Trust prediction based on grey exponential smoothing method in VANETs

Sanshun Zhang[1,2], Li Li[1,2], Hui Xia[*1,2], Rui Zhang[1,2], Ye Li[2]
{zhangss0815@163.com, lili_08173724@163.com, xiahui@qdu.edu.cn}

College of Computer Science and Technology, Qingdao University, Qingdao, Shandong, 266000[1], Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan, Shandong 250014[2]

Abstract. In vehicular ad hoc networks (i.e., VANETs), normal communications between vehicles are vulnerable to attacks from malicious vehicles. Trust-based solution is a feasible method to solve the routing security problem. In this paper, a trust prediction model based on grey exponential smoothing method is proposed by combining the grey model, the exponential smoothing prediction method and the golden section search method. A multicast routing protocol based on the grey exponential smoothing trust prediction model, named ESGM-ODMRP, is presented to verify the validity of this new method. In the experiments, the evaluation of four routing metrics (i.e., packet delivery ratio, overhead, average latency and byte sent per byte delievered) prove that our protocol performs better in identifying malicious vehicles and establishing secure routes.

Keywords: vehicular ad hoc network; trust prediction; grey model; routing protocol

1 Introduction

With the increasing number of vehicles and frequent occurrence of traffic accidents, human beings are increasingly demanding to improve the efficiency and safety of transportation systems. Currently, vehicular communications between vehicles are the predominant mode of transferring information [1]. One of the most promising applications of vehicular communications is the vehicular ad hoc networks (VANETs). The up-to-date traffic information about traffic jams, traffic accidents and road constructions can be obtained by drivers in VANETs. By getting these information in time, drivers can choose the optimal route to their destinations. As a prerequisite for the effective operations in VANETs, the routing protocol designed must be secure and efficient to ensure timely and reliable data transmission between vehicles [2,3].

However, different from traditional wireless network, VANETs are harder to design an appropriate routing protocol due to their distinctive characteristics, such as self-organization, high node mobility, dynamic network topology, and error-prone transmission media. Furthermore, with the increasing of relying on communication and control technologies, VANETs are more vulnerable to security attacks from malicious vehicles [4]. Meanwhile, they also pose the unique privacy and security questions comprised of data integrity, availability, access control, and confidentiality. Therefore, routing security has become the main problem in VANET research.

MOBIMEDIA 2019, June 29-30, Weihai, People's Republic of China

DOI 10.4108/eai.29-6-2019.2282065

In order to effectively identify malicious vehicles and ensure reliable transmission of data between vehicles, the recently popular solutions are to apply trust mechanism to a few common routing protocols [5]. However, the trust prediction schemes used in the common trust models, such as analytic hierarchy process and Bayesian prediction, cannot accurately predict a vehicle‘s trust value based on this vehicle‘s historical trust values, especially when the sample set is small. Therefore, in order to address the abovementioned issues, we propose a trust prediction model based on the grey exponential smoothing method in this paper. This model avoids the influence of data fluctuation on the prediction result by processing the original prediction sequence. Moreover, the accuracy of prediction is further enhanced by considering the influencing factors associated with trust values.

2 Related work

To ensure the routing security, many trust models have been applied to routing protocols [6, 7, 8]. In the process of model design, trust prediction is considered to be the focus of current research. Xia et al. [9] improved the traditional Markov prediction algorithm and proposed a new dynamic grey Markov chain prediction model. The model can predict the future trust value of the node based on the historical behavior of the node. Cai et al. [10] proposed a trust prediction framework which takes both the trust network itself and the user interaction environment into account. Experiments show that trust relationships can be predicted more effectively by combining user interactions. A trust model based on historical trust assessment and trust prediction was proposed in [11]. In the model, multiple trust attributes are presented and assigned different weights by the fuzzy AHP method based on entropy weights, and the improved Markov model is used to predict the trust value of aspecific node. In [12], Bhargava et al. presented an automatic trust prediction mechanism by using Kalman filter to fuse existing trust with the verified behavior of nodes. In order to effectively calculate the trust value of the safety path between vehicles in VANETs, Malhi et al. [13] proposed a trust prediction model based on fuzzy logic. In [14], a novel multicast routing protocol based on the reactive trust model (TAPtrust) was presented by Xia et al. The trust value is updated by the fuzzy logic rules prediction mechanism. Sengathir et al. [15] presented a semi-Markov prediction model based on trust coefficient, called FTCSPM, to quantify the impact of selfish behavior on network survivability.

