Behavioral Feature and Correlative Detection of Multiple Types of Node in the Internet of Vehicles

Pengshou Xie[1], Guoqiang Ma[1, *], Tao Feng[1], Yan Yan[1, 2] and Xueming Han[1]

Abstract: Undoubtedly, uncooperative or malicious nodes threaten the safety of Internet of Vehicles (IoV) by destroying routing or data. To this end, some researchers have designed some node detection mechanisms and trust calculating algorithms based on some different feature parameters of IoV such as communication, data, energy, etc., to detect and evaluate vehicle nodes. However, it is difficult to effectively assess the trust level of a vehicle node only by message forwarding, data consistency, and energy sufficiency. In order to resolve these problems, a novel mechanism and a new trust calculating model is proposed in this paper. First, the four tuple method is adopted, to qualitatively describing various types of nodes of IoV; Second, analyzing the behavioral features and correlation of various nodes based on route forwarding rate, data forwarding rate and physical location; third, designing double layer detection feature parameters with the ability to detect uncooperative nodes and malicious nodes; fourth, establishing a node correlative detection model with a double layer structure by combining the network layer and the perception layer. Accordingly, we conducted simulation experiments to verify the accuracy and time of this detection method under different speed-rate topological conditions of IoV. The results show that comparing with methods which only considers energy or communication parameters, the method proposed in this paper has obvious advantages in the detection of uncooperative and malicious nodes of IoV; especially, with the double detection feature parameters and node correlative detection model combined, detection accuracy is effectively improved, and the calculation time of node detection is largely reduced.

Keywords: IoV, behavioral feature, double layer detection feature, correlation analysis, correlative detection model.

1 Introduction

Internet of Vehicles is used as a typical application of the Internet of Things in the transportation field, aiming to realize an integrated intelligent transportation system [Sun,

[1] School of Computer and Communications, Lanzhou University of Technology, Lanzhou, 730050, China.

[2] Department of Computing, Faculty of Science and Engineering, Macquarie University, Sydney, NSW 2109, Australia.

[*] Corresponding Author: Guoqiang Ma. Email: magq1514@163.com.

Received: 15 January 2020; Accepted: 17 April 2020.

CMC. doi:10.32604/cmc.2020.09695 www.techscience.com/journal/cmc

Wu and Wu (2017); Nebbou, Lehsaini and Fouchal (2018); Zhao, Liu and Guo (2018)]. It is used to realize the dissemination of information, communication between nodes, and improve traffic safety and efficiency [Horng, Tzeng and Li (2017); Cao, Yang and Zuo (2017); Zeng, He and Chen (2018)].

However, the Internet of Vehicles is a wireless self-organizing network. The network's highly dynamic connection, unstable network topology, sensitive information sharing, time sensitivity and communication environment provide an opportunity for illegal nodes to launch attacks and obtain illegal benefits. For example, malicious nodes spread false information to disrupt traffic; in order to save their own energy, some selfish nodes refuse to forward information sent by other nodes, resulting in the inability to transfer key information and greatly reduce network transmission performance. The traditional security mechanism mainly relies on a trusted third party, namely the certificate authority (CA) for encryption and verification, to achieve secure network access, thereby ensuring the reliability of communication. But traditional security mechanisms can not solve the malicious behavior of nodes the network. In mobile ad hoc networks, trust and reputation are mainly used as an important means to ensure the security of autonomous networks. Many researchers have also proposed related trust management models for detecting malicious nodes. The trust parameters are mainly divided into direct trust parameters and recommended trust parameters. However, most of the recommended trusts use node passed recommendations, which are more complicated to calculate and increase the delay [Arsalan and Rehman (2018)]. It is difficult to meet the requirements for vehicles to quickly detect malicious nodes during high speed movement.

Therefore, designing reasonable detection feature parameters and studying the behavioral features of nodes are of great significance to solve the safety problem and promote the development of the IoV.

2 Related works

For a long time, safety issues have always been an important issue, and they have seriously restricted the promotion and application of Internet of Vehicles. The current main research directions include trust models, behavior monitoring, metrics, trust rating, trust calculation, application scenarios, and adaptability.

