Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 182 (2021) 71–79

Procedia Computer Science

www.elsevier.com/locate/procedia

17th International Learning & Technology Conference 2020 (17th L&T Conference)

Location Closeness Model for VANETs with Integration of 5G

Muhammad Haleem Junejo[a], Ab Al-Hadi Ab Rahman [a], Riaz Ahmed Shaikh [b], Kamaludin Mohamad Yusof [a]

[a]*Faculty of Electrical Engineering Universiti Teknologi Malaysia, 81310, Skudai, Johor, Malaysia*
[b]*Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*

Abstract

Nowadays, 5G is playing a significant role in the efficiency of network security and creating more and faster channels for communication. 5G is evolving industries such as healthcare, education, marketing, transportation, and V2X (Vehicle-to-everything). In addition, 5G considers a new radio access technology that is adding new applications like the Internet of Things (IoT), Augmented Reality, Virtual Reality, connected cars, connected people-to-people, smart city, connected homes that are considered using higher bandwidth and low latency. Mainly, this paper is focusing on security challenges faced by the Vehicular ad-hoc network (VANET). VANET faces threats in three different fields; security, safety, and infotainment, which further have numerous attacks. More precisely, this research conducted an in-depth study and proposed a VANET trust model. Therefore the proposed model deals specifically with the "location closeness" parameter. Moreover, the trust model integrated with 5G cloud to support greater coverage, effective network density with respect to network infrastructure and IoT as well. Therefore, in this article, an effort has been put forward to implement the model using case studies to validate the trust model based on the "location closeness" parameter. The results proved the valid implementation of the model by identifying the trusted communication between the vehicles.

Keywords: VANET; 5G, Trust Model; Location Closeness

1. Introduction

The 5G technology enables wireless communication to connect the people with others and especially with the large information in an efficient manner [1]. The 5G technology enables wireless communication to connect the people with others and especially with the large information in an efficient manner. It is the latest technology developed to ultimate requirements of the intelligent transport system (ITS), smart cities, health industry applications, advanced appliances and other IoT application [2], [3].

Vehicular Ad-Hoc Networks (VANETs) are considered subclasses of Mobile Ad-Hoc Networks (MANETs) [4], [5]. In VANETs, vehicles are capable of communicating among others such as; (i) Vehicle to vehicle (V2V), (ii) vehicle to infrastructure (V2I). VANET allows vehicles to exchange messages with regard to safety, road efficiency, and infotainment [6]–[8]. In vehicular ad-hoc networks (VANETs), vehicles exchange information related to road safety and traffic efficiency via vehicle to vehicle (V2V) or vehicle to infrastructure (V2I) communication. In case the exchanged information is incorrect, it leads to counterproductive; hence accidents and traffic congestion would increase. VANET is an important part of ITS [3], [9]. It utilizes the ITS infrastructure to offer secure information about the vehicle's location. For providing the ultimate services to the community, ITS is developed to avoid congestion, traffic violations, and other unforeseen incidents, and it further enhances the efficiency of traffic.

10.1016/j.procs.2021.02.010

Location closeness is an important variable in VANET, which plays a significant role in the trust model. The location closeness is a procedure to share the position of all neighboring vehicles with a period of time using all precautions such as; time, safety, and reliability [10].

It also describes the physical position of the actual vehicle with the help of location coordinates using VANET technology. The location closeness is used to verify vehicle information such as vehicle location at a certain time or the area in which the vehicles followed, and use personal information such as user ID and vehicle ID [11].

In location closeness, there are chances of receiving wrong messages or information regarding the vehicles. These attacks are known as "Global Position System Faking Attack"; this attack occurs when attacker broadcasts fake positioning information which can punish certain applications based on geographical routing, or even nodes located at that same falsified position [4], [12]. In addition, "Replayed, Altered, and Injected Messages Attack" is another kind of attacks, which can be defined as "dishonest vehicles can replicate many copies of the same message, modify the message, or create and inject new messages in the system while acting as a relay node for inter-vehicular communication". These attacks can clearly reduce the performance of all network applications, as well as the exchanged data trustiness.

