Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 194 (2021) 45–59

Procedia Computer Science

www.elsevier.com/locate/procedia

18th International Learning & Technology Conference 2021

# Lightweight Trust Model with Machine Learning scheme for secure privacy in VANET

Muhammad Haleem Junejo[a], Ab Al-Hadi Ab Rahman[a], Riaz Ahmed Shaikh[b] , Kamaludin Mohamad Yusof[a] Dileep Kumar[c] and Imran Memon[d]

[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*
[c]*State Key Laboratory of Industrial Control Technology, College of Control Science & Engineering, Zhejiang University, Hangzhou ,china*
[d]*Department of computer science , bahria university , Karachi campus , sindh , Pakistan ;*

**Abstract**

A vehicular ad hoc network (VANETs) is transforming public transport into a safer wireless network, increasing its safety and efficiency. The VANET consists of several nodes which include RSU (Roadside Units), vehicles, traffic signals, and other wireless communication devices that are communicating sensitive information in a network. Nevertheless, security threats are increasing day by day because of dependency on network infrastructure, dynamic nature, and control technologies used in VANET. The security threats could be addressed widely by using machine learning and artificial intelligence on the road transport nodes. In this paper, a comparison of trust and cryptography was presented based on applications and security requirements of VANET.



*Keywords:* VANET, Trust Model, Machine Learning

## 1. Introduction

In recent times, intelligent and smart devices became more and more common in everyday life. Machine Learning (ML) and Artificial Intelligence (AI) help devices to perform complex tasks efficiently[1]. These devices consist of mobile phones, vehicles, airplanes, trains, household items, doors, and in summary, almost every electronic device is connected to the Internet[2]. This phenomenon is leading to the era of smart homes, AI-based systems, the Internet of Things (IoT). IoT-enabled devices examined the gathered data to make a meaningful correlation based on AI and ML algorithms to make decisions. IoT enables devices to have the monitor capability, device management, datastore


10.1016/j.procs.2021.10.058

analyze received data, and took an appropriate decision based on ML and AI-based algorithms[3]. Vehicles enabled with IoT and embedded sensors possibly offer an optimized route, safety, security, accident prevention, congestion avoidance, and autonomous driving. Expansion of IoT technology created new applications which make the life of people better and easy[4]. The technology advancement in IoT and smart applications helping cities to become smarter. The integration and emergence of IoT in the field of transportation bringing the concept of Intelligent Transportation Systems(ITS)[5], [6]. ITS attracts the attention of academia, industry, and research as there is huge space available for further enhancement. The most significant area of research in ITS is the Vehicular Ad-Hoc Network(VANET)[7]. In VANET the vehicle equipped with sensing technology and onboard computing brings an advanced level of connectivity in smart cities and ITS. The sensing system consists of a wide range of sensors that includes radars, engine control units, cameras, light detection, and ranging and others help the vehicle to predict the surrounding environment in real-time and take decisions. Smart sensing technology along with computing capabilitytransforming vehicles into a powerful intelligent device. VANET will ultimately have a great impact on thedevelopment of the smart city, society helps traveling safer and comfortably. This advancement in VANET bringing the concept of autonomous driving into reality. Vehicular Ad-Hoc Networks (VANETs) are considered subclasses of Mobile Ad-Hoc Networks (MANETs) [8]–[10]. In VANETs, vehicles are communicating with each other and infrastructure; (i) Vehicle to vehicle (V2V), (ii) vehicle to infrastructure (V2I). VANET permits vehicles to transfer messages with several applications of life safety, road efficiency, and infotainment[11]–[13]. In case the if vehicle received false information, it leads to counterproductive; hence accidents and traffic congestion would increase. VANET consists of several nodes most important are RSU and vehicles. The nodes connect with other nodes employing short radio signals dedicated short-range communication DSRC 5.9 GHz, inside 1000 meters [14], [15]. The rest of the paper is organized as follows. Section 2 presents the related work, Section 3 describes the VANET security, section 4 Authentication Schemes based on a pseudonym, section 5 represents VANET challenges in aroad network, section 6 represents the proposed trust model. Finally, section 7 location closeness, and section 8 conclude the paper.

## 2. Related work

Machine Learning (ML) is a new theory closely linked with artificial intelligence. ML-based devices perform tasks for example clustering, pattern recognition, classification, and prediction. The ML-based devices are best suitable to solve the problem for example classification, regression, classification, and associated rules determinations. ML is broadly categorized into four parts. They have Supervised Learning(SL), Unsupervised Learning(UL), semi-supervised Learning(SsL), and Reinforcement Learning(RN).

### *2.1. Supervised Learning*

Supervised learning (SL) is applied random forest or linear regression algorithms to solve a problem in the field of the weather forecast, population growth prediction, and weather forecasting. Furthermore, it solves problems such as speech recognition, identity fraud detection, digital recognition, and diagnostic by using algorithms like random forest, support vector machines, and Nearest Neighbour.

### *2.2. Unsupervised Learning*

Unsupervised learning(UL) on the based-on testing data predicts future incidents. It deals with problems like big data visualization, the discovery of hidden structures, and feature elicitation.

### *2.3. Semi-supervised Learning*

Semi-supervised(SsL) learning is the combination of SL and UL and using the algorithms used by both learning methods.

### 2.4. Reinforcement Learning

Reinforcement learning using the chain method to solve a problem such as a robot navigation, AI gaming, skill acquisition, and real-time decision. Moreover, in this learning method the algorithms trying to predict the future incident based on several tuning parameters. The two important fields like Deep Learning and Artificial Neural Networks (ANN) are based on Reinforcement Learning. Table 1 defines the literature review based on different ML learning techniques based on different smart traffic applications such as parking, route optimization, accident detection and prevention, traffic lights, road congestion and anomalies, and infrastructure.

