TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 19, No. 5, October 2021, pp. 1688~1696
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v19i5.19358

Malicious vehicle detection based on beta reputation and trust management for secure communication in smart automotive cars network

Dilshad Ara Hossain[1], S. M. Salim Reza[2]
[1]Faculty of Information and Communication Technolog, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2]Faculty of Engineering and Built Environment, The National University of Malaysia, Selangor, Malaysia
[2]Dept. of Information and Communication Technology, Bangladesh University of Professionals, Dhaka, Bangladesh

Article Info

Article history:

Received Jan 4, 2021
Revised Apr 10, 2021
Accepted Apr 22, 2021

Keywords:

Artificial intelligence
Communication security
Cyber security
IoT
Network
Security
Smart car
Trust management reputation

ABSTRACT

High reliance on wireless network connectivity makes the vehicular ad hoc network (VANET) vulnerable to several kinds of cyber security threats. Malicious vehicles accessing the network can lead to hazardous situation by disseminating misleading information or data in the network or by performing cyber-attacks. It is a requirement that the information must be originated from the authentic and authorized vehicle and confidentiality must be maintained. In these circumstances, to protect the network from malicious vehicles, reputation system based on beta probability distribution with trust management model has been proposed to differentiate trustworthy vehicles from malicious vehicles. The trust model is based on adaptive neuro fuzzy inference system (ANFIS) which takes trust metrics as input to evaluate the trustworthiness of the vehicles. The simulation platform for the model is in MATLAB. Simulation results show that the vehicles need at least 80% trustworthiness to be considered as a trusted vehicle in the network.

Corresponding Author:

S. M. Salim Reza
Faculty of Engineering and Built Environment
The National University of Malaysia
43600 Bangi, Selangor, Malaysia
Email: salim4419@gmail.com

1. INTRODUCTION

To increase the safety of road users and to enhance the efficiency of the transportation system, the vehicles are equipped with wireless networking. When vehicles connect by forming this wireless network, then it is referred to as vehicular ad-hoc network (VANET). The automotive car onboard network is a subclass of VANET where one subclass of mobile ad hoc network (MANET) is VANET [1]. Dedicated short range communication (DSRC) occurs among the entities of the network through IEEE 802.11p [2]. The number of vehicles is increasing day by day and the probable number is forecasted to be 2 billion within 10 or 20 years. VANET plays an important role to create a future intelligent transportation system. So VANET is an important topic in the intelligent transportation system [3]. In VANET, communication occurs between 2 nodes or entities, which are the on-board unit (OBU) and the road side unit (RSU) [4]. Therefore, we can classify the communication topology as OBU to OBU and OBU to RSU. OBU to OBU communication topology is known as vehicle-to-vehicle (V2V) communication and OBU to RSU communication topology is known as vehicle-to-infrastructure (V2I) communication. In VANET, the nodes (vehicles and RSUs) share

various types of messages for different example applications to avoid road accidents, or to avoid traffic congestion in a multi-hop fashion [5]. Other applications of VANETs are but not limited to building traffic information system, safety, and entertainment services, platooning service, collision avoidance, vehicle post crashing warning, road collision warning, lane changing assistance, car parking service, electronic toll collection [6]. These applications of VANET are facilitating peoples' daily lives through modernizing the transportation system by integrating artificial intelligence into it.

VANET is a special type of wireless network where a node can pass by other nodes with high-speed providing very less time and scope to evaluate the reliability or trustworthiness of other vehicles. The above issue refers to the fact that the network is highly dynamic and comprises of time-varying topology. However, this characteristic makes the network vulnerable to several types of cybersecurity threats such as message forging, wormhole attack, and black hole attack [2]. Utilizing wireless communication, limited power, error-prone transmission media makes the network vulnerable to different cybersecurity threats. Cyber-attacks that disrupt communication can lead to hazardous and life-threatening situations as the VANET technology is trying to merge with human life. Ensuring reliable and secure communication in VANET is challenging because of its demerits. Only the vehicles that are authentic, authorized, and trusted, can ensure reliability and security in the network. Otherwise, malicious vehicles or adversaries will disrupt the communication and consequently hamper the network. In recent years, researchers have proposed several kinds of security measures to ensure secure communication in VANET. The proposed methods range from strong cryptographic mechanisms to trust management and reputation management system. Insider attack and outsider attack are the 2 types of attacks that can harm the network. In an insider attack, a legitimate vehicle behaves maliciously and in an outsider attack, an unauthorized vehicle tries to get access to the network and launches different types of attacks. Cryptography can only detect and prevent outsider attacks but cannot eliminate insider attacks. Insider attacks need to be addressed with equal importance; otherwise, compromised vehicles can create a dangerous situation through cyber-attacks [7]. Cryptography mechanisms require excessive time to compute secret keys which is a major drawback in VANET due to fast-moving vehicles. Furthermore, the sensors, processors, computational power of the on-board units are resource-constrained and manufacturers are now considering controllers with built-in cryptographic modules.