VANET encounters several security challenges and problems to deal with authentication and privacy securely [13]. Therefore, untrustworthy or malicious vehicles increase the chances of transforming insecure information among the vehicles in VANETs. It is a fact that, in VANETs, the overall communication is executed in open access methods, which is the major fact to make this network vulnerable and post attacks by the attackers. The malicious vehicles can overwrite, modify, and can delete the messages in VANETs.

Vehicular Networks System comprises of a number of nodes such as RSU and vehicles. In this scenario, every node can communicate with other nodes by using short radio signals dedicated short-range communication DSRC (5.9 GHz), within a 1-kilometer range area [14], [15].

The communication between each vehicle is an Ad-hoc communication that means each connected node can move freely, usually, in a VANET each node is supposed to have an onboard unit (OBU) and there are RSU that is mounted along the roads. We present validation mechanisms to provide location closeness in VANET. In our approach, we use four different methods to calculate the location closeness: The trusted zone consists of Road Side Trust Zone coverage area (RSU_{TZ}), vehicle trust zone coverage area (V_{TZ}), vehicle zone coverage area ((V_Z (V_r, (V_s)) for the sender and receiver vehicle.

The rest of the paper is organized as follows. Section 2 presents the security challenges of VANET. Section 3 describes the proposed trust model and its implementation. Finally, section 4 concludes the paper.

2. VANET Security Challenges

According to Gartner, the research suggests that things are more connected than people in the world. Based on the report, approximately 8.4 billion IoT applications and devices were connected in use in 2017, which has been increased by 31% from 2016 [16],[17],[18]. This will probably reach to 20.4 billion by 2020. Moreover, another research conducted by International Data Corporation (IDS), which indicated that IoT spending was almost $772.5 billion in 2018, which was around 15% more than in 2017. IDC also forecasts that overall investment in 2020 and 2021 will touch $1 trillion and $1.1 trillion respectively [19].

It is important in VANET to reduce the security attacks in different infotainment, safety and security-related applications that require the secure exchange of data among nodes. In VANET there are six major requirements [4], [11], [20], [21] as shown in Table 1 and defined as follows [4], [11], [20], [21]:

i. Availability: VANET network should be available to utilize the security, safety, and infotainment application.
ii. Authenticity: This is the most important factor in VANET. It consists of identification, authentication, and access control.
iii. Confidentiality: It enables secure communication between the nodes.
iv. Integrity: It ensures that the node receives the messages in a correct form without alteration or modification.
v. Privacy: The location and identity will keep private and secure.
vi. Non-repudiation: In VANET non-repudiation confirms that the given information sends by a node cannot be denied that it has transmitted.

2.1. Attacks in VANET

This section listed the common threats faced by VANET [4], [5], [11], [20]–[22] also mentioned in Table 1.

i. Certificate Replication Attack: In this attack, the certificate is replicated multiple times.

ii. Eavesdropping Attack: Attacker intercept transmitted the communication to gain access or password.

iii. Tracking Tracing Attack: Trace or track the correct position of device and vehicle.

iv. DoS Attack: it is caused by any action that prevents to access part of a network from functioning correctly and timely manner. This causes a legitimate vehicle to access the application or services.

v. Jamming Attack: This attack is almost the same as a DoS attack, but this time the shared bandwidth among the nodes or network is jammed.

vi. Coalition and Platooning Attack: This attack work in a group where multiple dishonest vehicles collaborate with each other to perform malicious activities such as; bandwidth usage or stopping any services.

vii. Betrayal Attack: This attack occurs when honest vehicles become dishonest during transmission.

viii. Replayed, Altered, and Injected Messages Attack: This attack altered or modify the information during messages transmission. This will cause to send multiple erroneous messages.

ix. Illusion Attack: Typically this attack is related to hardware component for example wrong sensor reading, incorrect messages are sent to other vehicles.

x. Masquerading Attack: This attack caused by a dishonest vehicle wearing a legitimate certificate by disturbing and doing malicious activities.

xi. Impersonation Attack: A dishonest node assumes to another node by using the wrong identity.

xii. Sybil Attack: A dishonest node transmits multiple fabricated message IDs to the legitimate node where the legitimate nodes assume that they are dealing with multiple devices.

xiii. GPS Position Faking Attack: Falsified positioning based on geographical coordinates.

xiv. Timing Attack: The attacker adds the delay between the packets, which cause unforeseen incidents.

xv. Blackhole Attack: A dishonest node transmits the false reply message to the other vehicle that dishonest host is optimal route information to the destination.

xvi. Gray hole Attack: A dishonest host drops the packet of the particular vehicle in the network and transmits other packets to its destination.