3 Trust prediction model based on grey exponential smoothing method

It is well known that the traditional grey model is not ideal for predicting sequences with fluctuations. Due to this, we propose a novel grey prediction model by using exponential smoothing method, which can optimize the calculation of background values. This new model is mainly composed of the following steps:

(1) Get the original sequence of trust values and the corresponding influencing factor sequences;

(2) Process the sequences by exponential smoothing method to reduce their random fluctuations;

(3) Improve the gray prediction model by optimizing the background value to predict the smooth sequence;

(4) The final prediction result is obtained by the inverse exponential smoothing method;
(5) Determine whether the prediction result meet the fitting error or not. If it does, the prediction result is obtained; if not, the step (2) is re-executed and the improve golden section search method is used to reselect the subinterval of smoothing coefficient and determine the optimal smoothing coefficient.

3.1 Acquisition of the original sequence

In order to effectively predict the trust value of a node, we first divide the interaction history of vehicles into *m* evaluation periods. According to the actual transaction record of node interactions, we can get the node trust values for each evaluation period, which is represented by the sequence $A_1^0 = (A_1^0(1), A_1^0(2), ..., A_1^0(m))$.

$$A_1^0(t) = N^s(t) / N^r(t) \tag{1}$$

where $N^s(t)$ is the total number of packets received by the node during the *t*-th period, and $N^r(t)$ is the total number of packets forwarded by the node during this period.

In the calculation of trust value, the number of transactions and the frequency of transactions affect the accuracy of calculation. Therefore, these two influence factors must be considered when predicting the trust value of a specific node. The corresponding sequences are represented by A_i^0 :

$$A_i^0 = (A_i^0(1), A_i^0(2), ..., A_i^0(m)), (i = 2, 3, ..., n) \tag{2}$$

where *n* indicates the total number of influence factors.

3.2 Processing the sequence using the exponential smoothing method

The exponential smoothing method is a deterministic smooth prediction method developed on the basis of the moving average method. The essence of this method is to smooth the time series by calculating the exponential smoothing average and eliminating the random fluctuations in the historical statistical sequence. In order to make the sequence meet the requirement of grey prediction model, the first exponential smoothing method is used to smooth the original sequence. The process is as follows:

$$S_i^0(k) = \lambda^* A_i^0(k) + (1 - \lambda^*) S_i^0(k-1) \tag{3}$$

where $i = 1, 2, ..., n$, $k = 2, 3, ..., m$. S_i^0 is the smooth sequence after processing. λ^* is the optimal smooth coefficient which can be obtained by the improved golden section method.

The accumulative sequence A_i^1 can be computed by the smooth sequence S_i^0 , as follows:

$$A_i^1(k) = S_i^0(k) + S_i^0(k+1) \tag{4}$$

3.3 Optimization parameters of the grey model

In the traditional grey prediction model, the weight of the background value is fixed, set to 0.5. However, this default value may cause a large prediction error. Therefore, we redefine this weight by using the optimal smoothing coefficient and optimize the calculation of the background value in the grey prediction. The calculation formulas are as follows:

$$\alpha = \frac{1}{\lambda^*} - \frac{1}{e^{\lambda^*} - 1} \tag{5}$$

$$Z_i^1(k) = \alpha A_i^1(k-1) + (1 - \alpha) A_i^1(k) \tag{6}$$

where Z_i^1 is the background value, and α is its weight.

The matrix C can be obtained from the sequence of optimized background values, and the matrix D can be calculated according to the smooth sequence. Finally, we can get the grey parameters X and Y using equation (9):

$$C = \begin{bmatrix} Z_1^1(2) & Z_2^1(2) & \cdots & Z_n^1(2) & 1 \\ Z_1^1(3) & Z_2^1(3) & \cdots & Z_n^1(3) & 1 \\ \vdots & \vdots & \vdots & \vdots & \\ Z_1^1(m) & Z_2^1(m) & \cdots & Z_n^1(m) & 1 \end{bmatrix} \tag{7}$$

$$D = \begin{bmatrix} S_1^0(2) & S_2^0(2) & \cdots & S_n^0(2) \\ S_1^0(3) & S_2^0(3) & \cdots & S_n^0(3) \\ \vdots & \vdots & \vdots & \vdots \\ S_1^0(m) & S_2^0(m) & \cdots & S_n^0(m) \end{bmatrix} \tag{8}$$

$$\begin{bmatrix} X^T \\ Y^T \end{bmatrix} = H = (C^T C)^{-1} C^T D \tag{9}$$

where H is an $(n+1) \times n$ order matrix. X^T represents the first n rows of the matrix H, and Y^T is the last row of the matrix H. The grey parameters X and Y can be got by transposing the two matrices, respectively.