Table 1 ML algorithms in IoT smart transportation applications

| | | Author | Algorithm | Algorithm type |
|---|---|---|---|---|
| Type of learning method | Supervised | A Ghosh [16] | AdaBoost | Ensemble |
| | | G Fusco [17] | Bayesian Network Seasonal Autoregressive Integrated | Bayesian |
| | | Devi[18] | Decision Tree | Decision Trees |
| | | G Fusco | Feed Forward Neural Networks (FF-NN) | Artificial Neural Networks(ANN) |
| | | Devi[18] | FF-NN | ANN |
| | | Hou[19] | FF-NN | ANN |
| | | Kulkarni[20] | FF-NN | ANN |
| | | Munoz-Organero[21] | k-Nearest Neighbor (k-NN) | Instance-Based (IB) |
| | | Ozbayoglu[22] | k-NN) | IB |
| | | NG[23] | k-Nearest Neighbor (k-NN) | IB |
| | | Devi[18] | Logistic Regression | Regression |
| | | Devi[18] | Random Forest (RF) | Ensemble |
| | | Hou[19] | RF | Ensemble |
| | | Ghadge[24] | RF | Ensemble |
| | | NG[23] | RF | Ensemble |
| | | Dogru[25] | RF | Ensemble |
| | | Hou[19] | Regression Tree | Decision Trees |
| | | Ozbayoglu[22] | Regression Tree | Decision Trees |
| | | Wu[26] | Support-VectorMachine (SVM) | Non-probabilistic Linear Classification-NPLC |
| | | Devi[18] | SVM | NPLC |
| | | Munoz-Organero[21] | SVM | NPLC |
| | | NG[23] | SVM | NPLC |
| | | Dogru[25] | SVM | NPLC |
| | | Almeida[27] | SVM | NPLC |
| | Reinforcement | D Kwon [28] | Convolutional Neural Network (CNN) and Deep CNN | Deep Learning (DL) |
| | | G Amato [29] | CNN and Deep CNN | DL |
| | | K Gopalakrishnan [30] | CNN and Deep CNN | DL |
| | | W Liu[31] | Coupled Hidden Markov Model (CHMM) | Markov Model |
| | | Yang [32] | Deep Belief Networks (DBN) | DL |
| | | Munoz-Organero[21] | DBN | DL |
| | | Jimmy Ba[33] | Deep Recurrent Attention Model (DRAM) | Recursive Neural Networks |
| | | Amato[29] | Fully Connected Networks (FCN) | DL |
| | | Ryder[34] | Inception Neural Networks | DL |
| | | Sang[35] | Markov Decision Process (MDP) | Discrete Time Stochastic Control |
| | | Fusco[17] | Nonlinear Auto Regressive eXogenous model (NARX) | Recursive Neural Networks |
| | | Sang[35] | Q-Learning | Stochastic Control-Markov Model |

| | | | | |
|---|---|---|---|---|
| | | Y. Lv[36] | Stacked Auto Encoder (SAE) with Greedy Layer-wise training | DL |
| | Unsupervised | Kanoh[37] | Fuzzy C-Means (FCM) | Clustering |
| | | Yang[32] | K-Means | Clustering |
| | | Al Mamun[38] | K-Means | Clustering |
| | | Ghadge[24] | K-Means | Clustering |
| | | Wu[26] | Markov Random Field (MRF) | Markov Model |

## 3. VANET SECURITY

The security of an intelligent vehicle is gaining importance as it is connected to IoT and brings enormous benefits to society. Information sharing is crucial in the vehicle as any forged, attacked information may cause serious injuries and accidents. Nowadays, securing VANET is a complex problem with several challenges. These challenges are listed, in detail below. To address these security challenges, several requirements have to be considered. These requirements are classified into six main categories, i.e. Availability, Confidentiality, Authentication, Privacy,Integrity, and Non-repudiation.

Table 2 Explanation of VANET Requirements

| Requirement | Definition / Explanation |
|---|---|
| Availability | This tells that VANET should be available and reachable all the time to guarantee the safety of the node. |
| Authentication | This means verifying the identity of a node and differentiates the honest vehicles from the dishonest ones. |
| Confidentiality | nodes |
| Integrity | The Integrity ensures that the message transmitted between two nodes has not been altered, modified, and/or changed during the transmission |
| Privacy | Privacy is the primary significant requirement in VANET. The key sensitive information is 1. Vehicle location, 2.Identification of vehicle, 3. identification of the driver, and details of the traffic route to be followed by the vehicle. |
| Non–repudiation | The non-repudiation requirement confirms that the sending node cannot deny a sent message. |