		VANET Application Threats		
		Security	Safety	Infotainment
VANET Security Requirements	Availability		Denial of Service	
			Jamming	
			Coalition and Platooning	
			Betrayal	
				Replayed, Altered, and Injected Messages
		GPS Position Faking		GPS Position Faking
			Timing	Timing
			Blackhole	Blackhole
			Greyhole	Greyhole
	Authenticity	Certificate Replication	Certificate Replication	
			Betrayal	
				Replayed, Altered, and Injected Messages
		Masquerading	Masquerading	
		Impersonation	Impersonation	
			Sybil	
	Integrity		Betrayal	
				Replayed, Altered, and Injected Messages
				Illusion
	Privacy	Eavesdropping		
		Tracking/Tracing		
			Coalition and Platooning	
	Non-repudiation	Sybil		Sybil

		GPS Position Faking		GPS Position Faking
	Privacy	Eavesdropping		

Target Attacks on multiple applications		
Safety & Security	Security& infotainment	Safety & infotainment

Table. 1. Trust VANET Application Threats and Attacks

Table 1 illustrates the attacks on the application of VANET specific to particular requirements. In the table, the “Safety and Security Attacks” are highlighted in the “BLUE” color, “Security and Infotainment Attacks” are highlighted in the “GREEN” color, and finally the “Safety and Infotainment Attacks” are showing in “ORANGE” color.

3. VANET Proposed Trust Model

This section describes the proposed model and its implementation using case studies. Figure 1. is showing the proposed model which has different components. The first part of this model is the “Trust Estimation Model”, it starts to receive a message and then calculates the trust value on the bases of four cases. Further, the trust value will be forwarded to the next part of the model known as the “Decision Model”. The decision model processes the trust value and checks whether to process the message or discard it on the bases of the application-specific threshold value.

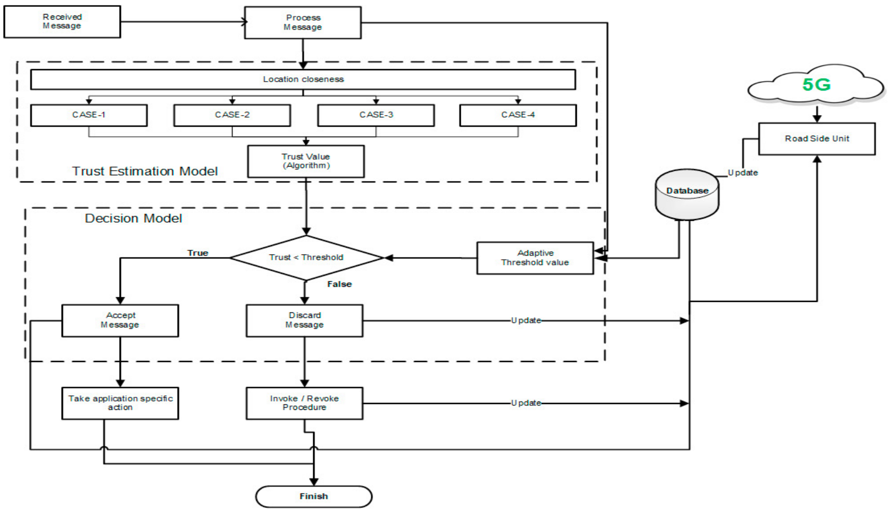

Fig. 1. Proposed Trust Model

As described above, the proposed trust model consists of two main blocks; (i) Trust Estimation Model, (ii) Decision Model. The decision Model in our model received trust value from the trust model to decide whether to process the message or discard it on the bases of the threshold value. If the trust value is less than the threshold value a TRUE message is generated and the decision box accepts the value send an update to a database and takes an application-specific decision. Our Trust Model is for two types of applications that are safety and traffic efficiency.

i. If the trust value exceeds the application-specific threshold value, the message is discarded and the FALSE message is generated.

ii. The false generated message will be discarded and information related to the false message will be stored in the database. Based on the value of the false generated message, invoke/revoke procedure will be executed.