The communication parameter calculates the trust value based on whether the information is forwarded or not. Data parameters determine whether a node is trustworthy based on whether the perceived data is consistent with other nodes. The energy parameter determines the credibility of the node based on whether the remaining energy of the node can complete the normal task [Ramadan, Tawfik and Riad (2018)]. Commonly used indicators include the routing forwarding rate and the packet forwarding rate. According to the above three trust measurement elements, Liu [Liu (2019)] defines trust as each specific operation in the network, such as controlling the trust of packet forwarding and the trust of data packet forwarding, and performing trust evaluation based on direct evidence of these measurement options; Borkar et al. [Borkar and Mahajan (2017)] added the consideration of time when considering the forwarding rate, which was measured by the forwarding rate and window forwarding rate; Zhu et al. [Zhu, Wang and Yang (2018)] aiming at the fuzziness of node trust evaluation and the dynamic evolution of trust decision in spatial information network, a network node trust evolution model based on fuzzy correlation measures is proposed; Najib et al. [Najib and Sulistyo (2019)] addresses a survey of trust calculation models for IoT systems, i.e., what are available models or methods used by researcher to compute trust in IoT system. In addition, classification is also developed to categorize trust calculation model using five parameters including trust metric, trust source, trust algorithm, trust architecture, and trust propagation; He et al. [He, Yu, Chen et al. (2017)] aiming at the multi-dimensional and polymorphic characteristics of IoT data, a data processing process from XML metadata description to relational database storage was designed on the service oriented IoT data management framework; Wei [Wei (2019)] based on the video surveillance data and RFID data as the monitoring data, the ARM embedded platform and the ethereum blockchain platform are integrated into the video surveillance, smart contract and other technologies to complete the collection, processing, uploading, storage, and query of surveillance data.

However, just whether the information is forwarded, whether the data is consistent, and whether the maximum remaining energy is used as the basis for behavior detection is not enough to reflect the trustworthiness of the node, because the actual behavior of the node is normal and whether it is offensive. Elements, data elements, and energy elements more directly reflect whether the node should be trusted in the network.

Therefore, this paper combines the special environment of the Internet of Vehicles and the requirements for rapid detection of malicious nodes. First, the common node types in the Internet of Vehicles are summarized, then a quaternary representation to describe the IoT nodes qualitatively is designed; finally, the double layer detection feature parameters are designed, and an association detection model is constructed.

3 Types of node and behavioral feature in the IoV

3.1 Types of node and description

According to the impact of nodes on the security of the Internet of Vehicles, the nodes can be divided into three types: normal nodes, non-cooperative nodes, and malicious attack nodes.

A normal node is a node that is active in the network and is willing to forward data for other nodes [Huang, Cai and Qu (2018)]. A non-cooperative node is a self-contained node and is unwilling to provide routing request packets and packet forwarding nodes for other nodes [Wang, Jiang and Zhao (2019)]. Malicious attack nodes include nodes that implement various attack behaviors, destroying route, and destroying data. Common attacks include: selective forwarding, Sybil attacks, etc. [Xin, Feng and Li (2017)].

In the Internet of Vehicles, these types of node may exist at the same time. Therefore, we first researched the nodes in the Internet of Vehicles and found that the nodes in the Internet of Vehicles generally have three attributes, as follows:

Member: Insider and Outsider.

An Insider is an authenticated node that can legitimately communicate with other members in the Internet of Vehicles, that is, the insider has a legitimate public key that can communicate within the network. The outsider does not obtain a legitimate public key that can communicate within the network. Members of the network can easily identify such a node and treat it as an intruder, refusing to communicate with it in order to achieve the purpose of strictly limiting the malicious attacks it generates.

Motivation: Blind and Rational.

The blind node does not focus on its own benefit from the attack the internal members of the network or the network function. Therefore, a very important feature of this type of attack node is that it may ignore the cost of launching the attack. On the contrary, the rational node chooses the corresponding attack mode in order to achieve its own benefit, so it has higher predictability than the blind node in terms of attack means and attack target.

Method: Active and Passive.