3.4 Acquisition of final prediction sequence

According to the grey model, the predictive sequence $\hat{A}_1^1$ of the sequence A_1^1 is computed by the grey parameters X and Y, as follows:

$$\hat{A}_1^1(k) = e^{X(k-1)}(A_1^1(1) + X^{-1}Y) - X^{-1}Y \tag{10}$$

The predictive sequence $\hat{S}_1^0$ can be obtained by the first order inversely accumulative generation operation:

$$\hat{S}_1^0(k) = \hat{A}_1^1(k) - \hat{A}_1^1(k-1) \tag{11}$$

Finally, the predictive sequence of original sequence A_1^0 is obtained using the inverse exponential smoothing method:

$$\hat{A}_1^0(k) = \frac{(\hat{S}_1^0(k) - (1-\lambda^*)\hat{S}_1^0(k-1))}{\lambda^*} \tag{12}$$

3.5 Computation of optimal smoothing coefficient

According to the above prediction process, the value of the smoothing coefficient directly affects the accuracy of the exponential smooth grey prediction model. How to determine the best smoothing factor which is used to minimize the prediction error is the most critical issue at present. The traditional method of determining the optimal smoothing factor requires multiple iterations, calculations, and even human interventions, which is very inefficient. Therefore, we propose an improved golden section search method to update the value of smoothing coefficient.

The traditional golden section method uses the mean square error as the objective function to determine the optimal smoothing coefficient. However, we can see that using MAPE (i.e., the mean absolute percent error) can more accurately reflect the deviation between the

predicted value and the actual value. Using the function *f* to represent the value of MAPE, as follows:

$$f = \frac{1}{m}\sum_{k=1}^{m}\left|\frac{A_1^0(k)-\hat{A}_1^0(k)}{A_1^0(k)}\right|\times 100\% \tag{13}$$

The process of calculating the optimal smoothing parameters using the improved golden section search is as follows:

(1) Divide $\lambda \in (0,1)$ average into 10 subintervals and use $\lambda_1, \lambda_2, ..., \lambda_{10}$ to represent respectively. A subinterval $\lambda_i \in (a,b)$ is selected to search for the optimal smoothing coefficient, where *a* and *b* represent the left and right ends of the *i*-th subinterval, respectively;

(2) The two trial points can be obtained utilizing the golden section search method, as follow:

$$\lambda_i = 0.618a + 0.382b \tag{14}$$

$$\lambda_i' = 0.382a + 0.618b \tag{15}$$

(3) If two test points satisfy the formula $|\lambda_i - \lambda_i'| < \delta$, let $\delta = 0.01$, the optimal smoothing coefficient is calculated by the equation $\lambda^* = (\lambda_i - \lambda_i')/2$. Otherwise, go to the next step.

(4) Calculate the value of MAPE $f(\lambda_i)$ and $f(\lambda_i')$ when $\lambda^* = \lambda_i$ and $\lambda^* = \lambda_i'$, respectively. If $f(\lambda_i) > f(\lambda_i')$, let $a = \lambda_i$, $\lambda_i = \lambda_i'$, *b* keeps constant and recalculate λ_i'; If $f(\lambda_i) < f(\lambda_i')$, let $b = \lambda_i'$, $\lambda_i' = \lambda_i$, *a* keeps constant and recalculate λ_i.

4 Model comparison

Based on the NS2 platform, the trust values, the number of transactions and the frequency of transactions of the vehicles in 10 periods are counted separately. The data of the first 8 periods is used as the original sequence of prediction, as shown in Table 1. The new model, the traditional grey model [17] and the improved Markov grey model [13] are compared together to predict the original sequence. Their predictionsand errors are shown in Table 2. The error is calculated by the difference between the predicted value and the true value. For example, the error of the new model in 9-th period is calculated by (|0.8684-0.8591|)/0.8591*100%=1.08%. As shown in Table 2, the mean error of the new model is 1.305%, which is much smaller than the GM(1,3). And the mean error of Markov-GM(1,3) is 3.84%, which is about 3 times larger than that of the new model. It can be more clearly seen that the prediction accuracy of the new model is significantly better than the other two models.