Trust management is one of the alternative promising solutions to these cryptography schemes. Trust management can eliminate both insider and outsider attacks. It detects malicious vehicles in the network by evaluating their trust value. There are three varieties of trust management, namely, the hybrid trust model, entity centric trust model, and data-centric trust model [8]. The trust value of the vehicles is evaluated by the trust management model in the entity-centric trust model. In this model, one vehicle evaluates another vehicle through direct or indirect interaction. Indirect interaction means collecting recommendations from other vehicles, which have already communicated with the suspected vehicle. Trust is measured by the vehicles in the data-centric trust model for the incoming received messages to detect whether the message is contaminated with false data. The entity-centric trust model and data-centric trust models are associated with a hybrid trust model so that data, as well as vehicles, can be evaluated. In recent literature, various categories of trust models have been proposed but trust models alone cannot provide enough strength to ensure secure communication. If only the trust model is used, then the trustor (who measures trust) needs to measure the trust of a trustee (whose trust value will be measured) every time it interacts. So, in this paper, a new trust management model is being proposed, combined with a reputation system. Integrating reputation system with trust management model will help vehicles to overcome the vehicles to eliminate above mentioned problem that could have occurred from using trust management alone. In the proposed model the trust management model is a hybrid trust model and it is based on subjective logic and the trust model will be evaluated through adaptive neuro fuzzy inference system (ANFIS). Subjective logic has been considered as it factors in uncertainty to model trust management and in this case, the VANET network comprises of uncertainty. ANFIS has been exploited to measure the trust value and detail discussion about ANFIS is in subsequent section. The reputation system is based on beta distribution. The parameters of beta distribution comprise of positive interaction and negative interaction which helps to differentiate vehicles good behavior from bad one. In general, the beta distribution-based reputation system will project the future behavior of vehicles from analyzing past behavior. Thus, in this process the trusted legitimates vehicles reputation will always remain above the threshold. A reputation system gathers, distributes and aggregates feedback about participants behavior and provides a measure of trustworthiness and it also provides an incentive for honest behavior [9]. The proposed trust management model in this paper has been integrated with reputation engine that will successfully eliminate malicious vehicles from the smart cars network and ensure trusted communication among the vehicles and RSU.

The main contribution of this paper can be summarized as; Firstly, the previous works of VANET on trust management and security models have been investigated and it has been found out that in most of the cases, only trust management models alone have been proposed to ensure security. Secondly, a beta

distribution-based reputation system has been proposed. The reputation function will provide rating and based on this rating reputed vehicles will be identified to perform network operation. Then only reputed vehicles data trust will be measured and will be considered as legitimate data. Thirdly, a hybrid trust management model has been proposed. Hybrid trust management model has been considered as it can ensure both node trust and data trust. The trust model has been modeled based on subjective logic and will be evaluated through ANFIS. In section two, detail review work has been presented. In section three, a reputation model and trust management models has been depicted. Section four covers the simulation portion of the work and section five concludes the paper.

2. RELATED WORKS

Koirala *et al.* [1], a trust management model has been proposed that is based on stay-time of nodes which can evaluate the trust behavior of other nodes. They have emphasized on newly joined vehicles trust behavior. The trust model is based on three factors-current trust level, reward point and punishment factor. The evaluator vehicle is selected based on its stay time. One of the limitations of this work is generating extra public key (PU) and private key (PR) pair is unnecessary for newly joined vehicle. The proposed trust model in [2] considers communication behavior where the communication behavior is observed for measuring the direct reputation of the nodes through certain factor method. The indirect reputation (collected from neighbor vehicles and RSU) then combined with direct reputation through uncertain deductive method. The authors proposed a trust model that comprises of both node trust and data trust. The trust model is based on certain factor model or certain theory. The proposed scheme has high detection accuracy in trust calculation. Lu *et al.* [3] proposed a distributed trust management based on block chain that can protect the privacy of vehicle. This trust management model (TMM) completes two process to reach the objective are certificate update process and authentication process. No solution has been shown for any vehicle becoming compromised.