The active node can actively generate packets, while the passive node obtains the content it needs by eavesdropping on the wireless communication channel.

Based on the three attributes of nodes in the Internet of Vehicles, a four-tuple description method is designed to qualitatively describe the nodes in the Internet of Vehicles.

$$Node\ \left(Node\_ID,\ Member,\ Motivation,\ Method\right)$$

Here, the *Node_ID* is the unique identifier of the node, and the Member is identified by I_m and O_n, where m and n are both positive integers, the Motivation is identified by B and R, and the Method is identified by A and P. Therefore, the nodes studied in the paper are based on insider, rational and active nodes, such as Eq. (1).

$$Node\left(Node\_ID, I_m, R, A\right) \tag{1}$$

3.2 Behavioral feature and correlation analysis of nodes

In order to achieve the purpose of distinguishing node behavior and considering the enforceability of behavioral detection, the behaviors of various types of nodes commonly are studied, and the behavioral feature is analyzed in the IoV, as shown in Tab. 1.

The following is a detailed analysis of the behavioral feature of various types of node as middle nodes. Because the purpose of malicious nodes is to destroy the route or the data, in order to achieve its purpose, the malicious node will inevitably leave behavior traces to affect certain parameter statistics.

First, we define as follows:

Definition 1. Route forward rate: $R_r = \frac{n_{rf}}{n_{rr}}$, where, n_{rf} is the number of request packets actually forwarded, and n_{rr} is the number of request packets that need to be forwarded.

Definition 2. Data forward rate: $R_d = \frac{n_{df}}{n_{dr}}$, where, n_{df} is the number of packets actually forwarded, and n_{dr} is the number of packets that need to be forwarded.

Definition 3. Node data check result: V, where, V=0 means no change; V=1 means change.

Definition 4. Node i identity authentication result: A_i, where, A_i=0 means that node i has been registered, and qualified; A_i=1 means that node i has not been registered and failed.

Table 1: Behavioral feature of various nodes in the Internet of Vehicles

Behavioral types	Route phase		Data phase	
	Middle node	Behavioral feature	Middle node	Behavioral feature
Normal behavior	Receive request and forward	Route forward rate is higher	Receive and forward	Data forward rate is higher
Non-cooperative behavior	Receive request but not forward	Route forward rate is 0	Unable to establish route	Forward rate is 0
Malicious behavior	Receive request packet and response	Posing as other nodes to attract traffic	Eavesdrop, and tamper with data	Aggregation is not obvious, and throughput is large

Then, we analyze in detail the behavioral feature of each state node:

1) Normal behavior

A normal node is active in the network. As a middle node, it is willing to forward routing request packets and data packets for other nodes. Therefore, the normal behavior has a higher route forward rate and data forward rate, that is, the Eq. (2) is satisfied:

$$(R_r \geq R_{r0}) and (R_d \geq R_{d0}) \tag{2}$$

where, R_{r0} and R_{d0} are the normal minimum thresholds of the set route forward rate and the data forward rate respectively. If the threshold is lower than the normal minimum threshold, it is considered abnormal.

2) Non-cooperative behavior

A non-cooperative node is a self-serving node, and as a middle node, it is unwilling to forward routing request packets and data packets for other nodes. Therefore, the route forward rate and data forward rate of the non-cooperative behavior are very low, that is, the Eq. (3) is satisfied:

$$\left(0 < R_r < R_{r0}\right) and \left(0 < R_d < R_{d0}\right) \tag{3}$$

3) Malicious behavior

The main behavior of malicious attack nodes is that witch network attacks are the most common in the Internet of Vehicles.

In the Sybil attack, when a malicious node participates in network communication, it continuously declares its multiple identities to other nodes. The information falsified by the node will appear in various routing request packets or data packets in the network to establish a fake route. In fact, those nodes do not exist, and all data is sent to the nodes will be obtained by the wizard node. After receiving the data, the wizard node can arbitrarily eavesdrop, tamper, forge, and discard.

The nodes faked by the Sybil node can be divided into two categories: one is a node that is not in the Internet of Vehicles; the other is a node that is pretending to be in the Internet of Vehicles.

