Forgery Node Detection Algorithm Based on Dynamic Reputation Value in the Internet of Vehicles

Peng-Shou Xie, Guo-Qiang Ma, Tao Feng, Yan Yan, and Xue-Ming Han
(Corresponding author: Guo-Qiang Ma)

School of Computer and Communications, Lanzhou University of Technology
No. 287 Lan gong ping road, Lanzhou, Gansu 730050, China
(Email: magq1514@163.com)

(Received Sept. 23, 2019; Revised and Accepted Jan. 15, 2020; First Online Feb. 5, 2020)

Abstract

Abnormal traffic messages may be sent by the internal forgery nodes to influence the normal behavior of other nodes in the Internet of Vehicles. However, the detection efficiency of the forgery nodes causing such attacks is generally low, and the accuracy of the detection algorithm is not high. Aiming at the above problems, the traffic messages published, forwarded and received by nodes are defined, and the effective features are extracted. On this basis, the forgery node detection model based on traffic messages is constructed, and the detection algorithm based on dynamic reputation value is designed. Finally, simulation experiments and performance analysis are completed. The results show that the time overhead of the detection algorithm is reduced, and the accurate detection rate of the detection algorithm is improved. It achieves the effect of quickly and accurately detecting the forgery nodes, and enhances the security of the Internet of Vehicles.

Keywords: Detection Algorithm; Detection Model; Dynamic Reputation Value; Forgery Node; Internet of Vehicles

1 Introduction

A special mobile ad hoc network is the Internet of Vehicles (IoV). Each vehicle is used as the message source to establish an information system that uses vehicles as nodes and communicates between people, vehicles and roads [19]. Its communication methods are mainly vehicles to vehicles (V2V) or vehicles to infrastructure (V2I). Road information (such as road congestion, collision accidents, *etc.*) is sent to nearby vehicles to realize timely sharing of traffic messages, in order to avoid potential accidents and enhance the safety of traffic roads [5]. Therefore, the Internet of Vehicles is widely used in the field of intelligent transportation. However, because of the wireless multi-hop communication, high mobility and the operation of vehicle nodes is limited, the security problem of the IoV is becoming more and more serious [11]. Among many security problems, abnormal and unreliable traffic messages by attackers are sent to surrounding vehicles to falsify traffic scenes, they damage the benefits brought by the application of the Internet of Vehicles, and even lead to more serious traffic accidents. This type of attack is called internal forgery node attack [21]. Then how to avoid the internal forgery node attack, ensure that the node can receive normal and reliable road traffic messages and select legal node to complete the service, which is one of the key issues in the research of the IoV.

In view of the safety of the IoV, many scholars at home and abroad have done a lot of research on this. At present, two types of detection schemes are proposed for internal attacks in the Internet of Vehicles.

1) Entity-based detection scheme. It is the judgment of the legal nodes through the communication between the node and other nodes. There are mainly identity-based authentication, trust-based evaluation and dynamic game-based schemes [14, 17, 20]. The advantages of such schemes are simple detection methods and low computational power requirements for processors. However, these schemes can only exert better detection performance when the number of normal nodes is more than the number of malicious nodes, otherwise its false detection rate is high.

2) Message-based detection scheme. It detects the abnormal message through the effective feature. There are mainly message authentication, deductive-based trust models, and message-based encryption schemes [2, 4, 15]. The advantage of such scheme is that it can avoid attacks caused by abnormal messages published or forwarded by the node. However, such these schemes can not detect and cull the nodes that send or forward abnormal messages, avoid continuing attacks in the future, and also has high time

overhead.

Therefore, in view of the shortcomings of the forgery node detection algorithm in the Internet of Vehicles, with the advantages of the existing two types of detection schemes, a forgey node detection algorithm based on dynamic reputation value (FNDA-IoV) is designed. Firstly, the effective features of the traffic messages of the Internet of Vehicles are described. The forgery node detection model of Internet of Vehicles is constructed. Secondly, the forgery node detection process of the Internet of Vehicles is extracted. Finally, the forgery node detection algorithm is designed to detect the internal forgery node of the Internet of Vehicles.