A cryptography and feedback-based trust management has proposed in [4] where trust is measured by combing the opinion of neighbor nodes. The opinion combining operation is performed by RSU. However, in case of low amounts of neighbors the decision taken by RSU will be vulnerable as trust value of newly joined vehicles is measured by the neighbor vehicles recommendation only. The art model proposed in [5] can prevent malicious attack and evaluates data and node trust for the vehicles in the network. The proposed trust management model comprises of data trust and node trust. Node trust itself is a combination of functional trust and recommendation trust. Dempster shafer theory is proposed to combine multiple trust evidence to evaluate the behavior of the nodes properly. To evaluate the recommendation trust collaborating filter is utilized. Also, to find the similarities between two nodes recommendation, cosine-based similarity metric has been used. Wei and Chen [10] have proposed adaptive decision-making model which can prevent delay in decision making that can solve traffic accident due delayed decision. The proposed method is very simple. It just follows a threshold value. However, the decision-making vehicles may not get proper information from RSU within the allocated time which can lead to improper decision. Hash function based method has been proposed in [11] to prevent data falsification attack in VANET. The authors have proposed an authentication mechanism to prevent man in the middle attack who can inject false message or can modify the relayed message. The authentication mechanism is based on hash chain where a source vehicle sends a message with a hash of the message. However, Hash does not ensure that whether the message is from legitimate vehicle or compromised vehicle that is it cannot detect the truth or legitimacy of the message. It can only be ensured through trust management.

Kerrache *et al.* [12] have proposed a hierarchical hybrid trust model excluding both dishonest messages and nodes. The provided TMM can offer service for few different conditions are no delay, average delay and no delay limits. Suman and Kumar [13] have proposed a recorded different routing protocols in VANETs and compared their performance in presence of sybil attack. They have defined existing routing protocols and classified it in proactive (table-driven) and reactive (on-demand) mode. An attack resistant based vehicle to vehicle algorithm has been proposed in [14] which provides better performance than the existing schemes. They analyzed end to end delay (EED) and trust computation error (TCE) in trust in scheme ARV2V. A certificate revocation based VANET has been proposed in [15] focused on how network secrets are distributed confidentially among the legitimate members of the network, securing with certificate revocation process and using only a secret to prove the authenticity, replacing the time-consuming database searching mechanism. In this paper communication between two vehicles is simply proposed. The leakage of that model is a bunch of compromised nodes can run DoS attack. A scheme has been proposed in [16] to prevent any quantity sending fake requests and trying to break the security of the network.

3. SYSTEM MODEL

3.1. Reputation model

One of the continuous probability distributions is beta distribution which is utilized to predict the posteriori probability distribution based on some number of evidences observed in an experiment. The prior distribution is the uniform distribution of the parameters of the beta distribution such as $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. If a probabilistic model has binary outcomes say either success or failure with probability P(X) and 1-P(X) respectively then posteriori probability of the outcomes can be derived through beta distribution where P(X) is unknown meaning it is totally uncertain and follows uniform distribution. After performing some experiment, some evidence about success or failure of that probabilistic model can be identified which could be used to find the posteriori distribution as parameters of the beta distribution function. If there are s number of success and f number of failures, then the parameters of the beta distribution will be $\boldsymbol{\alpha}$=s+1 and $\boldsymbol{\beta}$=f+1. Beta distribution can be modeled as in (1),

$$Beta(\alpha, \beta) = \Gamma(\alpha + \beta)/\Gamma(\alpha)\Gamma(\beta)x^{\alpha-1}(1-x)^{\beta-1} \quad (1)$$

The expected value and variance can be written as,

$$E[x]=\alpha/(\alpha+\beta) \quad (2)$$

$$Var[x] = \alpha\beta/(\alpha + \beta + 1)(\alpha + \beta)^2 \quad (3)$$

The expected value defines the posterior probability of a given outcome after some past observation and the variance defines the deviation from the expected value. A beta distribution-based reputation rating function [10] has been proposed as in (6). The reputation rating function will compute reputation value for the vehicles on two parameters-packet loss ratio and packet error ratio. Then the overall reputation will be measured through averaging the reputation value for the two reputation parameters. The overall reputation rating is defined in (8).