If all nodes are required to register when they are enrolled in the network, then the forged new node will definitely fail in identity authentication. If the Sybil node impersonates other nodes, their physical location must be different. At the normal node, the data forward rate and the data check value are definitely normal. At the node where the Sybil node is impersonating, the low data forward rate is the packet loss behavior, and the data check value is changed.

Therefore, if node has two different physical locations, but it has the same ID, and the identity authentication result, the data forward rate, and the data check result satisfy the Eq. (4), the Sybil node can be more determined to be a malicious attack node.

$$\left(A_i = 0\right) and \left(\left(0 < R_d < R_{d0}\right) or \left(R_d \geq R_{d0}\right)\right) and \left(V = 1\right) \tag{4}$$

4 Detection feature and correlative detection model

4.1 Double layer detection feature

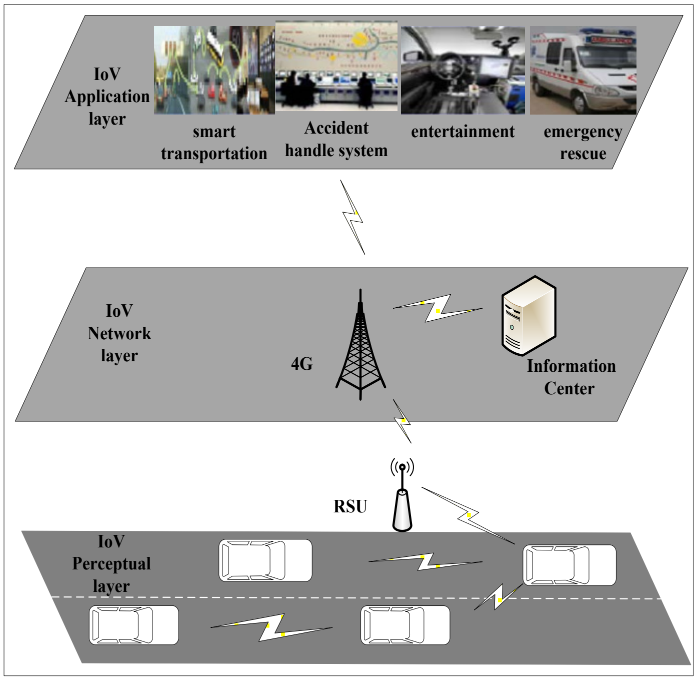

Figure 1: Architecture of the IoV

In the last section, we analyzed the behavioral feature of each state node in the Internet of Vehicles and found that there is a correlation between the behaviors.

Therefore, some typical behavioral features can be used as a detection criterion for monitoring and distinguishing between non-cooperative nodes, malicious attack nodes, and normal nodes. We combined the architecture of Internet of Vehicles [Rai, Yadav and

Sagar (2018)], as shown in Fig. 1.

And a double layer detection feature is designed, as shown in Fig. 2.

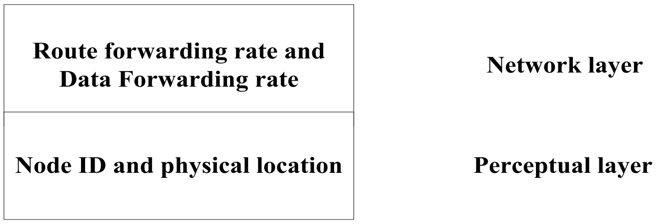
Route forwarding rate and Data Forwarding rate
Network layer
Node ID and physical location
Perceptual layer

Figure 2: Double layer detection feature

The detection features of the perceptual layer are mainly: the physical location of the node and the node ID; the detection features of the network layer are mainly: the route forward rate and the data forward rate.

4.2 Correlative detection model

Since most nodes in the Internet of Vehicles must be combined with multiple layer detection to make a correct distinction, a double layer correlative detection model is designed, as shown in Fig. 3.