2 The Effective Features of Traffic Messages in the Internet of Vehicles are Described

The Internet of Vehicles plays an important role in traffic safety through the sharing and timely publishing of traffic messages. However, an open network environment, the complexity of road traffic, the numerous vehicle nodes and the fact that each node publishes or forwards a large number of various types of traffic messages at all times influence the security of the Internet of Vehicles [13]. In order to explain the problem more clearly, we define as follows:

Definition 1. *The traffic message type set is* $E=(e_1, e_2, e_3,..., e_n)$*, and* e_i *represents a certain type of traffic message published or forwarded by each node, such as emergency electronic brake lights (EEBL), post crash notification (PCN), road congestion notifyation (RCN),* etc.

Definition 2. *Traffic messages in the IoV can be divided into two types, namely* $\Theta = \{0, 1\}$*, where the "0" represents normal traffic messages and the "1" represents abnormal traffic messages. The normal traffic message refers to an instructive traffic message is published or forwarded by the legal node, and the abnormal traffic message refers to a malicious traffic message that is forged, falsified, published or forwarded by the forgery node. Here, it is assumed that the traffic messages published by the RSU are normal and trusted.*

Definition 3. *The set of vehicle nodes is* $V = (v_1, v_2,..., v_n)$*, vehicle nodes in the Internet of Vehicles broadcast traffic messages with digital signatures and public key certificates to other vehicle nodes in the process of traveling.*

Forgery node broadcasts abnormal messages means that the attacker changes the behavior of other nodes by publishing abnormal messages, tampering with real messages or injecting invalid messages [6,8,10]. For example, when a legitimate node receives a false alarm message, it may change its driving route, *etc.* As shown in Figure 1, the forgery node broadcasts an abnormal traffic message: the forgery node V_1 publishes or forwards an abnormal traffic message to the neighbor node V_2 to deceive the node V_2, and attempt to change the traveling path of the neighbor node V_2.

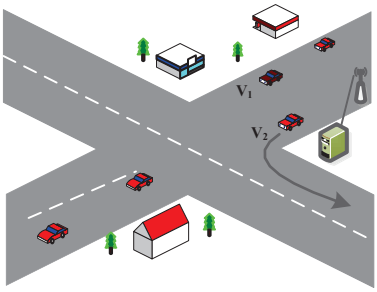

Figure 1: Forgery node broadcasts abnormal traffic messages

Since the features of traffic messages in the Internet of Vehicles have multiple dimensions, effective features (EF) in traffic messages are expressed in the form of a column vector, namely $EF = [x_1; x_2; x_3;...; x_n]$, then its corresponding data set (DS) can be expressed as $DS = \{(x_1, y_1), (x_2, y_2),..., (x_n, y_n)\}$, where $y_i \in \Theta$ represents the corresponding output result for the effective feature x_i, and n is the effective feature number. Table 1 lists the effective features in the traffic messages.

Therefore, the effective feature vector EF of the traffic messages in the Internet of Vehicles can be expressed as Equation (1).

$$EF = [e; d; v; a; t_0; s]. \quad (1)$$

3 Forgery node detection model in the Internet of Vehicles

The future behavior of vehicle nodes is uncertain, but the behavior trend of vehicle nodes can be predicted according to the historical behavior data of vehicle nodes. For this reason, the concept of trust is proposed in the nodes detection of Internet of Vehicles [9]. In human society, the trust is one of the most common concepts. Earlier, Mui *et al.* defined trust as follows: trust depends on experience and changes over time. When two people meet, their attitude towards each other is directly understood by the subject; The other is the recommender, neighbor node give recommendations based on own knowledge [1]. However, the evaluation of trust in social relations can also be carried out in the following ways: First, the subject directly determines the attitude toward the object according to the behavior of the object, and then feeds back its attitude to the third party who manages the subject and the object, and allows the third party to determine whether it continues to trust and whether it continues to exist in social relationships.

Therefore, referring to the trust evaluation method described above, the forgery node detection model as shown

Table 1: Effective features in traffic messages

number	feature	meaning
1	Sender(s)	The sender's identity type, including RSU (0) and vehicle node (1)
2	Time (t_0)	Timestamp of the sent traffic message
3	Direction(d)	The sender's direction of traveling
4	Vehicle (v)	The speed of the sender
5	Vehicle (a)	Sender's acceleration
6	Type(e)	Traffic message types, such as EEBL, PCN and RCN

in Figure 2 can be constructed. The model consists of three entities: A certificate authority (CA), a road side unit (RSU), and an on board unit (OBU) equipped with a vehicle. Among them, CA is responsible for distribution and revocation of certificates; RSU is responsible for publishing the normal and reliable traffic messages to vehicles within its communication scope; OBU is responsible for publishing, forwarding and receiving traffic messages [12].