Road Side Unit (RSU) is the trusted unit in the model. RSU will provide initial trust value to all vehicles in the region of interest. All vehicles will have a unique ID in the region. RSU generated an alert message to inform about a malicious vehicle in the region of interest. This alert message helps vehicles in the region not to trust the information received from the malicious node.

3.1. Model Implementation

Vehicular Networks System comprises of a number of nodes such as RSU and vehicles. In this scenario, every node can communicate with other nodes by using short radio signals dedicated to short-range communication DSRC (5.9 GHz), within a 1-kilometer range area.

The communication between each vehicle is an Ad-hoc communication that means each connected node can move freely, usually, in a VANET each node is supposed to have an onboard unit (OBU) and there are RSU that is mounted along the roads. We present validation mechanisms to provide location closeness in VANET. In our approach, we use four different methods to calculate the location closeness: The trusted zone consists of Road Side Trust Zone coverage area ($\mathrm{RSU_{TZ}}$), vehicle trust zone coverage area ($\mathrm{V_{TZ}}$), vehicle zone coverage area ($\mathrm{V_Z}$ ($\mathrm{V_r}$, $\mathrm{V_s}$)) for the sender and receiver vehicle.

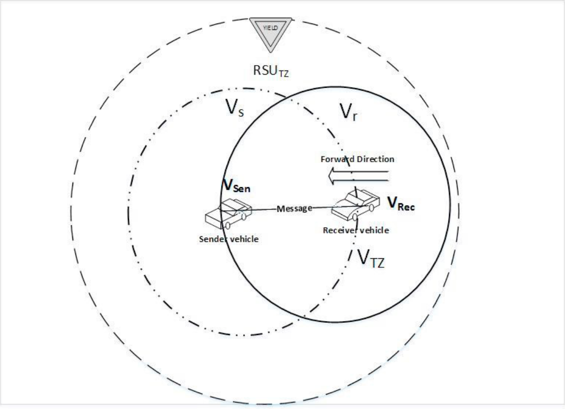

Fig2: Location Verification Trust Zone

As shown in Figure 2, the RSU_{TZ} coverage is larger in the trust zone than the coverage area of the sender and receiver vehicles $V_Z(V_r, V_s)$.

The trust calculation can take place in the following four possible cases/scenarios.

3.1.1 Case 1

In this case, as shown in Figure3, the vehicle received a message from another vehicle inside the roadside unit trust zone coverage area RSU_{TZ} and vehicle trust coverage areaV_{TZ}. Vehicle location closeness L_c computes as

$$\boldsymbol{L_C = 1 \qquad if \quad V_L \in |RSU_{TZ}| \cap |V_{TZ}|} \tag{1}$$

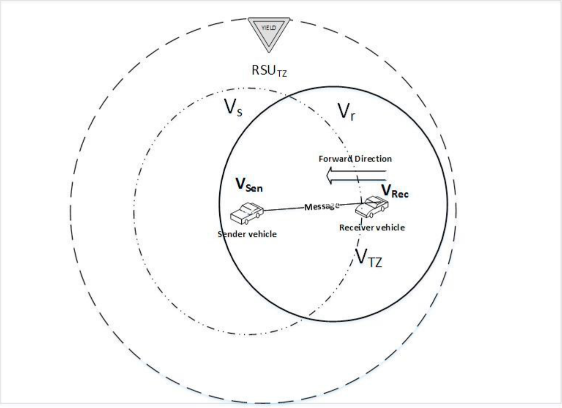

Fig. 3 Received message from Road site unit trust zone and vehicle trust zone the value one shows to trust the message.

3.1.2 Case 2

In case two (Figure 4) the vehicle received a message from the vehicle from another vehicle that in the coverage area of RSU but outside the vehicle trust coverage area V_{TZ}. Furthermore, the received message direction is opposite to vehicle movement.

In this case, the vehicle location closeness calculated as,

$$L_C = \frac{\mathbf{2}}{\mathbf{3}} + \frac{\mathbf{1}}{|\boldsymbol{Send_{loc}} - \boldsymbol{Recv_{loc}}|} \qquad \boldsymbol{if} \quad \boldsymbol{V_L} \in |\boldsymbol{RSU}| \setminus |\boldsymbol{V_{TZ}}| \tag{2}$$

Whereas $Send_{loc}$ sender location and $Recv_{loc}$ is the receiver location.