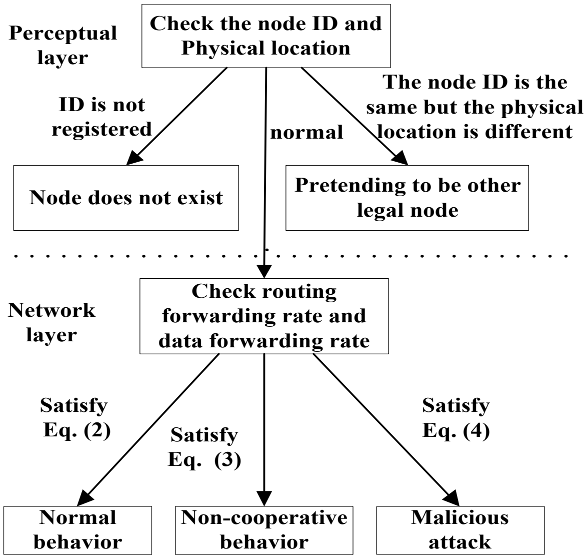
Perceptual layer
Check the node ID and Physical location
ID is not registered
normal
The node ID is the same but the physical location is different
Node does not exist
Pretending to be other legal node
Network layer
Check routing forwarding rate and data forwarding rate
Satisfy Eq. (2)
Satisfy Eq. (3)
Satisfy Eq. (4)
Normal behavior
Non-cooperative behavior
Malicious attack

Figure 3: Correlative detection model

Process 1: Perceptual layer detection. According to the behavioral feature of the node in the perceptual layer, we all know that the ID of the normal node must be registered and unique. Therefore, if the node ID is not registered, it is determined that the node is not forged. The ID of the node is registered, and the nodes with the same ID have different physical locations. In this case, the node is determined to be another legitimate node that impersonates.

Process 2: Network layer detection. After the perceptual layer is detected, the route forwarding rate and data forwarding rate of the node are checked at the network layer to determine whether there are obvious non-cooperative nodes and malicious attack nodes in the Internet of Vehicles. The judgment is based on: if the check result satisfies the Eq. (3), the node is judged to be a non-cooperative node, and if the Eq. (4) is satisfied, the node is judged to be a malicious attack node, otherwise if the Eq. (2) is satisfied, it is judged to be a normal node.

5 Simulation experiment and performance analysis

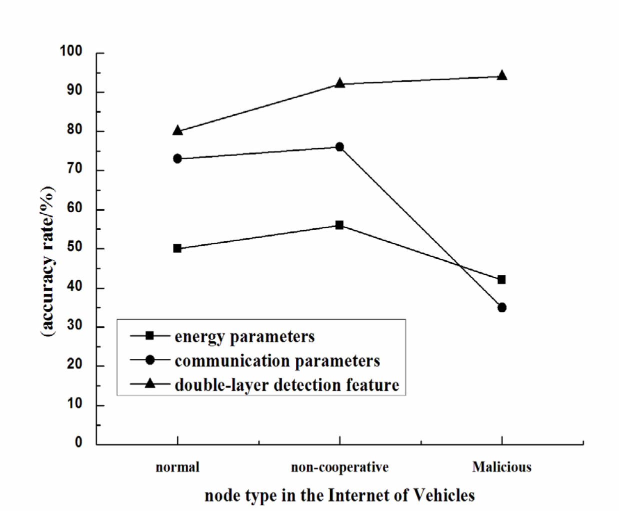

Figure 4: Comparison of accuracy rate of node behavior at medium speed in Internet of Vehicles

In order to verify the validity of the double layer detection features, we use the NS2 simulator to compare the energy and communication parameters [Priyan and Devi (2018)]. The data of the experiment came from the taxi company. Focusing on the detection rate and detection efficiency of non-cooperative behavior and malicious attack behavior, the detection accuracy rate refers to the ratio of correctly detecting the number of nodes and the total detection nodes, and the detection efficiency refers to the time required to detect the node category.

Fig. 4 shows the experimental comparison results based on energy parameters, communication parameters and double layer detection features in the Internet of Vehicles. It can be seen that when the network topology changes to medium speed, the detection accuracy rate of using double layer detection features is significantly higher than the other two parameters. Therefore, the double layer detection feature is extracted in this paper, it is better to detect multiple nodes in the Internet of Vehicles.