However, in order to clearly illustrate the model, some connection parts are omitted here, such as the connection between the RSU and the CA. Where V_i is the node that publishes or forwards the traffic messages, and V_j is the node that receives the traffic messages.

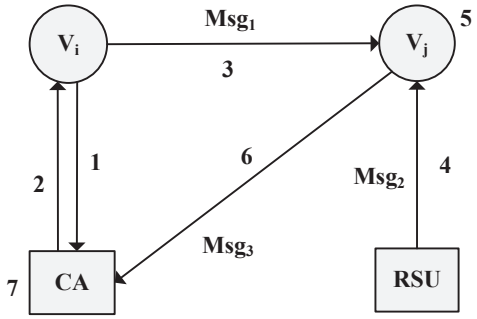

Figure 2: Forgery node detection model

Considering the non-repudiation of traffic messages, the effective feature of traffic messages, and the dynamics in the security requirements of the Internet of Vehicles, we design the communication message format as follows.

The communication messages between nodes are defined as follows:

$$Msg_1(Node\_Id_i,\ msgContent1_i).$$

Where $Node\_Id_i$ represents the node unique ID, and $msgContent1_i$ represents the traffic message sent by the node.

The communication messages sent by the RSU to the node is defined as follows:

$$Msg_2(Rsu\_Id_i,\ msgContent2_i)$$

Where Rsu_Id_i represents the RSU unique ID, and $msgContent2_i$ represents the traffic message sent by the RSU.

The feedback messages sent by the node to the CA is defined as follows:

$$Msg_3(Node\_Id_j,\ Node\_Id_i,\ \text{msgType}).$$

Where $Node\_Id_j$ represents the node unique ID of the receiving the traffic message, and $Node\_Id_i$ represents the node unique ID of the publishing or forwarding the traffic message. The $msgType$ is of the Boolean type, and the receiving node V_j informs the CA that the traffic message published or forwarded by the node V_i is normal (set to 0), or abnormal (set to 1).

Based on the above detection model, the seven steps are as follows:

Step 1. Node V_i requests a certificate from the CA. The node V_i needs to obtain communication and legal rights with other nodes in the network, and apply for a digital certificate to the CA according to its unique identity ID;

Step 2. The CA issues a certificate to V_i. The node V_i uses the digital certificate as an identifier that has communication authority in the network;

Steps 3, 4. Send the traffic message. The node V_i sends a traffic message $msgContent1_i$ to the node V_j, and the RSU sends a traffic message $msgContent2_i$ to the node V_j;

Step 5. Detect traffic messages. After receiving the traffic message of the node V_i, the node V_j starts detecting the traffic message according to the reliable traffic message sent by the RSU, and determines whether it is abnormal;

Step 6. Feedback to the CA. After the node V_j completes the detection of the traffic message published or forwarded by the node V_i locally, if the traffic message is normal, it is received; otherwise, it is discarded. At the same time, the node V_j sends a feedback message (Msg_3) to the CA;

Step 7. The CA updates the node reputation value (RV). The CA dynamically updates the reputation value of the node V_i according to the feedback message of the node V_j, and determines whether the node V_i is a forgery node.

4 Forgery Node Detection Process in the Internet of Vehicles

According to the above detection model, it can be seen that the forgery node detection process is as shown in Figure 3, and the specific detection steps are as follows.