Table 1. The original data

period	*Trust value*	*Number of transactions*	*Frequency of transactions*
1	0.8336	563	6
2	0.7584	894	3
3	0.5796	265	2
4	0.9054	862	4
5	0.8778	964	3
6	0.6462	403	2
7	0.8245	1034	9

8	0.8963	326	3

Table 2. Predictions and errors of each model

period	*Trust value*	*The new model*		*GM(1,3)*		*Markov-GM(1,3)*	
		Predictions	*Error(%)*	*Predictions*	*Error(%)*	*Predictions*	*Error(%)*
1	0.8336	0.8336	0	0.8336	0	0.8336	0
2	0.7584	0.7728	1.44	0.8042	6.04	0.7903	4.206
3	0.5796	0.5643	2.63	0.6518	12.45	0.6010	3.69
4	0.9054	0.9101	0.52	0.8668	4.26	0.8632	4.66
5	0.8778	0.8918	1.59	0.9095	3.61	0.8531	2.81
6	0.6462	0.6631	2.61	0.6954	7.61	0.6856	6.09
7	0.8245	0.8184	0.73	0.7618	7.60	0.7863	4.63
8	0.8963	0.8873	1.00	0.8645	3.54	0.8786	1.97
Mean Error		1.36		5.93		3.72	
9	0.8591	0.8684	1.08	0.8026	6.57	0.8354	2.75
10	0.7079	0.7188	1.53	0.7598	7.33	0.7428	4.93
Mean Error		1.305		6.95		3.84	

5 Experiment

In order to ensure reliable data transmission between vehicles, we present a novel multicast routing protocol ESGM-ODMRP by applying the trust prediction algorithm to the ODMRP in VANETs. According to the trust predictions , malicious vehicles in the network can be identified and isolated, and the system can establish trusted routing paths. Moreover, we also add the trust prediction model in [9], [13] to the ODMRP, named the FL-ODMRP and the Markov-ODMRP. Then wecompare the extended two versions with the original ODMRP and our proposed protocol ESGM-ODMRP. The performance of these protocols are evaluated by four routing metrics, i.e. *Packet Delivery Ratio*, *Average Latency*, *Overhead* and *Byte Sent per Byte Delivered*.

5.1 Experimental scenario

We estimate the performance of several trust-based protocols using the SUMO and NS-2.35 [16] simulator. In this simulator, the SUMO is used to establish the simulation scenarios. In order to simulate the real road traffic environment, we select partial map of Laoshan District, Qingdao as the road model by using OpenStreetMap (OSM), as show in Fig. 1.

To make the map to adapt the simulation of protocol in NS2, the JOSM is utilized to delete the buildings and modified slightly the roads of the map. Then, we convert the modified map data to road model file using the tool NETCONVERT in SUMO, as show in Fig. 2.

Fig. 1. The partial map of Qingdao in OSM

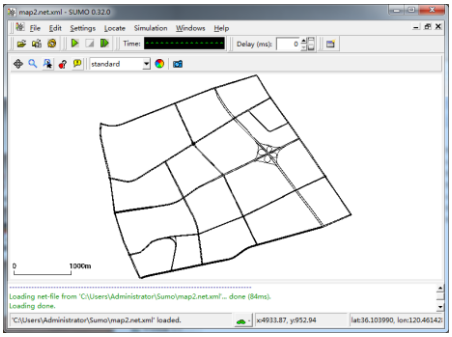


Fig. 2. The road mode in SUNO

After the road model is created, we still need to establish appropriate vehicle moving model by SUMO. The starting point and end point of the vehicle in the map are randomly set to ensure the authenticity of the simulation. The specific parameters of the simulation scenario are shown in Table 3. Finally, the output file of simulation scenario in SUMO is embedded in NS2 to realize the coupling of loose open-loop mode. In the NS2, we observe changes in performance metrics for each protocol by changing the number of malicious vehicles.