### *3.1. Attacks in VANET*

Table 3 Threats faced by VANET

| | |
|---|---|
| Certificate Replication Attack | The certificate is duplicated and replicated several times. |
| Eavesdropping Attack | In this attack, communication intercepts to gain access or password. |
| Tracking Tracing Attack | The correct position of the device and vehicle that is easily traceable. |
| Denial of Service Attack (DoS) | DoS is caused by stopping accessing the VANET from functioning appropriately and timely manner. This results from a legitimate vehicle not gaining access to the VANET. |
| Jamming Attack | Shared bandwidth among the nodes or network is jammed. |
| Coalition and Platooning Attack | This is a group-based attack, where multiple untrusted vehicles cooperate with each other to perform malicious activities such as; bandwidth usage or stopping any services |
| Betrayal Attack | This attack occurs when a legitimate vehicle becomes dishonest during a journey in the network. |
| Replayed, Altered, and Injected Messages Attack | In this attack, the information is altered or modify during message sending. This will result to send multiple erroneous messages. |
| Illusion Attack | Mostly this attack is related to hardware components for example wrong sensor reading, incorrect messages are sent |
| Masquerading Attack | This attack is caused by a dishonest vehicle wearing a legitimate certificate by disturbing and doing malicious activities. |
| Impersonation Attack | A untrusted node presumes another node by utilizing the wrong identity. |
| Sybil Attack | An attacker node transmits multiple fabricated message IDs to the honest node where the honest nodes assume that they are dealing with multiple devices. |
| GPS Position Faking Attack | In this attack, dishonest none Falsified positioning based on geographical coordinates. |
| Timing Attack | The attacker node adds the delay between the messages |
| Blackhole Attack | An attacker node sends a false reply message to the other vehicle that the dishonest host is optimal route information to the destination. |
| Gray hole Attack | A dishonest host falls the packet of the specific node in the network and sends out other packets to its destination. |

Table 4 VANET Applications threats and solutions based on Trust vs Cryptography

| | | | VANET Application Threats | | | Solution Based | | Attacked Scenario | |
|---|---|---|---|---|---|---|---|---|---|
| | | | Security | Safety | Infotainment | Trust | Cryptographic | V2V | V2I |
| VANET Security Requirements | Availability | Security& infotainment | | Denial of Service | | Yes | Yes | Yes | No |
| | | | | Jamming | | Yes | Yes | Yes | No |
| | | | | Coalition and Platooning | | Yes | No | Yes | No |
| | | | | Betrayal | | Yes | No | Yes | No |
| | | | | | Replayed, Altered, and Injected Messages | Yes | Yes | Yes | No |
| | | | GPS Position Faking | | GPS Position Faking | Yes | No | Yes | Yes |
| | | | | Timing | Timing | Yes | Yes | Yes | Yes |
| | | | | Blackhole | Blackhole | Yes | Yes | Yes | No |
| | | | | Greyhole | Greyhole | Yes | Yes | Yes | No |
| | Authenticity | Safety & infotainment | Certificate Replication | Certificate Replication | | No | Yes | Yes | Yes |
| | | | | Betrayal | | Yes | No | Yes | No |
| | | | | | Replayed, Altered, and Injected Messages | Yes | Yes | Yes | No |
| | | | Masquerading | Masquerading | | Yes | No | Yes | No |
| | | | Impersonation | Impersonation | | Yes | Yes | Yes | No |
| | | | | Sybil | | Yes | Yes | Yes | No |
| | Integrity | | | Betrayal | | Yes | No | Yes | No |
| | | | | | Replayed, Altered, and Injected Messages | Yes | Yes | Yes | No |
| | | | | | Illusion | Yes | No | Yes | No |
| | Privacy | Safety & Security | Eavesdropping | | | Yes | Yes | Yes | No |
| | | | Tracking/Tracing | | | No | Yes | Yes | Yes |
| | | | | Coalition and Platooning | | Yes | Yes | Yes | No |
| | Non-repudiation | | Sybil | | Sybil | Yes | No | Yes | No |
| | | | GPS Position Faking | | GPS Position Faking | Yes | Yes | Yes | Yes |
| | Privacy | | Eavesdropping | | | Yes | Yes | Yes | No |

Table 4 illustrates the attacks on the application of VANET specific to requirements. In the table, the "Safety and Security Attacks" are highlighted in the "BLUE" colour, "Security and Infotainment Attacks" are highlighted in the "GREEN" colour, and finally the "Safety and Infotainment Attacks" are showing in "ORANGE" colour.

### 4. Pseudonym based authentication scheme

The primary requirements of privacy in VANETs are two unlikability and the secrecy of the message. Every 300ms in a V2V communication the safety-related beacons are broadcast. This may result to potential threatens the privacy of node by tracking the mobility scheme and pattern of the targeted host. This attack is carried to get sensitive information about vehicles and drivers[39]. The main purpose of the pseudonym scheme to hide the identity of a vehicle and focus on the privacy and security needs of the system[40]. Moreover, a Pseudonym is a temporary certificate given to a node to hide its real identity[40]–[45].

### 5. VANET challenges in a road network

Modeling of trustworthiness peers in road journey faces huge challenges in VANET[45]. The important challenges faced by VANET may be characterized into two conditions. Primarily, the nodes are continuously traveling in the network and are tremendously dynamic[46]–[48]. The speed of a node is on the road typically lies between 100 to 120km/h. Moreover, at this high speed on the highway to respond to an upcoming event is critical in real-time, and peers must be able to validate incoming information[49], [50]. Furthermore, it may be predictable thatthe number of nodes in the VANET can rise in any moment. For example, in metropolitan cities, all the time ten thousand nodes are present in the network and especially during rush hours it will surge dramatically to a higher number. This leads to congestions in the network which poses several issues. Moreover, the VANET is a shared channel network during rush hour peers received a lot of information from other peers in a network which results in information overload[51]. Subsequently, there is space for intelligent vehicle communication systems that address and potentially answer to hazardous conditions [52][53].

A third major challenge is to relate modeling trust in the network as it is a decentralized and open system [54]. Furthermore, the vehicle at any instance joins or leaves the VANET and there is no guarantee that in future interaction with the same node will happen. Consequently, it is not useful to depend upon the mechanism which is based on a centralized system, for instance, using Central Certificate Authority (CCA) and Trusted Third Party (TTP) or to create long term relationship depends on a social network.