Fig. 5 shows the average time required for node detection when the Internet of Vehicles topology is at different speeds of change. It can be seen that when the topology change speed is medium and low speed, the required detection time is less, and at medium and high speeds, the required detection time is longer. This is because when the topology change speed in the Internet of Vehicles is low, the relationship between the nodes is relatively stable and easier to detect, while at medium and high speeds, the relationship between the nodes is rapidly changing, and the detection is relatively speaking. Thus, it is more difficult and the longer the time required.

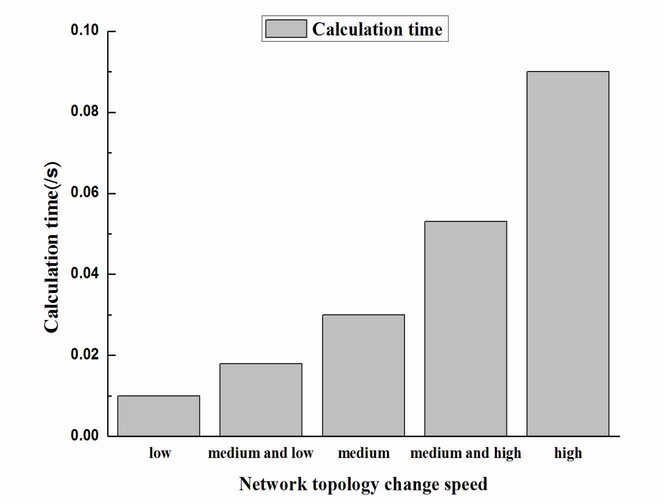

Figure 5: Calculation time required for network topology changes

As shown in Fig. 6, by comparing the method of this paper with the two methods of the reference [Sharma and Kaul (2018)] and the reference [Subba, Biswas and Karmakar (2018)], when the topology is at different speeds, three different methods are used to compare the calculation time required for vehicle node detection. It can be seen that when the network topology changes at a high speed, the calculation time of the three methods increases faster, but the calculation time of the correlative detection model in this paper is slightly lower than the other two methods.

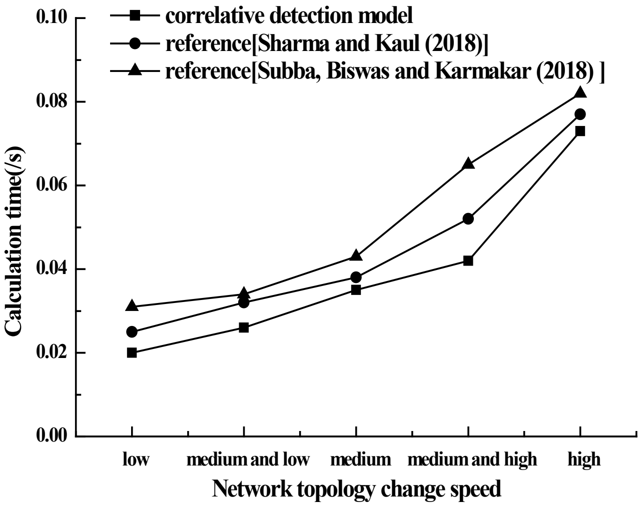

Figure 6: Calculation time corresponding to the three methods

6 Conclusion

Node detection is an effective way to solve the security problem of the Internet of Vehicles. Therefore, this paper first summarizes several common types of node in the Internet of Vehicles, and then analyzes their behavioral features. Finally, the correlative detection model is established to verify the effectiveness of the double layer detection feature. Simulation experiments show that the double layer detection feature, the detection of normal nodes, non-cooperative nodes and malicious attack nodes have high accuracy, and also verify that the detection time required for different network topology changes is also different. However, the following research deficiencies still exist in this paper: on the one hand, only the double layer detection feature is considered, and other features are not involved. On the other hand, only the node detection rate when the topology is at the medium speed is verified. Some researches have been done on the situation of medium and high speed and high speed. The shortcomings of these two aspects will be our future research tasks.

Funding Statement: This research is supported by the National Natural Science Foundations of China under Grants Nos. 61862040, 61762060 and 61762059. The authors gratefully acknowledge the anonymous reviewers for their helpful comments and suggestions.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Arsalan, A.; Rehman, R. A. (2018): Prevention of timing attack in software defined named data network with VANETs. *International Conference on Frontiers of Information Technology*, pp. 247-252.