3.1.1. Packet loss ratio

It can be defined as the ratio of number of packets lost to the total number of packets sent. It has been taken as a reputation parameter as, if a vehicle becomes malicious or compromised then it will intentionally loss packet for disrupting network operation. For example, in sinkhole attack a compromised vehicle or malicious vehicle will drop all the packets it will receive. A trustor (the vehicle which will evaluate trust value) vehicle *i* will observe a trustee (the vehicle whose trust value will be measured) vehicle *j* on packet loss as in (4);

$$X = PLR = n/N \quad (4)$$

where, n denotes the number of packets lost and N represents the total number of packets sent.

3.1.2. Packet error ratio

It can be represented as the proportion of the number of error packet received to the entire number of packets received. A malicious vehicle may modify a packet or inject erroneous data to mislead the receiver vehicle. Also, packet can be altered due to noise or other parameters of the wireless channel which leads to uncertainty in the communication among the vehicles. Similarly, the opinion about packet error ratio can be represented as in (5),

$$Y=PER= e/N \quad (5)$$

where, e defines the number of packets received which is erroneous and N denotes the total number of packets received. The model considers vehicle $v_{i,}$ will compute the rating for vehicle v_j for PLR and PER as $r_{PLR}^{v_i,v_j} and\ s_{PLR}^{v_i,v_j}$ respectively. Then the rating function can be defined as [10] in (6). Here, the rating is scaled for -2 to 2. All vehicles will measure the rating for the trustee vehicles and rate it on the scale -2 to 2. Every vehicle is supposed to communicate with another vehicle on basis of most elevated scale.

$$Rating\left(r_{PLR}^{v_i,v_j}, s_{PLR}^{v_i,v_j}\right) = 3\left(E\left(\phi\left(p\middle|r_{PLR}^{v_i,v_j}, s_{PLR}^{v_i,v_j}\right)\right) - (1/3)\right) \quad (6)$$

$$= (2r_{PLR}^{v_i,v_j} - s_{PLR}^{v_i,v_j} - 1)/(r_{PLR}^{v_i,v_j} + s_{PLR}^{v_i,v_j} + 2)$$

Similarly, for PER

$$Rating\left(r_{PER}^{v_i,v_j}, s_{PER}^{v_i,v_j}\right) = (2r_{PER}^{v_i,v_j} - s_{PER}^{v_i,v_j} - 1)/(r_{PER}^{v_i,v_j} + s_{PER}^{v_i,v_j} + 2) \quad (7)$$

Total rating:

$$R_{total} = (Rating\left(r_{PLR}^{v_i,v_j}, s_{PLR}^{v_i,v_j}\right) + Rating\left(r_{PER}^{v_i,v_j}, s_{PER}^{v_i,v_j}\right))/2 \quad (8)$$

3.2. TMM

In this section, the proposed trust management model is described. In VANET, a vehicle will evaluate the trustworthiness of its peer vehicle through trust model. Three trust parameters have been considered as trust evaluation metrics for this proposed trust model. The model will be evaluated through ANFIS.

3.2.1. Availability

It measures whether a device is available or unavailable based on the request. It is a logical trust parameter. A legitimate vehicle will be available whenever it is required to communicate but if it is compromised then the intruder (compromised vehicle) can bypass all the information to third party device which hinders it from communicating with the legitimate vehicle thus making the vehicle totally unavailable. The following mathematical (9) has been modelled for availability of a vehicle,

$$A = C_{ij}/(C_{ij} + C_{jk}) \quad (9)$$

Here, C_{ij} denotes the communication between a trustor vehicle i and trustee vehicle j and C_{jk} denotes the communication between the trustee vehicle j and the third-party vehicle k.