## 6. A proposed trust models

This section represents, the proposed trust model. The trust is calculated based on the message received from the other nodes in the coverage area. In the presented trust model Road-side Unit (RSU) covers the coverage area. The model is hybrid by way of it calculates trustworthiness on Data (Message) and Node (Vehicles). Moreover, the trust model divided into two main parts,

1. Trust Estimation Model
2. Decision Model

### *6.1.* Trust Estimation Model

The enormous sources of data produce by VANET encourage to use of machine learning and artificial intelligence approaches to make efficient decisions. The presented trust model utilized ML algorithms to estimate the threshold value received from several parameters. These parameters are Location closeness, Data Integrity, Authentication, Time Stamp verification, and Peer Alert Message. These parameters collectively help machine learning techniques to estimate the threshold value. In the presented model to address the privacy and security requirements, a pseudonym scheme is used. This facilitates hiding the identity of a vehicle by issuing a temporary certificate to a

vehicle to hide its identity. In the TM model node will not send beacons if its process value is reduced to a given threshold.

### *6.2.* Decision Model Process

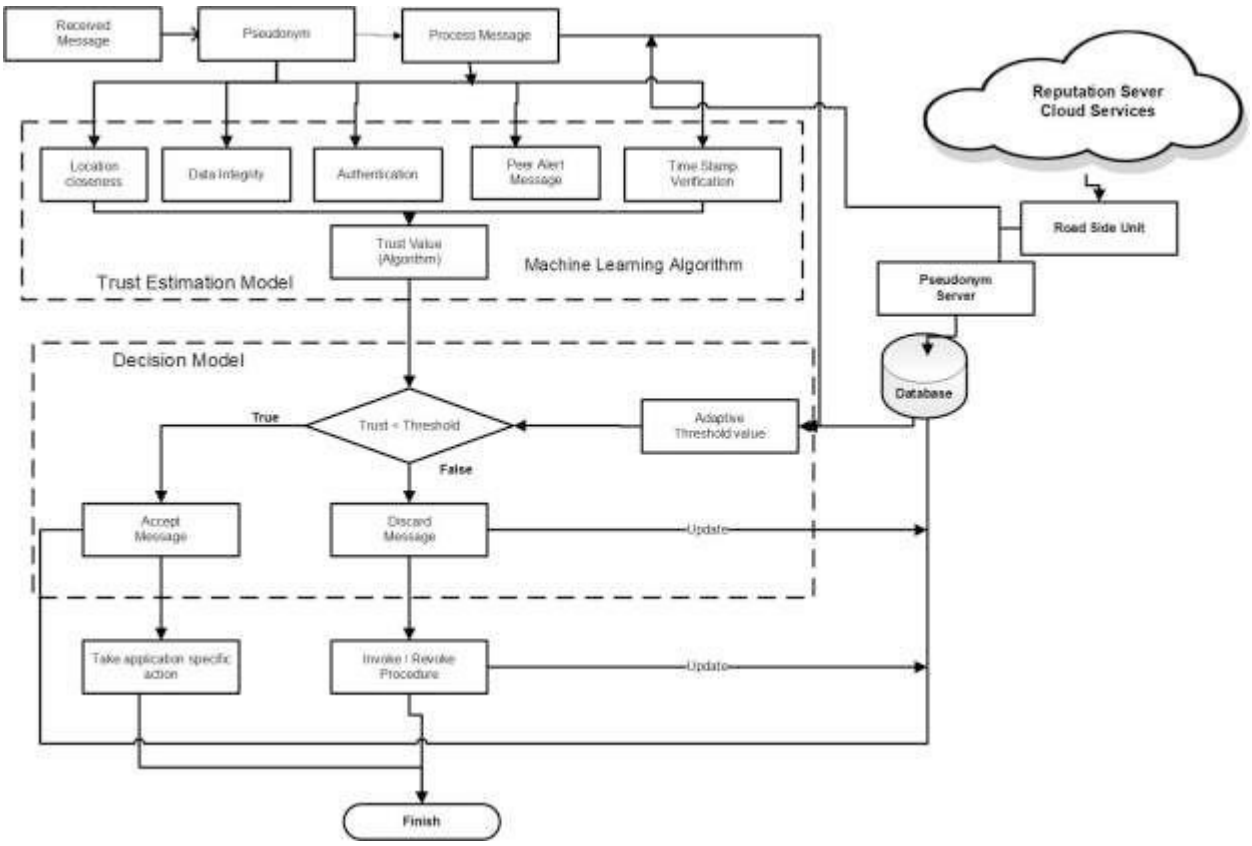
The decision model in trust calculation process threshold value that is transferred by the estimation model. The decision was taken on the based on received message threshold value whether the message is processed or discard. The two possibilities of the process are given,

Primary 1: If the "received trust value" is < less than the "threshold value" a TRUE message is created and forwarded to a database to takes an application-specific decision.

Secondary 2: If the received trust value is > greater than the threshold value a FALSE message is generated, and an update is sent to the database. FALSE generated message value procedure decides to invoke or revoke the message.

Based on cases 1 and 2 a message is forwarded to RSU and RSU triggered an alert message in the coverage area to inform about the dishonest vehicle. this triggered message enables vehicles in the coverage area not to trust the information received from the dishonest node. Figure 1 shows the presented trust model.

Fig. 1 Proposed Trust Model




- Trusted Authority (TA): is the key component of the VANET. The TA has two core responsibilities. The primary responsibility is the registration of RSUs, OBUs, and nodes. The secondary responsibility is guaranteeing security management by verifying authentication of a node, user identification, OBU identification to secure the node from attack[10].