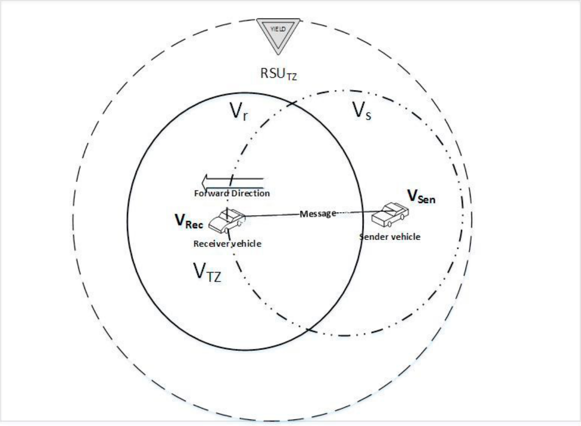

Fig. 4 Received message from a vehicle in the coverage area of RSU and outside Vehicle trust zone

3.1.3 Case 3

In case three as illustrated in Figure 5, the received message is from the vehicle coverage area V_Z but outside the roadside coverage area RSU. In addition, the received message direction is the same as the vehicle movement. In this case, the vehicle location closeness calculated as,

$$L_C = \frac{\mathbf{1}}{\mathbf{3}} + \frac{\mathbf{1+\Upsilon}}{|\boldsymbol{Send_{loc}} - \boldsymbol{Recv_{loc}}|} \qquad \boldsymbol{if} \quad \boldsymbol{V_L} \in |\boldsymbol{V_Z}| \setminus |\boldsymbol{RSU}| \tag{3}$$

Whereas, ϒ is the distance between the sender vehicle and receiver,

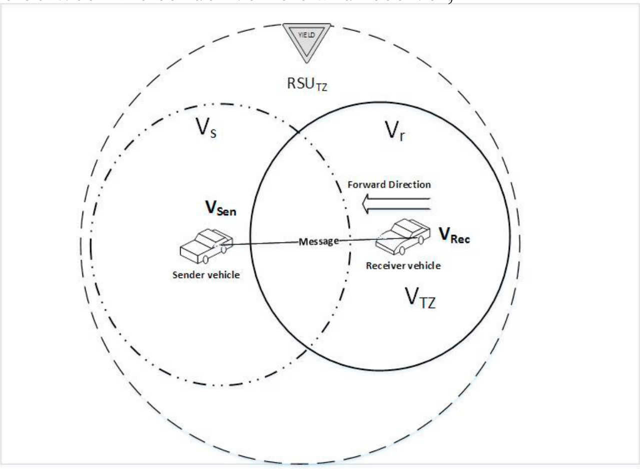

Fig. 5 The vehicle received a message from a vehicle in the vehicle trust zone in the direction of movement

3.1.4 Case 4

In this case, as showing in Figure 6, the vehicle received a message from another vehicle that is in the coverage area of the vehicle zone $\mathrm{V_Z}$ but outside the road site unit trust zone RSU_{TZ},

$$\boldsymbol{L_C = 0 \qquad if \quad V_L \notin |V_{TZ}| \cap |RSU_{TZ}|} \tag{4}$$

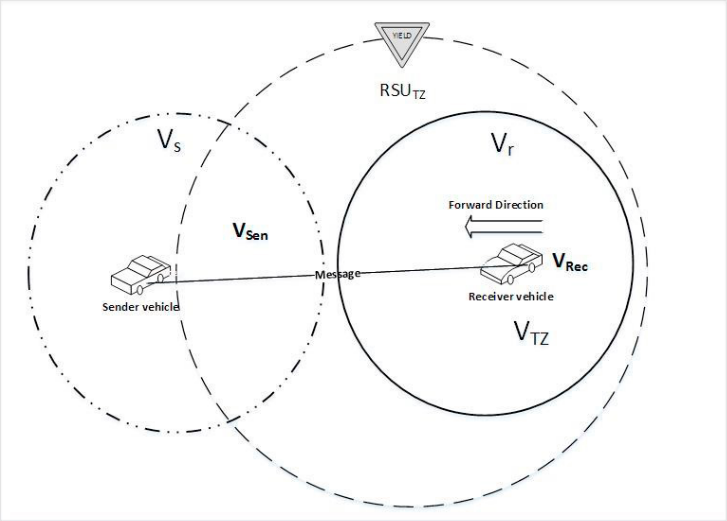

Fig. 6 The vehicle received a message from the vehicle outside of $\boldsymbol{RSU_{TZ}}$and Vehicle trust zone $\boldsymbol{V_{TZ}}$