3.2.2. Intimacy

Interaction period or time is an additional substantial parameter to determine trust of a vehicle. If a trustee vehicle expends extra time with trustor vehicle then its inwardness will increase, or its closeness will be high enough to verify its reliability. Let, the total time a trustee vehicle i spends with trustor vehicle j is T_{ij} and the time trustor vehicle spends with other vehicles such as k is T_{jk}. Then agreeing to [17], the intimacy can be modeled as (10),

$$I = T_{ij}/(T_{jk} - T_{ij}) \quad (10)$$

3.2.3. Frequency

This parameter defines how frequently the trustee vehicle communicates with the trustor vehicle. If the relative frequency or the number of interactions increases between the trustee and trustor vehicle then the trust will be increased for the trustee vehicle. This trust parameter can be modeled as (11),

$$F = f_{ij}/(f_{jk} - f_{ij}) \quad (11)$$

where, f_{ij} denotes the total number of interactions between trustor vehicle j to trustor vehicle i and f_{jk} denotes the total number of interactions between the trustor vehicle j to another vehicles k.

3.3. ANFIS

Adaptive neuro fuzzy inference system is a machine learning approach that is comprises of neural network and fuzzy inference system [18]-[21]. ANFIS has been effectively utilized to evaluate trustworthiness value of trust model by [22]. In this paper, it has been used to evaluate trustworthiness of the above proposed trust model for vehicles. Figure 1 demonstrates ANFIS architecture. ANFIS utilizes neural networks learning algorithm to tune the parameters of the fuzzy system which is based on Takagi Sugeno fuzzy system [23], [24]. The rules of ANFIS can be represented as,

$$R_i = IF\ X\ is\ \mu_1\ and\ Y\ is\ \mu_2\ THEN\ f = p_i x + p_i y + c_i$$

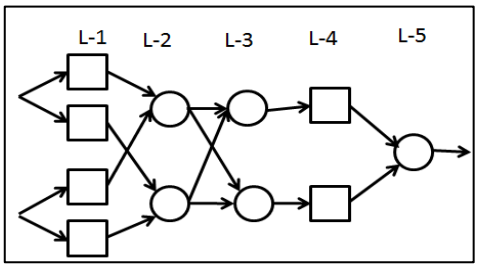

Figure 1. ANFIS architecture with five layers

where,
X and Y are input parameter.
μ_1 and μ_2 are membership function of fuzzy system.
f is the output of fuzzy system.
p, q and c are consequent parameters.

The first part of the rule before then is known as antecedent part and the next part that is after then is known as consequent part. The consequent parameters and antecedent parameters are tuned through neural network to get better error free output. The learning algorithm of ANFIS is hybrid learning algorithm that is a combination of gradient descent and least square methods. ANFIS comprises of five layers as depicted in the Figure 1. The layers can be described as [25],

In layer 1, the nodes represented as square nodes are adaptive nodes meaning it can adapt with the intended input by changing its parameter through neural network learning approach. This layer converts crisp value into fuzzy value. This conversion process is known as fuzzification and performed through membership function in (12).

$$O_{1,i} = \mu_{A,i}(x) \tag{12}$$

Where, $\mu_{A,i}(x)$ is the membership function of the fuzzy rules. In layer 2, all the nodes denoted as circle are fixed nodes and performs fuzzy operation using and, or, not on the fuzzy outputs from the first layer. Through these fuzzy rules desired output can be inferred. The output of this layer can be modeled as (13),

$$O_{2,i} = \mu_{A,i}(x) * \mu_{B,i}(y) \tag{13}$$

In layer 3, the nodes are known as normalized nodes. These nodes perform normalize operation on the output of the layer 2. Normalization operation can be represented as (14),

$$O_{3,i} = w_i/(w_1 + w_2) \tag{14}$$

Layer 4 nodes are adaptive node and they simply the product of the normalized output from the previous layer and the first order sugeno fuzzy model. The output can be represented as (15),

$$O_{4,i} = w_i f_i \tag{15}$$

Layer 5 performs defuzzification operation by summing the outputs of the previous layer. Defuzzification means conversion of fuzzy value to crisp value and the following (16) models this.

$$O_{4,i} = \sum_i w f_i \tag{16}$$

From this trust model trust metrics are taken as the input to the ANFIS structure. The rules of an ANFIS structure can be derived as m^n where m defines the number of membership functions and n defines the number of input variables. As the three-trust metrics have been considered as inputs and each input has three membership function, therefore the derived ANFIS comprises of 27 rules and the structure of the proposed ANFIS model is depicted in Figure 2,

The 27 rules of the ANFIS model are presented in Table 1 where one can fix availability, intimacy and frequency to take the corresponding decision value. Each trust metric has three membership function, high (H), medium (M), low (L) and the decision is divided into five parameters, they are-trust (T), untrust (UT), ignore (I), undistrust (UD) and distrust (D) [26]. Trust defines a vehicle is fully trusted and it reaches the threshold. Untrust means the trustee vehicle is not fully trusted but the trustor vehicle also does not distrust the trustee vehicle as it did not reach the threshold. Similarly, undistrust means a trustee vehicle has

lack of trust. Distrust decision is taken by a trustor vehicle for a trustee vehicle when the trustee vehicle is completely distrusted. Ignore decision is taken when the trustee vehicle is not completely trusted, also not completely distrusted.