- Roadside Units (RSU): These are installed on roads and transmitted useful information to nodes that are in the coverage area of RSU. They are linked to cloud servers employing wired or wireless technology.

- Vehicles (Nodes): Vehicles are primary components of VANET; they are fitted with the electronic device fixed on them known as the On-Board Unit (OBU). The key functions of OBU to communicate with neighboring OBU mounted on the node as well as RSU. Furthermore, the TA transmits multiple pseudonyms to registered nodes in the VANET.

- Centralized Reputation Serve (CRS): The key responsibility of CRS is assigning an initial reputation number for each registered node in the network. Furthermore, it is also responsible for managing and updating reputation.

- Pseudonyms: Pseudonyms are identities that are assigned to vehicles in the VANET and only one time used. The main use of Pseudonyms is to maintain the privacy of nodes. Central Authority(CA) periodically changing assigned pseudonyms.

## 7. Location closeness

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 using all precautions such as; time, safety, and reliability[55].

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 protect user's 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 [56].

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[8], [57]. Besides, "Replayed, Altered, and Injected Messages Attack" is another kindof 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 reduce the performance of all network applications, as well as the exchanged data trustiness.

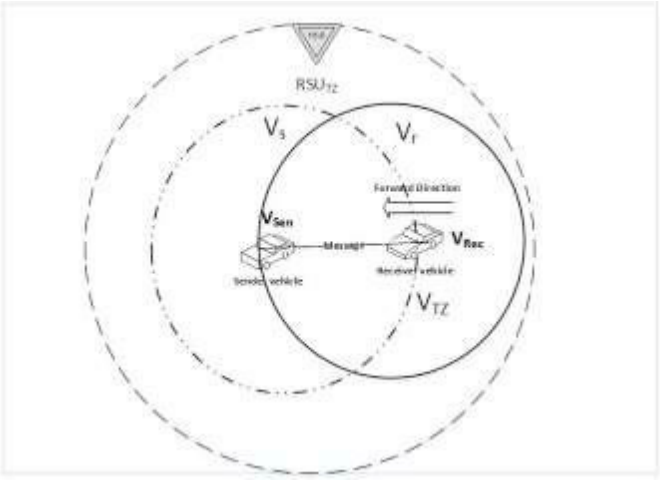
VANET encounters several security challenges and problems to deal with authentication and privacy securely[58]. Therefore, untrustworthy, or malicious vehicles increase the chances of transforming insecure information among the vehicles in VANETs. It is a fact that, in VANETs, the overall communication 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 several nodes such as RSU and vehicles. In this scenario, every node can communicate with other nodes by using short radio signals DSRC (5.9 GHz), within a 1000 meter 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[10]. We present in this paper a validation mechanism to provide location closeness in VANET. In our mechanism, we present four different approaches to calculate the location closeness.

The trusted zone comprises of Roadside 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.

Fig. 2 Location Verification Trust Zone



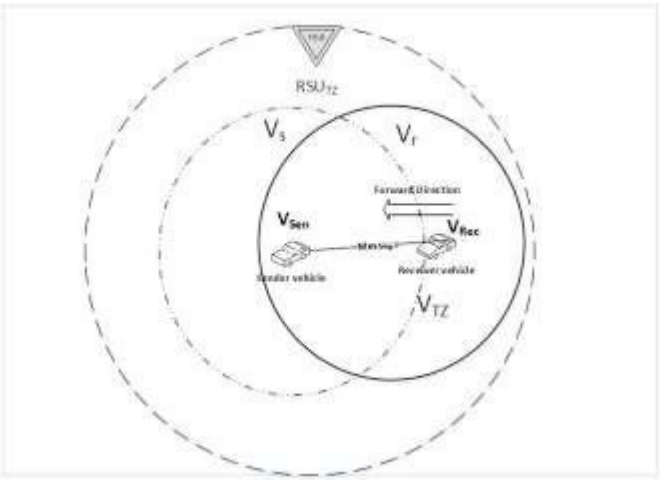

RSU_TZ In figure 2, the RSU_TZ coverage is larger in the trust zone than the coverage area of the sender and receiver vehicles V_Z (V_r, V_s).

### *7.1. Case 1*

In this case, as shown in Figure 3, the vehicle received a message from another vehicle inside the roadside unit trust zone coverage area RSU_TZ and vehicle trust coverage area V_TZ. Vehicle location closeness L_C computes as,

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

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



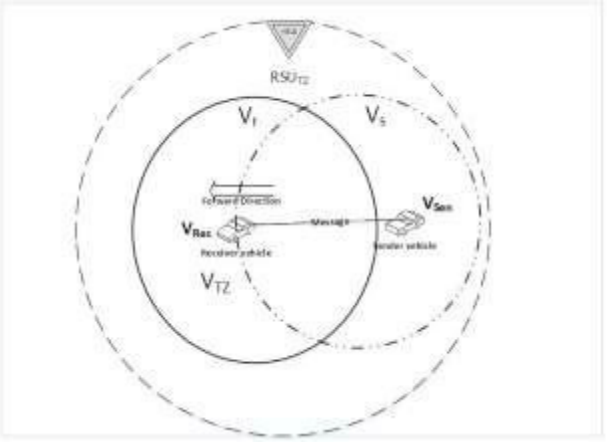
### 7.2. Case 2

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,

$$L_C = \frac{1}{3} + \frac{1}{|Send_{loc} - Recv_{loc}|} \quad if \quad V_L \in |V_Z| \; |RSU| \tag{2}$$