Borkar, G. M.; Mahajan, A. R. (2017): A secure and trust based on demand multipath routing scheme for self-organized mobile ad-hoc networks. *Wireless Networks*, vol. 23, no. 8, pp. 2455-2472.

Cao, Y.; Yang, Z. Z.; Zuo, Z. Y. (2017): The effect of curb parking on road capacity and traffic safety. *European Transport Research Review*, vol. 9, no. 1, pp. 4.

He, Y. X.; Yu, T.; Chen, Y. Z.; Li, Q. A.; Fan T. R. (2017): Research on data storage and query mechanism in internet of things environment. *Computer Science*, vol. 42, no. 3, pp. 185-190.

Horng, S. J.; Tzeng, S. F.; Li, T. (2017): Enhancing security and privacy for identity-based batch verification scheme in VANETs. *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235-3248.

Huang, X. L.; Cai, Y.; Qu, C. W. (2018): Improved node detection algorithm for improved markov model. *Computer Engineering and Design*, vol. 39, no. 6, pp. 1586-1590.

Liu, B. T. (2019): Research on self-organizing network malicious node detection method based on trust evaluation. *Xi'an University of Electronic Technology*.

Najib, W.; Sulistyo, S. (2019): Survey on trust calculation methods in internet of things. *Procedural Computer Science*, vol. 161, pp. 1300-1307.

Nebbou, T.; Lehsaini, M.; Fouchal, H. (2018): An urban location service for vehicular area networks. *Concurrency & Computation Practice & Experience*, vol. 1, pp. 4693.

Priyan, M. K.; Devi, G. U. (2018): Energy efficient node selection algorithm based on node performance index and random waypoint mobility model in internet of vehicles. *Cluster Computing*, vol. 21, no. 1, pp. 213-227.

Rai, K. M.; Yadav, A.; Sagar, A. K. (2018): Security provision in VANETs using group based key share algorithm. *International Conference on Advances in Computing, Communication Control and Networking*, pp. 261-266.

Ramadan, H.; Tawfik, B. S.; Riad, A. E. M. (2018): Energy aware routing algorithm in manet using linear programming. *Computer Systems Science and Engineering*, vol. 33, no. 6, pp. 421-428.

Sharma, S.; Kaul, A. (2018): A survey on intrusion detection systems and honey pot based proactive security mechanisms in VANETs and VANET cloud. *Vehicular Communications*, vol. 12, pp. 138-164.

Subba, B.; Biswas, S.; Karmakar, S. (2018): A game theory based multi layered intrusion detection framework for VANET. *Future Generation Computer Systems*, vol. 82, pp. 12-28.

Sun, Y.; Wu, L.; Wu, S. (2017): Attacks and countermeasures in the internet of vehicles. *Annals of Telecommunications*, vol. 72, no. 5, pp. 283-295.

Wang, X. L.; Jiang, J. M.; Zhao, S. J. (2019): A fair blind signature scheme to revoke malicious vehicles in VANETs. *Computers*, *Materials & Continua*, vol. 58, no. 1, pp. 249-262.

Wei, Z. C. (2019): Monitoring data access and query system based on blockchain technology. *China University of Geosciences*.

Xin, Y.; Feng, X.; Li, T. T. (2017): Location dependent lightweight sybil attack detection method in VANET. *Journal of Communications*, vol. 38, no. 4, pp. 110-119.

Zeng, Y. M.; He, M.; Chen, Y. (2018): New approach for privacy aware location-based service communications. *Wireless Personal Communications*, vol. 101, no. 2, pp. 1057-1073.

Zhao, W.; Liu, J.; Guo, H. (2018): Edge node assisted transmitting for the cloud centric internet of things. *IEEE Network*, vol. 32, no. 3, pp. 101-107.

Zhu, L.; Wang, L.; Yang, Y. (2018): Research on evolutionary model for trust of nodes based on the fuzzy correlation measures. *Wireless Personal Communications*.