3.2 Location Closeness Equation

The location closeness in our scenario depends on four cases, the location closeness is calculated below:

$$\boldsymbol{L_C} = \left\{ \begin{array}{ll} \mathbf{1} & \boldsymbol{if \quad V_L \in |RSU_{TZ}| \cap |V_{TZ}|} \\ \frac{\mathbf{2}}{\mathbf{3}} + \frac{\mathbf{1}}{\boldsymbol{|Send_{loc} - Recv_{loc}|}} & \boldsymbol{if \quad V_L \in |RSU| \setminus |V_{TZ}|} \\ \frac{\mathbf{1}}{\mathbf{3}} + \frac{\mathbf{1+\gamma}}{\boldsymbol{|Send_{loc} - Recv_{loc}|}} & \boldsymbol{if \quad V_L \in |V_Z| \setminus |RSU|} \\ \mathbf{0} & \boldsymbol{if \quad V_L \notin |V_{TZ}| \cap |RSU_{TZ}|} \end{array} \right\} \mathbf{(5)}$$

The Equation shows that the vehicle received a message from a number of sources and on the basis of received message calculates L_c to trust the message or discard it. Equation 5 shows that the vehicle received a message from a number of sources and on the basis of received message calculates location closeness L_c to trust the message or discard it. We assume four different cases to calculate location closeness as shown in Figure 7, one shows the distance between the two nodes, the distance between the sender and RSU, and location closeness on the basis of L_c. Here in our scenario, we assume the coverage area of RSU is (50, 50) whereas the radius is 25. Figure7 shows the location closeness in the case of V2V. Remarkable results to emerge from the graph are that values above the 0.5 are trusted. Case 1 and 2 of location closeness in our scenario shows the vehicle to vehicle communication is in the trusted range of RSU and vehicle zones. The case shows trust values between 0 and 1.Here we assume the value may be trusted and may not be. So the value forwarded to the trust decision model. The value 0 is not trusted value as the V2V is out of trusted zones of RSU and vehicle trust zone. The trust value less than 0.5 is less trusted value, whereas 0 is considered to be an un-trusted value. In the location closeness model, we combine all four cases (Equation 5), in which the value 1/3 is used to create a boundary between cases 3 and 4 and 2/3 is used to create a boundary between case 1 and 2.

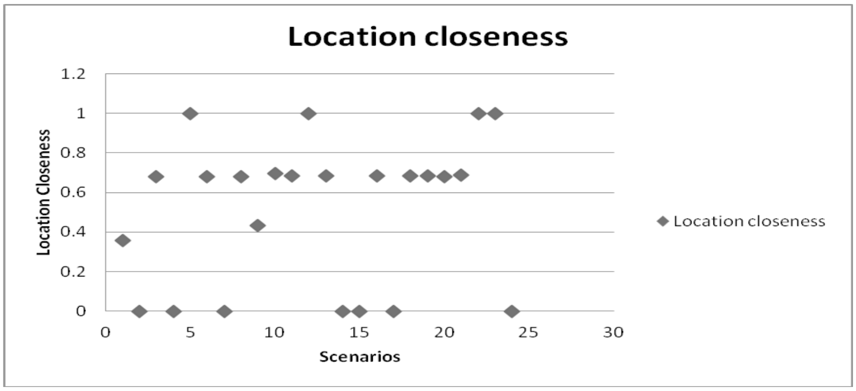

Fig. 7 Location Closeness

4. Conclusion and Future Work

The security and secure communication in the VANETs are important to provide better and actual communication between the nodes. This research highlights the importance of VANET security and described the list of common threats can be attacked on VANET. Moreover, the concept of integrating the 5G in the proposed model is establishing the process with higher bandwidth to secure the vehicular ad-hoc network. Therefore, this research proposed a model for measuring "location closeness", through two main blocks (Trust Model & Decision Model) for executing and transmits the messages between the nodes. The model further has been implemented and validated using four cases. The results represented the model validation was performed by measuring the trust value and taking the decision based on the pre-defined threshold. This research is useful for establishing the secured community with the help of the proposed trust model. The experiment was specifically based on calculating the "Location Closeness" parameter. In the future, the proposed model will be enhanced by adding other parameters such as Data Integrity and Authentication.