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

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

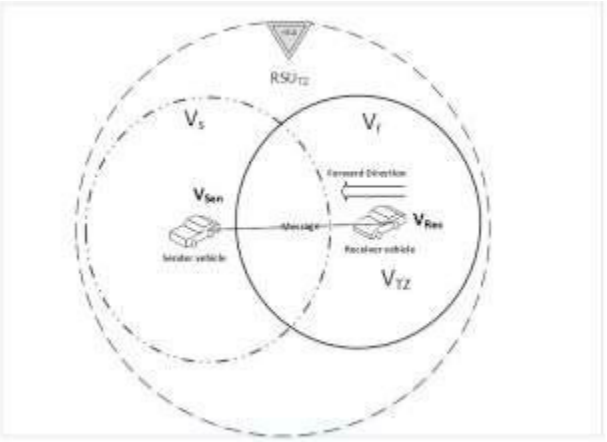



### 7.3. Case 3

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,

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

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

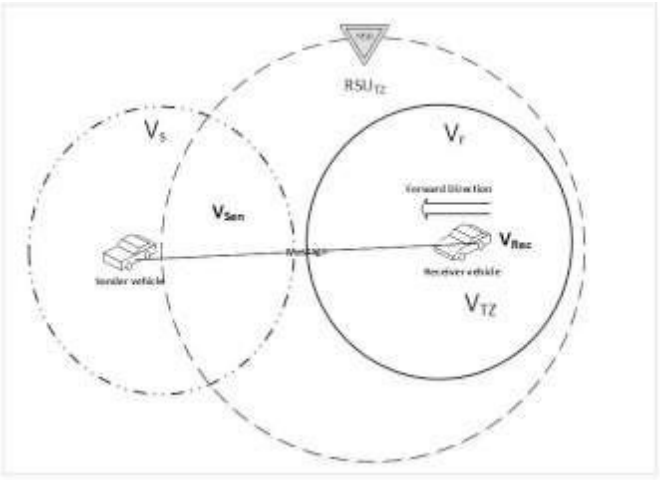


### 7.4. Case 4

In this case, as showing in Figure 6, the vehicle received a message from another vehicle that is in the coverage area of vehicle zone V_Z but outside the road site unit trust zone RSU_TZ

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

Fig. 6 The vehicle received a message from the vehicle outside of RSU_TZ and Vehicle trust zone V_TZ




### 7.5. Location Closeness Equation

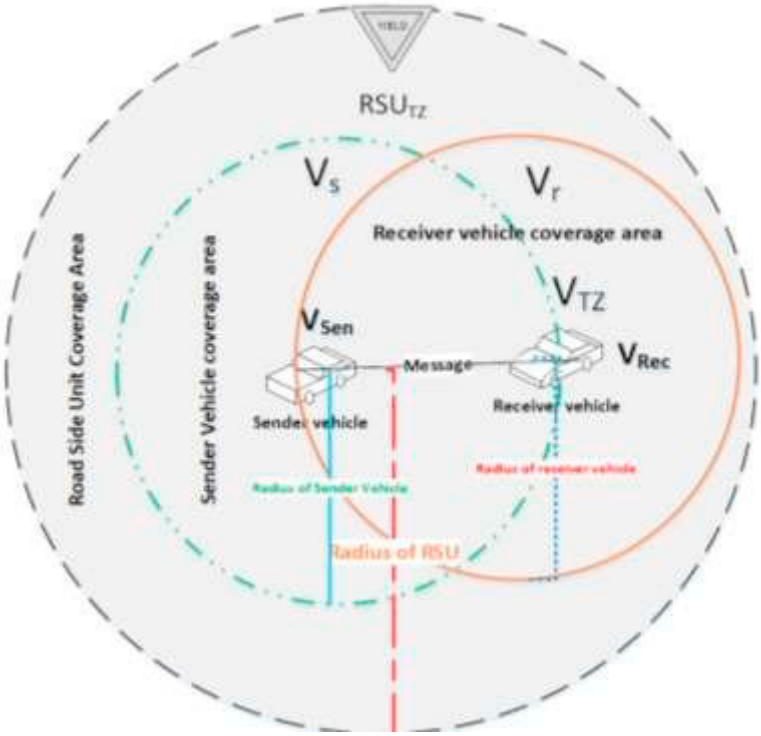
The location closeness in our scenario depends on four cases, the location closeness is calculated below:

$$L_C = \begin{cases} \frac{2}{3} + \frac{1}{|Send_{loc} - Recv_{loc}|} & if \ V_L \in |RSU_{TZ}| \cap |V_{TZ}| \\ 1 & if \ V_L \in |RSU| \setminus |V_{TZ}| \\ \frac{1}{3} + \frac{1}{|Send_{loc} - Recv_{loc}|} & if \ V_L \in |V_Z| \setminus |RSU| \\ 0 & if \ V_L \notin |V_{TZ}| \setminus |RSU_{TZ}| \end{cases} \tag{5}$$

Equation 5 described that the vehicle(node) received a message from several sources and based on received information in a message calculate $L_C$ to trust the message or discard it.

In the presented method, four different cases to compute location closeness as shown in Figure 7, show the distance between the sender and RSU , distance between the two nodes, and location closeness based on $L_C$. In the presented scenario, we presume the coverage area of RSU is (50, 50) while the radius is 25.

Fig 7 distance between the two nodes, the distance between the sender and RSU, and location closeness on the basis of L_C




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 based on L_C. Here in our scenario, we assume the coverage area of RSU is (50, 50) whereas the radius is 25.