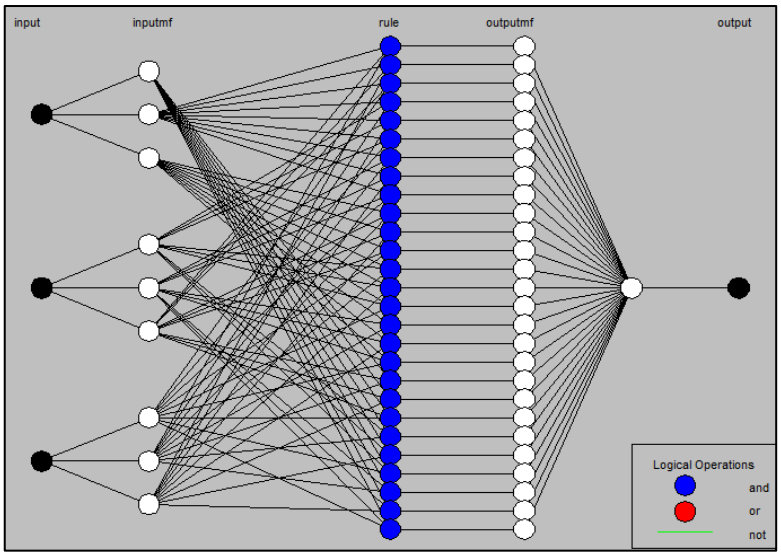

Figure 2. Proposed ANFIS structure

Table 1. Rules of ANFIS

Availability	Intimacy								
	H			M			L		
	Frequency			Frequency			Frequency		
	H	M	L	H	M	L	H	M	L
H	T	T	UT	T	UT	I	UT	I	UD
M	T	UT	I	UT	I	UD	I	UD	D
L	UT	I	UD	I	UD	D	UD	D	D

4. SIMULATION AND RESULTS

Simulation has been conducted in MATLAB. Each input parameter takes three membership functions. For low and high value, trapezoidal membership function has been assigned and for medium value it is triangular membership function and Figure 3 presents fuzzy member function for fuzzy input.

The output is scaled in five decisions such as trusted, untrusted, ignore, undistrusted and distrusted. All the output decisions have been assigned a constant value according to takagi sugeno fuzzy model of constant membership function. Then 27 rules of the ANFIS have been implemented and simulated. Figure 4 presents the simulation results for output decision against Availability, Intimacy and Frequency. From the simulation result, it can be seen that to be a trusted vehicle; it requires 80% trustworthiness value shaded in red color above blue region of Figure 4. Untrust decision shows the region below 80% and above 60% (blue region of the simulation results). Ignore follows the light blue color of simulation the figures that is from 50% to below 60%. The red zone underneath the simulation curve shows distrust region.