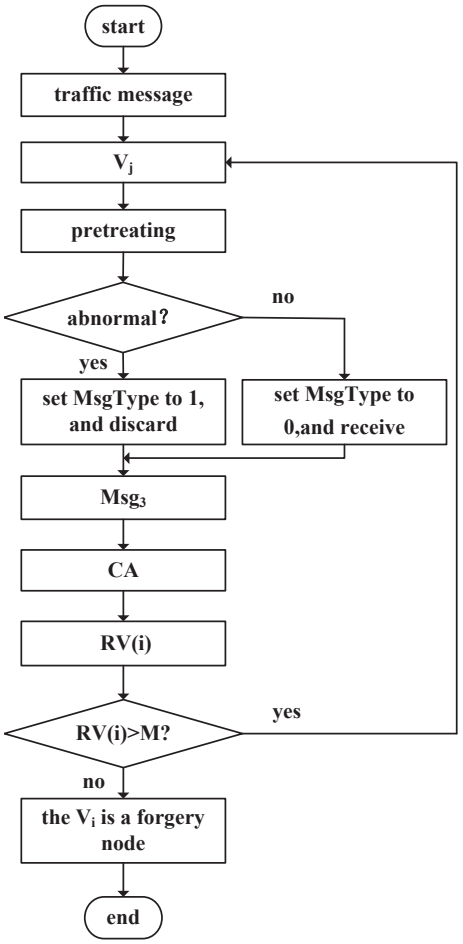

Figure 3: Forgery node detection process

Step 1. After receiving traffic message ($msgContent1_i$) and ($msgContent2_i$), the node V_j first preprocesses the traffic message according to the effective features of them;

Step 2. The node V_j performs a detection operation on the received traffic message. If it is a normal traffic message, it receives and sets the $msgType$ to 0. If it is an abnormal traffic message, it discards and sets the $msgType$ to 1. At the same time, the node V_j will send a feedback message (Msg_3) to the CA;

Step 3. After receiving feedback message, the CA updates the reputation value RV(i) of the node V_i, and compares the RV(i) with the threshold M, where M is the threshold of the node reputation, which can be set according to experience. If RV(i)>M, the CA continues to monitor its behavior; If RV(i)< M or RV(i)= M, then the node V_i is determined to be a forgery node, and the certificate issued to the node V_i is added to the revocation certificate list.

It can be seen that the detection process mainly includes three parts, namely, the traffic message is preprocessed, the traffic message is detected, and the node reputation value is dynamically updated.

4.1 Traffic Message Preprocessed

Preprocessing is to avoid the unnecessary computational overhead [22]. The traffic messages are preprocessed mainly from three aspects: the digital signature, the time validation, and the identity type verification. Firstly, the receiver verifies the integrity and non-repudiation of the traffic message by verifying the digital signature; then, using the batch authentication method to verify the timeliness, if the traffic message exceeds the time effective range, the traffic message is invalid, and the traffic message can be ignored. Finally, the traffic message sent by the RSU is used as a trained message, and the traffic message published or forwarded by the vehicle node is used as the detected message, as shown in Figure 4. The time validity of traffic messages is expressed as Equation (2):

$$t - t_0 < \Delta t. \tag{2}$$

Where t represents the time at which the node receives a traffic message, t_0 represents the time at which the traffic message was published or forwarded, and Δt represents the validity period of the traffic message.

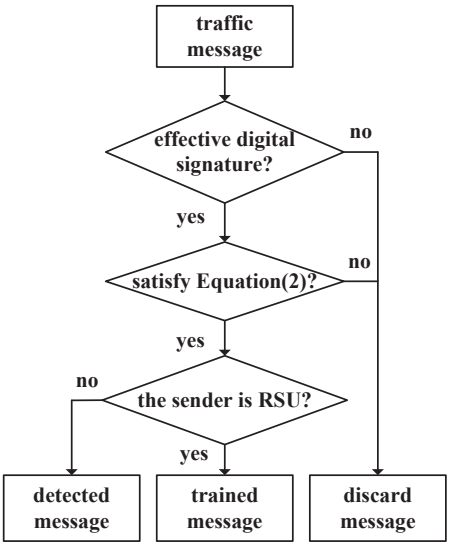

Figure 4: Traffic message preprocessed

4.2 Traffic Message Detected

At present, in the research field of intrusion detection algorithms, the main algorithms are the support vector machine (SVM), the clustering, naive bayes classifier(NBC),

the decision trees model (DTM), class association rules (CARS) and the deep learning [16]. The SVM is selected to realize the classification and detection of the traffic message in the Internet of Vehicles. The classification process is shown in Figure 5.