Fig. 8 Location Closeness case 1, 2, 3 and 4

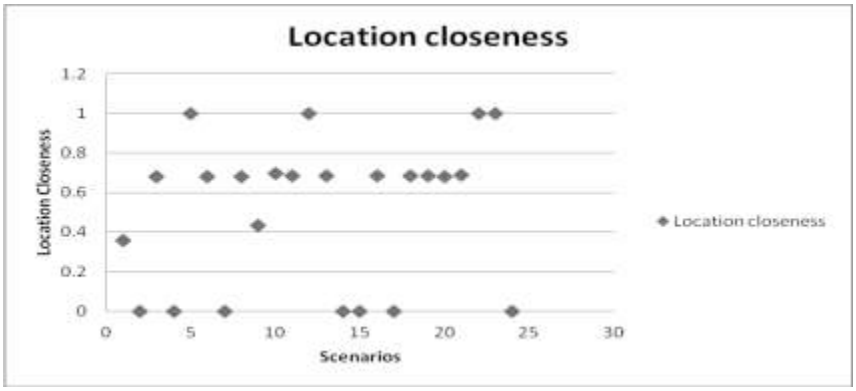



Figure 8 shows the location closeness in the case of V2V. Remarkable results to emerge from the graph are that values above 0.5 are trusted. Case 1 and 2 of location closeness in our scenario shows the vehicle-to-vehicle communication is in the trusted range of RSU and vehicle zones. The case shows threshold values between 0 to 0.5 and here we assume the value may be trusted and may not be. So the value is forwarded to the trust decision model. The value 0 is not a trusted value as the V2V is out of trusted zones of RSU and vehicle trust zone.

## 8. Conclusion

A vehicular ad hoc network (VANETs) is a network of connected wireless nodes like vehicles, buses, signals, RSU, and other road infrastructure devices that are participating in safer road transportation. The security, safety and privacy threats faced by VANETs consist of availability, authentication, confidentiality, integrity, privacy, Non – repudiation, and others. The security threats of VANETs could be addressed comprehensively by using machine learning and AI. In this paper, a comparison of trust and cryptography was presented based on applications and security requirements of VANET. Furthermore, A trust model design is presented based on five parameters. The privacy of the vehicle is an address by using the Pseudonym technique. In the future, the presented model will test inthe presence of a dishonest node.

## References


[1] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of Artificial Intelligence and Machine learning in smart cities," *Comput. Commun.*, 2020.

[2] P. Matta and B. Pant, "Internet of things: Genesis, challenges and applications," *J. Eng. Sci. Technol.*, vol. 14, no. 3, pp. 1717–1750, 2019.

[3] S. Aheleroff *et al.*, "IoT-enabled smart appliances under industry 4.0: A case study," *Adv. Eng. Informatics*, vol. 43, p. 101043, 2020.

[4] M. A. Rahim, M. A. Rahman, M. M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, "Evolution of IoT-enabled connectivity and applications in automotive industry: A review," *Veh. Commun.*, p. 100285, 2020.

[5] M. Won, "Intelligent traffic monitoring systems for vehicle classification: A survey," *IEEE Access*, vol. 8, pp. 73340–73358, 2020.

[6] A. K. Haghighat, V. Ravichandra-Mouli, P. Chakraborty, Y. Esfandiari, S. Arabi, and A. Sharma, "Applications of Deep Learning in Intelligent Transportation Systems," *J. Big Data Anal. Transp.*, pp. 1–31, 2020.

[7] K. Nk, K. Jain, and T. K. Bansal, "Privacy Preserving Security VANET Framework for Intelligent Transport Systems," *Available SSRN 3648099*, 2020.

[8] 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.

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

[10] M. H. Junejo *et al.*, "A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks," *Sci. Program.*, vol. 2020.

[11] 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.

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

[13] 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.

[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] A. Ghosh, T. Chatterjee, S. Samanta, J. Aich, and S. Roy, "Distracted driving: A novel approach towards accident prevention," *Adv. Comput. Sci. Technol*, vol. 10, no. 8, pp. 2693–2705, 2017.

[17] G. Fusco, C. Colombaroni, L. Comelli, and N. Isaenko, "Short-term traffic predictions on large urban traffic networks: Applications of network-based machine learning models and dynamic traffic assignment models," in *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, 2015, pp. 93–101.

[18] S. Devi and T. Neetha, "Machine Learning based traffic congestion prediction in a IoT based Smart City," *Int. Res. J. Eng. Technol*, vol. 4, pp. 3442–3445, 2017.

[19] Y. Hou, P. Edara, and C. Sun, "Traffic flow forecasting for urban work zones," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1761–1770, 2014.

[20] A. Kulkarni, N. Mhalgi, S. Gurnani, and N. Giri, "Pothole detection system using machine learning on Android," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 4, no. 7, pp. 360–364, 2014.

[21] M. Munoz-Organero, R. Ruiz-Blaquez, and L. Sánchez-Fernández, "Automatic detection of traffic lights, street crossings and urban roundabouts combining outlier detection and deep learning classification techniques based on GPS traces while driving," *Comput. Environ. Urban Syst.*, vol. 68, pp. 1–8, 2018.

[22] M. Ozbayoglu, G. Kucukayan, and E. Dogdu, "A real-time autonomous highway accident detection model based on big data processing and computational intelligence," in *2016 IEEE International Conference on Big Data (Big Data)*, 2016, pp. 1807–1813.

[23] J. R. Ng, J. S. Wong, V. T. Goh, W. J. Yap, T. T. V. Yap, and H. Ng, "Identification of road surface conditions using IoT sensors and machine learning," in *Computational Science and Technology*, Springer, 2019, pp. 259–268.