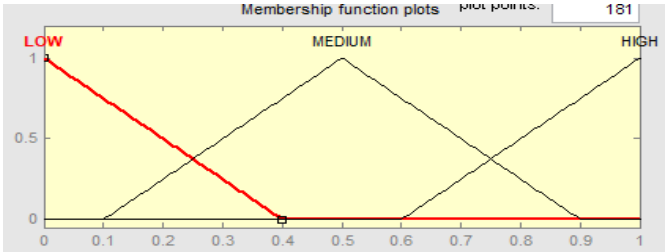

Figure 3. Declaring membership functions low, medium, high

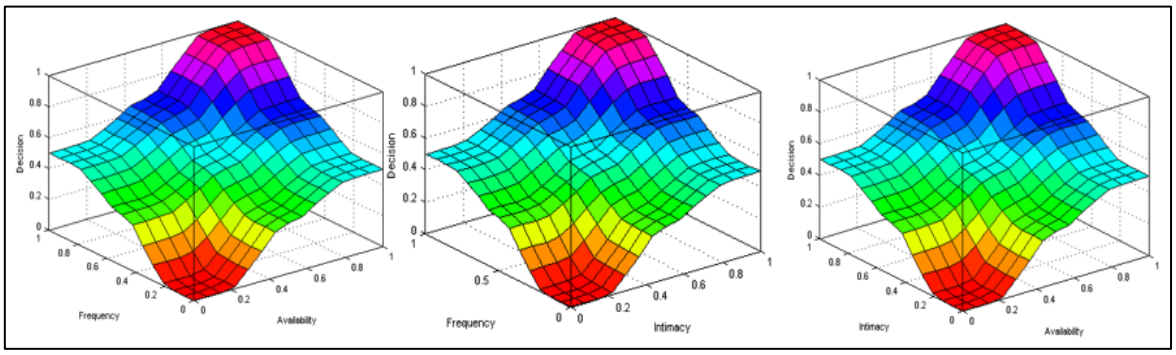

Figure 4. Decision against trust parameters

5. CONCLUSION

In this paper, to eliminate malicious or compromised vehicles which performs cyber-attacks from vehicular ad hoc network, a reputation management system based on beta probability distribution and a trust management model based on ANFIS have been proposed. The reputation management system takes two inputs such as packet loss rate and packet error rate. Average of the reputation for two different input reputation parameters have been calculated for deriving the overall reputation. The trust evaluation model based on ANFIS takes three major trust inputs as availability, intimacy and frequency. Each input is assigned three membership functions (for low and high it is trapezoidal and for medium it is triangular). The decision is classified as five variables (trust, untrust, ignore, undistrust, distrust). Simulation results reveal that to be a trusted vehicle it needs trust value above 80%. As a result, the proposed trust management model can effectively classify trustworthy vehicle from the network.

REFERENCES

[1] B. Koirala, S. S. Tangade and S. S. Manvi, "Trust Management Based on Node Stay Time in VANET," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 242–248, doi: 10.1109/ICACCI.2018.8554563.

[2] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Networks*, Aug. 2018, doi: 10.1016/j.adhoc.2018.08.010.

[3] Z. Lu, Q. Wang, G. Qu and Z. Liu, "BARS: a Blockchain-based Anonymous Reputation System for Trust Management in VANETs," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),* Jul. 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00025.

[4] S. Tangade and S. S. Manvi, "CBTM: Cryptography Based Trust Management Scheme for Secure Vehicular Communications," *15th International Conference on Control, Automation, Robotics and Vision (ICARCV),* 2018, doi: 10.1109/ICARCV.2018.8581173.

[5] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960-969, Apr. 2016, doi: 10.1109/TITS.2015.2494017.

[6] S. Tangade and S. S. Manvi, "Trust management scheme in VANET: Neighbour communication based approach," in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, 2017, pp. 741-744.

[7] T. Zaidi "An overview: Various attacks in VANET," *4th International Conference on Computing Communication and Automation (ICCCA),* IEEE, 2018, pp. 1-6, doi: 10.1109/CCAA.2018.8777538.

[8] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 6, pp. 28643-28660, 2018, doi: 10.1109/ACCESS.2018.2837887.

[9] A. Jøsang and R. Ismail, "The Beta Reputation System," *AIS eLibrary*, 2002.

[10] Y. C. Wei and Y. M. Chen, "Adaptive decision making for improving trust establishment in VANET," *16th Asia-Pacific Network Operations and Management Symposium*, 2014, pp. 1-4, doi: 10.1109/APNOMS.2014.6996523.

[11] D. B. Rawat, B. B. Bista and G. Yan, "Securing vehicular ad-hoc networks from data falsification attacks," in *2016 IEEE Region 10 Conference (TENCON)*, 2016, pp. 99-102, doi: 10.1109/TENCON.2016.7847967.

[12] C. A. Kerrache, C. T. Calafate, N. Lagraa, J. C. Cano and P. Manzoni, "Hierarchical adaptive trust establishment solution for vehicular networks," *IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016, pp. 1-6, doi: 10.1109/PIMRC.2016.7794617.

[13] A. Suman and C. Kumar, "A behavioral study of Sybil attack on vehicular network," *3rd International Conference on Recent Advances in Information Technology (RAIT)*, 2016, pp. 56-60, doi: 10.1109/RAIT.2016.7507875.