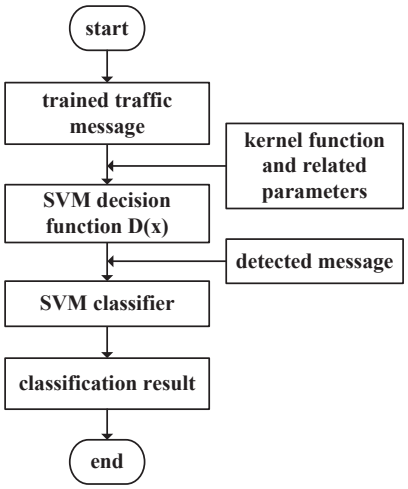

Figure 5: SVM classification process

The SVM algorithm classifies the traffic messages according to the effective feature vector EF of the multi-dimensional traffic message extracted by the Equation (1), and the classification result is a normal traffic message and an abnormal traffic message, where:
The SVM decision function is shown in Equation (3).

$$D(x) = sign[\sum_{i=1}^{n} \delta_i^* y_i K(x_i, x) + \theta^*]. \tag{3}$$

Where δ_i ($1 \leq i \leq$n) is the effective feature of the trained message x_i corresponds to the lagrangian factor, K($\bullet$) is the kernel function, and θ is the deviation.

The optimal classification hyperplane is shown in Equation (4).

$$\begin{cases} \phi(\omega, \varepsilon_i) = \frac{1}{2}||\omega||^2 + C\sum_{i=1}^{n} \varepsilon_i \\ y_i((\omega x_i) + b) \geq 1 - \varepsilon_i \qquad i = 1, 2, .., n \end{cases} \tag{4}$$

Where ε_i is the slack variable, C is the penalty factor, ω and b are the weight and threshold respectively, and n is the number of effective features of the traffic message.

4.3 Node Reputation Value Updated

After the traffic message is detected, the CA will automatically maintain a binary number based trust vector table to record the historical status of each node to publish or forward the traffic message based on the detection results of the node feedback. Currently, there are two methods for calculating the reputation value based on binary numbers: one is to calculate the reputation value according to the binary digital system, and the other is to calculate the reputation value by counting the number of the 0 or the 1 on the valid bit in the trust vector table [7].

Therefore, considering the features of the Internet of Vehicles, we design a new method for calculating the reputation value of the node by introducing the attenuation weights in combination with the existing two methods of calculating the reputation value.
The attenuation weight $g(k)$ represents the degree of attenuation of each bit in the binary valid bit in the trust vector table, and a valid bit represents a boolean judgment of the traffic message published or forwarded by node j to node i, the 1 and 0 respectively indicates an abnormal traffic message and a normal traffic message, and the conditions for satisfaction are as shown in Equation (5).

$$\sum_{k=1}^{m} g(k) = 1. \tag{5}$$

Where m is the number of the traffic messages communicated between nodes, and $0< g(k-1) < g(k) <1$.

Since the last calculated node reputation value should have different degrees of attenuation with traffic message detection time, the condition that the attenuation weight of the kth bit on the effective bit should satisfy is as shown in Equation (6).

$$g(k) = \frac{A}{t_t - t_k} \tag{6}$$

Where t_t is the current time, t_k is the time at which node j evaluates the kth the traffic messages sent by the node i, and A is the proportional coefficient.
Therefore, the calculation of the overall reputation value RV(i) of the node i can be expressed as shown in Equation (7).

$$RV(i) = 1 - \sum_{k=1}^{m} (\{1, 0\} * g(k)). \tag{7}$$

5 Forgery Node Detection Algorithm in the Internet of Vehicles

According to the above detection process, the designed the detection algorithm mainly includes:

Step 1. After receiving the traffic message, the node V_j preprocesses the message by using pre-processing function preTreat(), filters out the invalid traffic message, and verifies the identity of the sender. If the sender is an RSU, the traffic message to be sent is used as the trained traffic message. Otherwise, if the sender is a general vehicle node, the traffic message to be sent is used as the detected traffic message;

Step 2. The detected traffic message is sent as a parameter to the check() function, and traffic message is classified according to Equation (3) and Equation (4),

that is, when $D(x) = 0$, it is classified as a normal traffic message, and $msgType$ is set to 0. Otherwise, when $D(x) = 1$, it will be classified as an abnormal traffic message, and $msgType$ is set to 1;

Step 3. The vehicle node is determined by CA according to function isForgeryNode(), that is, if RV(i)> M, behavior is continuously monitored; otherwise, node V_i is determined to be the forgery node, and the certificate issued to node V_i is added to the revocation certifycate list. Among them, the main functions involved are:

1) PreTreat().
Preprocessing function.

```
Public void preTreat(String msg)
if (!imooc.jdkSign(msgNum)) then
  If the digital signature is incorrect, the
  node will discard the message discard();
else if (t − t0 > Δt) then
  /* If the Equation (2) is not met, the */
  /* message is discarded */
  discard();
else if (s==0) then
  /* If the sender is an RSU, the traffic */
  /* message is used as a training message */

  String trainMsg= msgContent2i ;
else
  /* If the sender is not an RSU, it is */
  /* used as a message to be detected. */
  String checkMsg = msgContent1i ;
end if
```