Table 3. The Parameters of Simulation Scenario

Parameter	*Value*
Scene range	1500m×1500m
The number of roads	12
The number of junctions	24
The number of vehicles	50
Vehicle length	5m
Maximum vehicle speed	10m/s

5.2 Performance evaluation

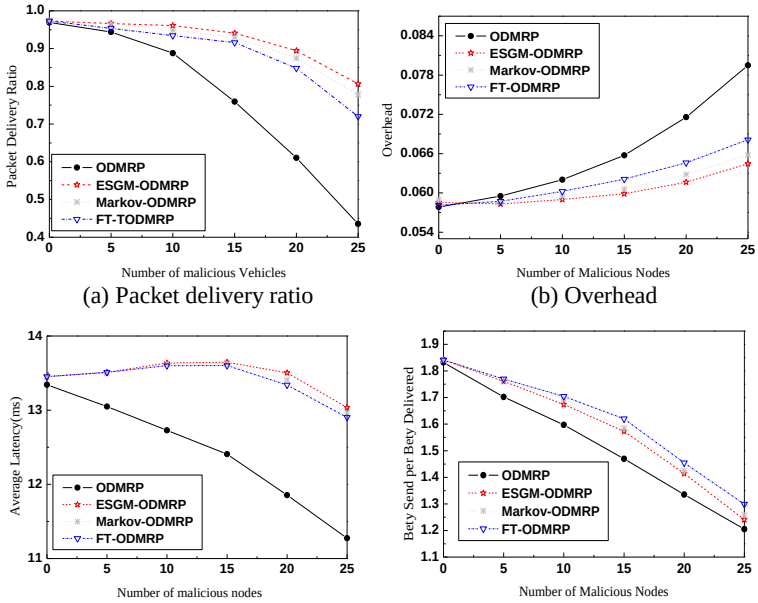
With the increase of malicious vehicles, the trend of the packet delivery ratio of each protocol is shown in Fig. 3(a). The packet delivery ratio of the ODMRP protocol decreases rapidly with the increase of malicious vehicles. This is because the original ODMRP protocol without the trust model does not make any processing to the malicious vehicles in the network, and the data packets are discarded in large quantities. Due to ESGM-ODMRP, Markov-ODMRP and FT-ODMRP protocols can identify malicious vehicles through trust prediction, their package delivery rate remains at a high level. However, The ESGM-ODMRP protocol has the highest package delivery ratio because the accuracy of our newly proposed trust prediction model is better than the fuzzy logic-based trust model in FT-ODMRP and the improved Markov-based trust model in Markov-ODMRP.

As shown in Fig. 3(b), The overhead of all protocols increases with increasing the number of malicious vehicles. Moreover, the more malicious vehicles, the greater the growth rate. The reason is that excessive malicious vehicles interfere with the collection of trust information, so that the collected historical trust values have large fluctuations, which affects the accuracy of trust prediction. More and more malicious vehicles cannot be accurately identified, and the overhead for routing maintenance will increase. Our trust prediction algorithm can effectively deal with data fluctuations by using the exponential smoothing method, so ESGM-ODMRP protocol has the lowest overhead.

As can be seen from Fig. 3(c), the average latency of ESGM-ODMRP is slightly higher than Markov-ODMRP and FT-ODMRP, but all their average latency is much higher than one of ODMRP. The establishment of trusted routing is at the cost of increasing hops. When a

malicious vehicle is identified, we need to bypass the malicious vehicle to establish a secure route by adding hops, which will result in a longer latency. Owing to ESGM-ODMRP can identify more malicious vehicles than other protocols, its average latency is the longest. In addition, when the proportion of malicious vehicles is greater than 30%, the ability of each protocol to identify malicious vehicles is significantly reduced. Therefore, the overall trend of the average latency is to increase first and then drop.

Fig. 3(d) shows the byte sent per byte delivered for all protocols decreases when malicious vehicles increases. The byte sent per byte represents the ratio of the total number of bytes of packets transmitted by the node to the number of bytes of the delivered data packets. For ESGM-ODMRP, Markov-ODMRP and FT-ODMRP protocols, the total number of bytes of the packet transmitted by the node is basically the same. The value of byte sent per byte delivered mainly depends on the number of bytes of the delivered data packet. As can be seen from Figure 3(a), ESGM-ODMRP has the highest packet delivery ratio, so its byte sent per byte delivered is lower than Markov-ODMRP and FT-ODMRP.