REFERENCES

[1] D. M. West, "How 5G technology enables the health internet of things," *Brookings Cent. Technol. Innov.*, vol. 3, pp. 1–20, 2016.

[2] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "Security Challenges and Concerns of Internet of Things (IoT)," in *Cyber-Physical Systems: Architecture, Security and Application*, Springer, 2019, pp. 153–185.

[3] I. García-Magariño, S. Sendra, R. Lacuesta, and J. Lloret, "Security in vehicles with IoT by prioritization rules, vehicle certificates and trust management," *IEEE Internet Things J.*, 2018.

[4] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," in *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on*, 2013, pp. 1–6.

[5] B. Mokhtar, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, 2015.

[6] Q. Alriyami, A. Adnane, and A. K. Smith, "Evaluation criterias for trust management in vehicular ad-hoc networks (VANETs)," in *Connected Vehicles and Expo (ICCVE), 2014 International Conference on*, 2014, pp. 118–123.

[7] P. Offor, "Vehicle ad hoc network (vanet): Safety benefits and security challenges," *Available SSRN 2206077*, 2012.

[8] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for vanets," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[9] B. Donnellan, C. Klein, M. Helfert, and O. Gusikhin, *Smart Cities, Green Technologies and Intelligent Transport Systems: 7th International Conference, SMARTGREENS, and 4th International Conference, VEHITS 2018, Funchal-Madeira, Portugal, March 16-18, 2018, Revised Selected Papers*, vol. 992. Springer, 2019.

[10] U. Ihsan, S. Yan, and R. Malaney, “Location Verification for Emerging Wireless Vehicular Networks,” *IEEE Internet Things J.*, 2019.

[11] M. S. Sheikh and J. Liang, “A Comprehensive Survey on VANET Security Services in Traffic Management System,” *Wirel. Commun. Mob. Comput.*, vol. 2019, 2019.

[12] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, “A survey on security attacks in VANETs: Communication, applications and challenges,” *Veh. Commun.*, p. 100179, 2019.

[13] A. Mondal and S. Mitra, “TDMAC: A timestamp defined message authentication code for secure data dissemination in VANET,” in *Advanced Networks and Telecommunications Systems (ANTS), 2016 IEEE International Conference on*, 2016, pp. 1–6.

[14] Y. P. Fallah and S. M. O. Gani, “Efficient and High Fidelity DSRC Simulation,” in *Connected Vehicles*, Springer, 2019, pp. 217–243.

[15] J. Choi, V. Marojevic, R. Nealy, J. H. Reed, and C. B. Dietrich, “DSRC and IEEE 802.11 ac Adjacent Channel Interference Assessment for the 5.9 GHz Band,” in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019, pp. 1–5.

[16] D. J. Mala, “IoT Functional Testing Using UML Use Case Diagrams: IoT in Testing,” in *Integrating the Internet of Things Into Software Engineering Practices*, IGI Global, 2019, pp. 125–145.

[17] Y. Tan, W. Yang, K. Yoshida, and S. Takakuwa, “Application of IoT-Aided Simulation to Manufacturing Systems in Cyber-Physical System,” *Machines*, vol. 7, no. 1, p. 2, 2019.

[18] R. van der Meulen, “Gartner Report,” 2017.

[19] FRAMINGHAM, “IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors,” 2019.

[20] M. S. Al-Kahtani, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs),” in *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, 2012, pp. 1–9.

[21] J. Zhang, “A survey on trust management for vanets,” in *Advanced information networking and applications (AINA), 2011 IEEE international conference on*, 2011, pp. 105–112.

[22] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, “A trust modeling framework for message propagation and evaluation in VANETs,” in *Information Technology Convergence and Services (ITCS), 2010 2nd International C*