2) Check().
The traffic message detection function.

```
public static boolean check(String msg)
/* If it is a message sent by the RSU, the */
/* node trains it. */
print("start training.....");
String[] trainArgs={"msg2File"};
String[] modelFile=svmTrain.tain(trainArgs);

/* if it is not a message sent by the RSU, */
/* it is detected. */
print("start checkting.....");
String[] checkArgs={"msg1File"};
/* The node identifies and classifies the */
/* message according to Equation (3) */
/* and Equation (4).*/
Boolean result= modelFile.classify(checkArgs);
return result;
```

3) Update().
The reputation value update function.

```
public double update(String msg, boolean
msgType)
String nodeId=getNodeId(Msg1)
if (msgType == 0) then
  int[] Vtable= nodeIdVtable.vInsert(0);
else
  int[] Vtable= nodeIdVtable.vInsert(1)
  /* CA calculates the reputation value */
  /* of the node according to Equation (7).*/

  double RV(i)=sum(Vtable[i].g(k));
  return 1-RV(i)
end if
```

4) IsForgeryNode().
Forgery node decision function.

```
public boolean isForgeryNode (String rv)
if (rv > M) then
  return true;
else
  return false;
end if
```

6 Simulation and Analysis

Under the same conditions, the support vector machine, the decision tree model, class association rules and the naive bayes classifier are applied in the FNDA-IoV, and the performances of the detection efficiency and accurate detection rate of the four classification algorithms applied to the FNDA-IoV algorithm are compared.

6.1 Simulation Environment Configuration

A professional open source microscopic traffic simulation platform is the SUMO [3], two-way and six-lane highway environment is set, and experimental data is generated on the 6km road near the real vehicle driving position, speed, *etc.* Then a certain trace file is formed, and finally loads the network simulator NS2, the vehicle nodes is generated by reading the position, speed and other data of different vehicles at different times in the trace file [18]. Finally, the detection algorithm is simulated. The parameters are shown in Table 2.

6.2 Results and Analysis

Firstly, the simulation time is set to 50s, 100s, 150s, 200s, 250s, 300s to simulate the communication situation of each time period, and the node reputation value is calculated. Figure 6 shows the selected two nodes, namely the change in the reputation value of a legal node and a forgery node.

Figure 6 shows that with the passage of time, the reputation value of the legal node is rising. At 300s, the reputation value reaches 0.96, which is much higher than

Table 2: Simulation main parameters

type	name	value
Network scenes	Communication radius /m	300m
	MAC layer protocol	802.11p
	Simulation time	1000s
	Simulation area	1000m × 1000m
Traffic scenes	Number of lanes	6
	Number of nodes	200
	Number of forgery nodes	20
	Vehicle speed	20−60km/m
	Number of traffic messages	10 messages / vehicle
	Traffic message detection algorithm	SVM, NBC, DTM, CARS
	Reputation threshold	0.5

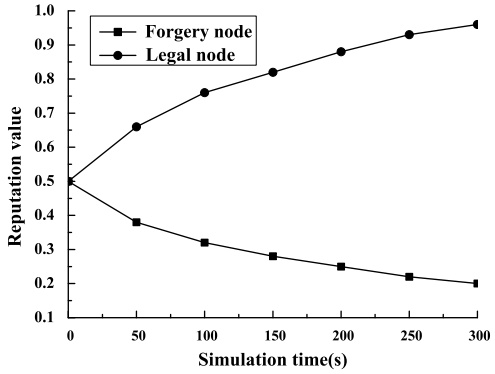

Figure 6: Node reputation value comparison

the threshold. The forgery node reputation value shows a downward trend. At 300s, the reputation value drops to about 0.2, which is far below the threshold. It can be seen that the FNDA-IoV algorithm can detect a forgery node whose reputation value is lower than the threshold.

Then, the detection overhead and the accuracy detection rate are analyzed.

1) The detection overhead. The detection overhead mainly measures the detection time required for detecting the forgery node, and the detection overhead is compared as shown in Figure 7. It can be seen that as the number of traffic messages published or forwarded by each vehicle is increasing, the detection time of the forgery nodes is gradually increasing.