(a) Packet delivery ratio (b) Overhead

(c) Average latency (d) Byte sent per byte delivered

Fig. 3 The impact of varying number of malicious vehicles on protocol performance

6 Conclusions

Routing security has become a serious problem that can not be ignored in the extensive applications of vehicular ad hoc networks. Trust prediction plays an important role in the establishment of secure routing. In this paper, a trust prediction model based on grey exponential smoothing method is proposed by combining grey model, exponential smoothing prediction method and golden section search method. Moreover, we combine the trust prediction model with the ODMRP protocol and perform simulation analysis. The simulation results show that our protocol performs better and identifys malicious vehicles more effectively. Moreover, the convincing experimental results prove that our trust prediction

algorithm has higher prediction accuracy than the other relevant algorithms.

Acknowledgments. This research is supported by the National Natural Science Foundation of China (NSFC) under Grant Nos.61872205, the Project of Shandong Province Higher Educational Science and Technology Program under Grant No.J16LN06, the Source Innovation Program of Qingdao under Grant No.18-2-2-56-jch, the Open Research Fund from Shandong Provincial Key Laboratory of Computer Networks under Grant No. SDKLCN-2018-07 and the State Foundation of China for Studying Abroad to Visit the United States as a 'Visiting Scholar'

References

[1] Cooper C, Franklin D, Ros M, et al.: A Comparative Survey of VANET Clustering Techniques. IEEE Communications Surveys & Tutorials. Vol.19, No.1, pp.657-681 (2017)
[2] Sharef B T, Alsaqour R A, Ismail M.: Vehicular communication ad hoc routing protocols: A survey. Journal of Network and Computer Applications. Vol. 40, pp.363-396 (2014)
[3] Cheng J, Cheng J, Zhou M, et al.: Routing in Internet of Vehicles: A Review. IEEE Transactions on Intelligent Transportation Systems. Vol. 16, No. 4, pp. 1-14 (2015)
[4] Abdelgadir M, Saeed R A, Babiker A.: Mobility Routing Model for Vehicular Ad-hoc Networks (VANETs), Smart City Scenarios. Vehicular Communications. Vol. 9, pp. 154-161 (2017)
[5] Kerrache C A, Calafate C T, Cano J C, et al.: Trust Management for Vehicular Networks : An Adversary-Oriented Overview. IEEE Access. Vol. 4, pp. 9293-9307 (2016)
[6] Li W; Song H.: ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems. Vol. 17, No. 4, pp. 960-969 (2016)
[7] Marmol FG, Martinez P G.: TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of Network and Computer Applications. Vol. 35, No. 3, pp. 934-941 (2012)
[8] Sharma K, Chaurasia B K.: Trust Based Location Finding Mechanism in VANET using DST. 2015 Fifth International Conference on Communication Systems and Network Technologies. pp. 763-766 (2015)
[9] Xia H, Wang G D, Pan Z K.: Node Trust Prediction Framework in Mobile Ad Hoc Networks. 2016 IEEE TRUSTCOM/BIGDATASE/ISPA. pp. 50-56 (2017)
[10] Cai G, Wang L, He H.: Trust Prediction Based on Interactive Relations Strength. Applications and Techniques in Information Security. Vol. 577, pp. 189-200 (2015).
[11] Xia H, Yu J, Pan Z K, et al.: Applying trust enhancements to reactive routing protocols in mobile ad hoc networks. Wireless Networks. Vol. 22, no. 7, pp. 2239-2257(2016)
[12] Bhargava A, Verma S, Chaurasia B K.: Kalman filter for trust estimation in VANETs. IEEE Uttar Pradesh Section Conference on Electrical Computer and Electronics. Allahabad, INDIA (2016)
[13] Malhi A K, Batra S.: Fuzzy-based trust prediction for effective coordination in vehicular ad hoc networks. International Journal of Communication Systems. Vol. 30, No. 6. (2017)
[14] Xia H, Sha H M, Jia Z.: Research of trust model based on fuzzy theory in mobile ad hoc networks. IET Information Security. Vol. 8, No. 2, pp. 88-103 (2014)
[15] Sengathir J, Manoharan R.: A futuristic trust coefficient-based semi-Markov prediction

model for mitigating selfish nodes in MANETs. Eurasip Journal on Wireless Communications & Networking. Vol. 2015, No. 1, pp.158 (2015)
[16] Behrisch M, Bieker L, Erdmann J, Krajzewicz D.: SUMO Simulation of Urban MObility. The Third International Conference on Advances in System Simulation. pp. 63-68 (2011)
[17] Deng J L.: Control problems of grey systems. Systems & Control Letters. Vol. 1, No. 5, pp. 288–294 (1982)