[14] M. U. Rehman, S. Ahmed, S. U. Khan, S. Begum and A. Ishtiaq, "ARV2V: Attack resistant vehicle to vehicle algorithm, performance in term of end-to-end delay and trust computation error in VANETs," *International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2018, pp. 1-6, doi: 10.1109/ICOMET.2018.8346338.
[15] N. Islam, "Certificate revocation in vehicular Ad Hoc networks: a novel approach," *International Conference on Networking Systems and Security (NSysS)*, 2016, pp. 1-5, doi: 10.1109/NSysS.2016.7400703.
[16] N. Kushwah and A. Sonker, "Malicious Node Detection on Vehicular Ad-Hoc Network Using Dempster Shafer Theory for Denial of Services Attack," *8th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2016, pp. 432-436, doi: 10.1109/CICN.2016.91.
[17] M. Mahmud *et al.*, "A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications," *Cognit. Comput.*, vol. 10, no. 5, pp. 864-873, Oct. 2018, doi: 10.1007/s12559-018-9543-3.
[18] A. M. Noman, K. E. Addoweesh and A. I. Alolah, "Simulation and Practical Implementation of ANFIS-Based MPPT Method for PV Applications Using Isolated Ćuk Converter," *International Journal of Photoenergy*, vol. 1, pp. 1-15, 2017, doi: 10.1155/2017/3106734.
[19] M. Alhamad, T. Dillon, and E. Chang, "A Trust-Evaluation Metric for Cloud applications," *nternational Journal of Machine Learning and Computing*, vol. 1, no. 4, pp. 416-421, 2011 doi: 10.7763/IJMLC.2011.V1.62.
[20] K. W. Nafi, T. S. Kar, M. A. Hossain, and M. M. A Hashem, "An Advanced Certain Trust Model Using Fuzzy Logic and Probabilistic Logic theory," I*nternational Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 3, no. 12, pp. 164-173 2012.
[21] Q. Ding and Xi Li, "A Novel Reputation Management Framework for Vehicular Ad Hoc Networks," *International Journal of Multimedia Technology*, vol. 3, no. 2, pp. 62-66, 2013.
[22] M. M. Arifeen, A. A. Islam, M.. M. Rahman, K. A. Taher, M. M. Islam and M. S. Kaiser, "ANFIS based Trust Management Model to Enhance Location Privacy in Underwater Wireless Sensor Networks," *International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2019, pp. 7-9, doi: 10.1109/ECACE.2019.8679165.
[23] S. A. Soleymani *et al.*, "A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks with Fog Computing," *IEEE Access,* vol. 5, pp. 15619-29, 2017, doi: 10.1109/ACCESS.2017.2733225.
[24] A. K. Jadoon, L. Wang, T. Li, and M. A. Zia, "Lightweight Cryptographic Techniques for Automotive Cybersecurity," *Wireless Communications and Mobile Computing*, vol. 1, pp. 1-15 2018, doi: 10.1155/2018/1640167
[25] A. A. Hmouz, J. Shen, R. A. Hmouz, and J. Yan, "Modeling and Simulation of an Adaptive Neuro-Fuzzy Inference System (ANFIS) for Mobile Learning," *IEEE Trans. Learn. Technol.*, vol. 5, no. 3, pp. 226-237, Jul. 2012, doi: 10.1109/TLT.2011.36.
[26] K. Chan and S. Adali, "A Survey on Trust Modeling," *ACM Computing Surveys,* vol. 48, no. 2, pp. 1-40, 2015, doi: 10.1145/2815595.

BIOGRAPHIES OF AUTHORS

Dilshad Ara Hossain has graduated in Computer Science and Engineering from Dhaka, Bangladesh. She has completed her final Masters (by research) in Department of Information and Communication Technology (ICT), from International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia. She has many Indexed Journal paper and renowned conference proceedings. Her research interest is in Cyber Security, IoT, Artificial Intelligence, Machine Learning, VANET and recent computer applications.

S. M. Salim Reza is an Assistant Professor of the Department of ICT, Bangladesh University of Professionals (BUP), Dhaka, Bangladesh. He is a Professional Member of IEEE and many other professional organizations. He is a keen planner & implementer with proficiency in managing academic and administrative activities entailing operational policies/norms, faculty appraisal/ computer science training. He has more than 50 research papers in ISI/ Scopus Indexed journal and many reputed international conferences.