   It is because the detection of the traffic messages published or forwarded by the vehicle takes time. The more traffic messages are detected, the longer the detection time required. However, The SVM has good recognition and generalization ability for non-linear and high dimensional data, and is suitable for traffic messages recognition and classification in the IoV. Therefore, the FNDA-IoV algorithm uses the SVM to detect traffic messages. Although the detection overhead of the algorithm is gradually increasing, it is slightly lower than a forgery node detection algorithm using the DTM, the CARS and the NBC.

2) The accuracy detection rate. The accurate detection rate refers to the probability that the detection algorithm can accurately detect the forgery node. The higher it is, the better the performance of the detection algorithm. The comparison results are shown in Figure 8.

As the number of the traffic messages published or forwarded by each vehicle is increasing, the accurate detection rate gradually is increasing. It is because the more messages published or forwarded by the node, the more accurate the judgment of the behavior of the node. At the same time, it can be seen that the FNDA-IoV algorithm designed by the SVM has a higher overall level than the NBC, the CARS and the DTM.

In summary, internal forgery nodes can be detected quickly and accurately by the FNDA-IoV algorithm in the Internet of Vehicles, and the security of the Internet of Vehicles is improved.

7 Conclusions

As a new type of wireless self-organizing network, Internet of Vehicles is well applied in the field of intelligent transportation. For the internal forgery node attack of the Internet of Vehicles, the detection efficiency and accuracy are improved by FNDA-IoV algorithm. However, the attack behavior of only a aspect of publishing or forwarding abnormal traffic messages is considered by the algorithm. The algorithm is considerd other aspects of the attack behavior, such as collusion between nodes, improved and optimized which will be the key tasks of the research work.

Acknowledgments

This research is supported by the National Natural Science Foundations of China under Grants No. 61862040,

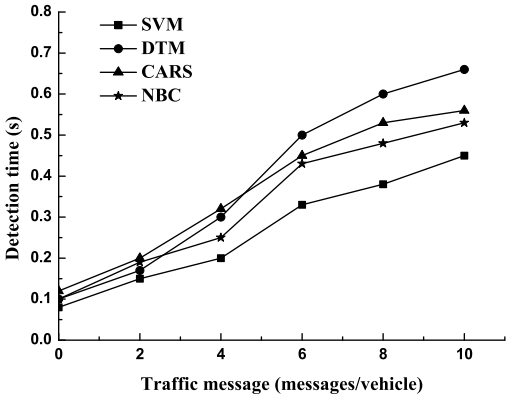

Figure 7: Detection overhead

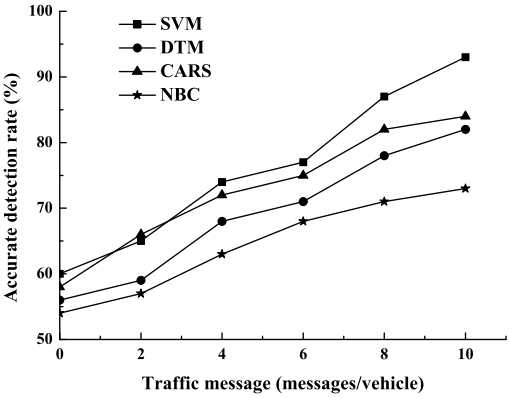

Figure 8: Accurate detection rate

No. 61762060 and No. 61762059. The authors gratefully acknowledge the anonymous reviewers for their helpful comments and suggestions.

References

[1] Z. Chen, L. Tian and C. Lin, "Trust evaluation model of cloud user based on behavior data," *International Journal of Distributed Sensor Networks*, vol. 14, no. 5, pp. 155–165, 2018.

[2] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 90, pp. 101740, 2019.

[3] M. A. Hassan, U. Habiba and U. Ghani, "Asecure message passing framework for inter vehicular communication using blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 2, pp. 155–177, 2019.

[4] S. Ibrahim, M. Hamdy and E. Shaaban, "Towards an optimum authentication service allocation and availability in VANETs," *International Journal of Network Security*, vol. 19, no. 6, pp. 955–965, 2017.

[5] C. Khurana and P. Yadav, "Prevention of malicious nodes using genetic algorithm in vehicular ad hoc network," in *The Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC'18)*, pp. 700–705, 2018.

