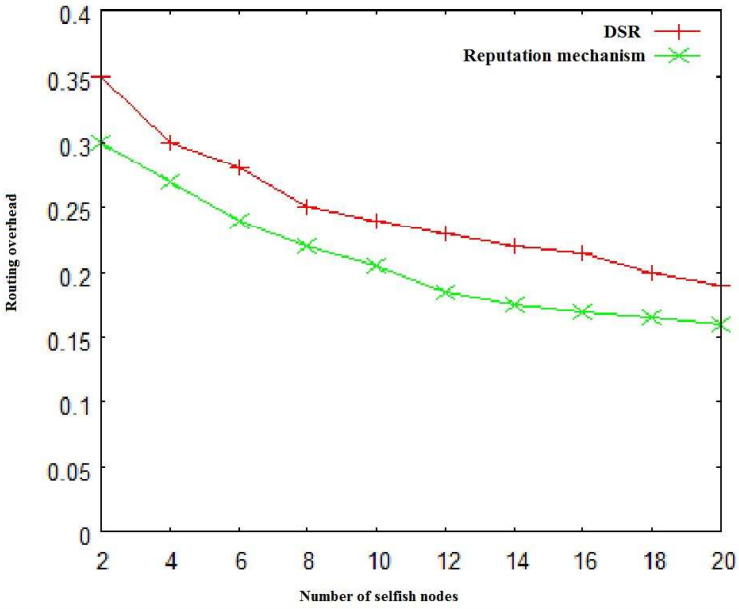

Figure 9: Relationship between routing overhead and the number of selfish nodes

6 Conclusion

This paper mainly studies the way to detect selfish nodes in the MANET, and thus prevent network intrusion. Specifically, a data-driven reputation evaluation model was proposed to detect selfish nodes. Then, based on the proposed model, a new reputation mechanism is proposed. The mechanism consists of a monitoring module, a reputation evaluation module, penalty module and a response module. The MANET integrated with our reputation mechanism was compared with the traditional MANET through simulation. The results show that the addition of reputation mechanism can suppress the selfish behavior of network nodes and enhance network security.

Funding

This work was supported by the Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant Numbers are KJ1602901 and KJQN201803102 respectively), Chongqing College of Electronic Engineering Scientific Research Project (Grant Number is XJZK201809) and Xinxiang Medical University Education and Teaching Reform Research Project (Grant Number is 2017-XYJG-41).

Author contributions. Conflict of interest

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

Bibliography

[1] Almousa, Z.; Nasir Q. (2015). cl-CIDPS: A cloud computing based cooperative intrusion detection and prevention system framework, *Communications in Computer & Information Science*, 523, 181-194, 2015.

[2] Al-Sultan, S.; Al-Doori, M. M.; Al-Bayatti, A. H.; Zedan, H. (2014). A comprehensive survey on vehicular Ad Hoc network, *Journal of Network & Computer Applications*, 37(1), 380-392, 2014.

[3] Azees, M.; Jegatha, D. L.; Vijayakumar, P. (2016). A comprehensive survey on security services in vehicular ad-hoc networks (VANETs), *IET Intelligent Transport Systems*, 10(6), 379-388, 2016.

[4] Camp, T.; Boleng, J.; Davies, V. (2002). A survey of mobility models for ad hoc network research, *Wireless Communications and Mobile Computing*, 2(5), 483-502, 2002.

[5] He, S.; Chen, J.; Li, X.; Shen, X. M.; Sun, Y. X. (2012). Leveraging prediction to improve the coverage of wireless sensor networks, *IEEE Transactions on Parallel & Distributed Systems*, 23(4), 701-712, 2012.

[6] Jaramillo, J. J.; Srikant, R. (2010). A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks, *Ad Hoc Networks*, 8(4), 416-429, 2010.

[7] Moati, N.; Otrok, H.; Mourad, A.; Robert, J. M. (2014). Reputation-based cooperative detection model of selfish nodes in cluster-based QoS-OLSR protocol, *Wireless Personal Communications*, 75(3), 1747-1768, 2014.

[8] Moussaoui, A.; Semchedine, F.; Boukerram, A. (2014). A link-state QoS routing protocol based on link stability for mobile Ad Hoc networks, *Journal of Network & Computer Applications*, 39(1), 117-125, 2014.

[9] Pan, D.; Zhang, H.; Chen, W. J.; Lu, K. (2015). Transmission of multimedia contents in opportunistic networks with social selfish nodes, *Multimedia Systems*, 21(3), 277-288, 2015.

[10] Patel, N.; Srivastava, S. (2012). Packet forwarding strategies for cooperation enforcement in mobile Ad Hoc wireless networks, *Lecture Notes in Computer Science*, 7154, 200-211, 2012.

[11] Rodriguez-Mayol, A.; Gozalvez, J. (2014). Reputation based selfishness prevention techniques for mobile ad-hoc networks, *Telecommunication Systems*, 57(2), 181-195, 2014.

[12] Subramaniyan, S.; Johnson, W.; Subramaniyan, K. (2014). A distributed framework for detecting selfish nodes in MANET using record- and trust-based detection (RTBD) technique, *EURASIP Journal on Wireless Communications and Networking*, (1), 205-221, 2014.

[13] Sun, G.; Bin, S. (2017). Router-level internet topology evolution model based on multi-subnet composited complex network model, *Journal of Internet Technology*, 18(6), 1275-1283, 2017.

[14] Sun, J.; Zhang, C.; Zhang, Y.; Fang, Y. G. (2011). SAT: A security architecture achieving anonymity and traceability in wireless mesh networks, *IEEE Transactions on Dependable and Secure Computing*, 8(2), 295-307, 2011.

[15] Tang, C.B.; Li, X.; Wang, Z. (2017). Cooperation and distributed optimization for the unreliable wireless game with indirect reciprocity, *Science China (Information Sciences)*, (11), 129-145, 2017.

[16] Umar, R.; Mesbah, W. (2018). Throughput-efficient coalition formation of selfish/altruistic nodes in ad hoc networks: A hedonic game approach, *Telecommunication Systems*, 67(1), 1-17, 2018.