*[24]* M. Ghadge, D. Pandey, and D. Kalbande, "Machine learning approach for predicting bumps on road," in *2015 International Conference*

*on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 2015, pp. 481–485.
[25] N. Dogru and A. Subasi, "Traffic accident detection using random forest classifier," in *2018 15th learning and technology conference (L&T)*, 2018, pp. 40–45.
[26] Y. Wu, F. Meng, G. Wang, and P. Yi, "A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks," in *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*, 2015, pp. 1–7.
[27] P. R. L. De Almeida, L. S. Oliveira, A. S. Britto Jr, E. J. Silva Jr, and A. L. Koerich, "PKLot–A robust dataset for parking lot classification," *Expert Syst. Appl.*, vol. 42, no. 11, pp. 4937–4949, 2015.
[28] D. Kwon, S. Park, S. Baek, R. K. Malaiya, G. Yoon, and J.-T. Ryu, "A study on development of the blind spot detection system for the IoT-based smart connected car," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1–4.
[29] G. Amato, F. Carrara, F. Falchi, C. Gennaro, C. Meghini, and C. Vairo, "Deep learning for decentralized parking lot occupancy detection," *Expert Syst. Appl.*, vol. 72, pp. 327–334, 2017.
[30] K. Gopalakrishnan, "Deep learning in data-driven pavement image analysis and automated distress detection: A review," *Data*, vol. 3, no. 3, p. 28, 2018.
[31] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: a lightweight self-organized trust model in VANETs," *Mob. Inf. Syst.*, vol. 2016, 2016.
[32] A. Yang, J. Weng, N. Cheng, J. Ni, X. Lin, and X. Shen, "DeQoS Attack: Degrading Quality of Service in VANETs and its Mitigation," *IEEE Trans. Veh. Technol.*, 2019.
[33] J. Ba, V. Mnih, and K. Kavukcuoglu, "Multiple object recognition with visual attention," *arXiv Prepr. arXiv1412.7755*, 2014.
[34] B. Ryder and F. Wortmann, "Autonomously detecting and classifying traffic accident hotspots," in *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*, 2017, pp. 365–370.
[35] K. S. Sang, B. Zhou, P. Yang, and Z. Yang, "Study of group route optimization for IoT enabled urban transportation network," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2017, pp. 888–893.
[36] Y. Lv, Y. Duan, W. Kang, Z. Li, and F.-Y. Wang, "Traffic flow prediction with big data: a deep learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 865–873, 2014.
[37] H. Kanoh, T. Furukawa, S. Tsukahara, K. Hara, H. Nishi, and H. Kurokawa, "Short-term traffic prediction using fuzzy c-means and cellular automata in a wide-area road network," in *Proceedings. 2005 IEEE Intelligent Transportation Systems, 2005.*, 2005, pp. 381–385.
[38] M. A. Al Mamun, J. A. Puspo, and A. K. Das, "An intelligent smartphone based approach using IoT for ensuring safe driving," in *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, 2017, pp. 217–223.
[39] J. M. De Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in *Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts*, IGI global, 2011, pp. 894–911.
[40] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surv. tutorials*, vol. 17, no. 1, pp. 228–255, 2014.
[41] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *2009 IEEE Vehicular Networking Conference (VNC)*, 2009, pp. 1–8.
[42] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 37, pp. 122–132, 2016.
[43] S. Wang and N. Yao, "A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs," *Wirel. Networks*, vol. 25, no. 3, pp. 1099–1115, 2019.
[44] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, 2011.
[45] I. Memon and H. T. Mirza, "MADPTM: Mix zones and dynamic pseudonym trust management system for location privacy," *Int. J. Commun. Syst.*, vol. 31, no. 17, p. e3795, 2018.
[46] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, and V. Odelu, "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Secur. Commun. Networks*, vol. 9, no. 17, pp. 4255–4271, 2016.
[47] A. Agrawal, A. Garg, N. Chaudhiri, S. Gupta, D. Pandey, and T. Roy, "Security on vehicular ad hoc networks (vanet): A review paper," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 1, pp. 231–235, 2013.
[48] P. Fabian, A. Rachedi, and C. Guéguen, "Programmable objective function for data transportation in the Internet of Vehicles," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 5, p. e3882, 2020.
[49] 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.
[50] R. A. Shaikh and A. S. Alzahrani, "Trust management method for vehicular ad hoc networks," in *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, 2013, pp. 801–815.
[51] W. Li, W. Song, Q. Lu, and C. Yue, "Reliable congestion control mechanism for safety applications in urban VANETs," *Ad Hoc Networks*, vol. 98, p. 102033, 2020.
[52] I. Memon, "A secure and efficient communication scheme with authenticated key establishment protocol for road networks," *Wirel. Pers. Commun.*, vol. 85, no. 3, pp. 1167–1191, 2015.
[53] I. Memon and Q. A. Arain, "Dynamic path privacy protection framework for continuous query service over road networks," *World Wide Web*, vol. 20, no. 4, pp. 639–672, 2017.
[54] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs," *IEEE Trans. Emerg. Top. Comput.*, 2020.

[55] U. Ihsan, S. Yan, and R. Malaney, "Location Verification for Emerging Wireless Vehicular Networks," *IEEE Internet Things J.*, 2019.
[56] M. S. Sheikh and J. Liang, "A Comprehensive Survey on VANET Security Services in Traffic Management System," *Wirel. Commun. Mob. Comput.*, vol. 2019, 2019.
[57] 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.
[58] 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.