[6] L. Li and X. D. Li, "Detection mechanism of VANET abnormal nodes based on greenshield model," *Computer Engineering (in Chinese)*, vol. 44, no. 2, pp. 114–118, 2018.

[7] F. Li, Y. L. Si and Z. Chen, " Decision making method for opportunistic network security routing based on trust mechanism," *Journal of Software (in Chinese)*, vol. 29, no. 9, pp. 2829–2843, 2018.

[8] X. W. Liu and Y. L. Shi, "Detection of false traffic information in internet of vehicles based on weak classifier integration," *Journal of Communications (in Chinese)*, vol. 37, no. 8, pp. 58–66, 2016.

[9] Y. B. Liu , X. L. Song and Y. G. Xiao, "Car network authentication mechanism and trust model," *Journal of Beijing University of Posts and Telecommunications(in Chinese)*, vol. 40, no. 3, pp. 1–18, 2017.

[10] P. Ounsrimuang and S. Nootyaskool, "Classifying vehicle traffic messages from twitter to organize traffic services," in *The IEEE 6th International Conference on Industrial Engineering and Applications (ICIEA'19)*, pp. 705–708, 2019.

[11] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud," *Vehicular Communications*, vol. 12, pp. 138–164, 2018.

[12] Y. L. Shi and L. M. Wang, "A method for detecting anti-collusion sybil attack based on space-time analysis in VANETs," *Chinese Journal of Computers (in Chinese)*, vol. 41, no. 9, pp. 2148–2161, 2018.

[13] M. Sohail, L. Wang and S. Jiang, "Multihop interpersonal trust assessment in vehicular ad-hoc networks using three valued subjective logic," *IET Information Security*, vol. 13, no. 3, pp. 223–230, 2018.

[14] B. Subba, S. Biswas and S. Karmakar, "A game theory based multi layered intrusion detection framework for VANET," *Future Generation Computer Systems*, vol. 82, pp. 12–28, 2018.

[15] H. Tan, Z. Gui and I. Chung, "A secure and efficient certificateless authentication scheme with unsupervised anomaly detectionin VANETs," *IEEE Access*, vol. 6, pp. 74260–74276, 2018.

[16] S. Vhaduri and C. Poellabauer, "Multi-modal biometric-based implicit authentication of wearable device users," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 955–965, 2019.

[17] Z. Wei and S. Yu, "Energy aware and trust based cluster head selection for ad-hoc sensor networks," *International Journal of Network Security*, vol. 20, no. 3, pp. 496–501, 2018.

[18] P. S. Xie, T. X. Fu and H. J. Fan, " An algorithm of the privacy security protection based on location service in the internet of vehicles," *International Journal of Network Security*, vol. 21, no. 4, pp. 556–565, 2019.

[19] Y. Xin and X. Feng, "A location dependent light weight sybil attack detection method in VANET,"

Journal on Communications (in Chinese), vol. 38, no. 4, pp. 110–119, 2017.

[20] W. Yang, M. R. Chen and G. Q. Zeng, "Cryptanalysis of two strongly unforgeable identity based signatures in the standard model," *International Journal of Network Security*, vol. 20, no. 6, pp. 1194–1199, 2018.

[21] W. Yu, Y. Li and Y. Xu, "Research on pseudo node detection algorithm in wireless sensor networks," *International Journal of Online Engineering*, vol. 13, no. 3, pp. 113–124, 2017.

[22] Q. Y. Zhang, W. J. Hu and S. B. Qiao, "Speech perceptual hashing authentication algorithm based on spectral subtraction and engery to entropy ratio," *International Journal of Network Security*, vol. 19, no. 5, pp. 752–760, 2017.

Biography

Peng-shou Xie was born in Jan. 1972. He is a professor and a supervisor of master student at Lanzhou University of Technology. His major research field is Security on Internet of Things. E-mail: xiepsh_lut@163.com.

Guo-qiang Ma was born in Jun. 1992. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: magq1514@163.com.

Tao Feng was born in Dec. 1970. He is a professor and a supervisor of Doctoral student at Lanzhou University of Technology. His major research field is modern cryptography theory, network and information security technology. E-mail: fengt@lut.cn.

Yan Yan was born in Oct. 1980. She is a associate professor and a supervisor of master student at Lanzhou University of Technology. Her major research field is privacy protection, multimedia information security. E-mail: yanyan@lut.cn.

Xue-ming Han was born in Jan. 1990. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: hxmhan@163.com.