Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.778235

AN EFFICIENT SECURED TRUST BASED APPROACH FOR VEHICULAR AD HOC NETWORK ROUTING

[1]Mrs. T. Lumina, [2]Ms. A. Lakshmi, [3]Mrs. V. Pavithra
[1]Assistant Professor, PG Department of Computer Science, Kathir College of Arts & Science, Neelambur.
[2]Assistant Professor, PG Department of Computer Science, Kathir College of Arts & Science, Neelambur.
[3]Assistant Professor, PG Department of Computer Science, Kathir College of Arts & Science, Neelambur.

Abstract - Vehicular Ad-hoc NETworks (VANETs) is a modern technology which help a vehicle and a driver in several ways. The main characteristics of VANETs are nodes i.e. vehicles with relatively high mobility and constantly changing topology. In case of data communication in VANETs, a source node must depend on the intermediate nodes to send its data packets to the destination node on multi-hop routes. VANETs can give better perfor¬mance if all its nodes work properly with full cooperation during the communication. In VANETs, a node can generate and broadcast important and essential messages to other nodes in the network for safety reason. However, the generated mes¬sage by a vehicle may not be reliable every time. In this situation, we have proposed a trusted and secured routing technique that evaluates the trust of a vehicle and also checks the message reliability. The proposed protocol is named as Secure Ad-hoc On Demand Distance Vector (SAODV) routing protocol which is the modification of Ad-hoc On-demand Distance Vector routing protocol. Since VANETs are mostly attacked by the malicious nodes; therefore better security solu¬tion is needed to stop such attacks. The proposed work introduces a trust model to establish a malicious node free route for source node to send its data packets to the destination node on multi-hop routes. In VANETs, a malicious node can broadcast false messages and can divert other vehi¬cles in wrong direction. Therefore, to stop such activities an effective trust management scheme is required for VANETs. The proposed work, addressed the above mentioned problem of selection of reliable or trusty vehicles i.e. to establish a malicious node free route by proposing a trust based model for VANETs. The proposed approach evaluated the reliability and trustworthiness of the message or the vehicle based on the trust metrics of that message or the vehicle.

Keywords: - Cloud Computing, Searchable Encryption, Decryption, ECC, Cloud Storage, and Cloud Server.

1 INTRODUCTION

Because of growing demand for higher capacity and higher data rates to accommodate data-intensive multimedia coupled with real-time services, wireless networks such as sensor networks, ad hoc mobile networks, cellular networks and satellite networks have experienced a explosive growth over the past few years. In ad hoc network, the mobile node, act as router exchange the information without any fixed base station [6]. The mobile nodes steer dynamically to form their own network. The development of ITS (Intelligent Transportation

System), to improve road safety and disseminate the emergency information in network, automobile industry triggered the researchers in the field of VANET. Two types of communication Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) are supported by VANET using the IEEE standard 802.11p.VANET is the sub-class of MANET here the nodes are mobile vehicles. There is a high possibility for the vehicles to mobile anywhere because of its natural characteristics. Because of high mobility there is a high chance for frequent link disconnection and it cannot provide reliable data transfer [1]. Due to the sparse connectivity, intermittent connectivity, high mobility and latency, long delay, high error rates data communication get interrupted between the vehicles, that can be handled and communication takes place between the vehicles by using the delay/disruption tolerant network (DTN).In this networks vehicles carries the data until it identifies the appropriate node to deliver or forward the data via the node. This is called as store-carry and forward mechanism [10]. Vehicle DTN supports for many applications like emergency information broadcasting, advertisements, displaying the vehicle parking slot availability etc. Opportunistic routing and VADD are the two routing algorithms used in VANET DTN. A node carries the data until it meets the trusted intermediate node or the destination node in its coverage range.

In vehicular ad-hoc Networks (VANETs) nodes are moving cars. Thus, every moving car is required to function as a router. As a result a wide range network can be created since cars which are 100 to 300 m apart are able to communicate with each other. Since VANETs are sub category of MANETs it shares some of its characteristics and has special properties or characteristics that distinguish VANETs from other types of networks [16]. In this section we discuss VANET properties in order to clarify why VANETs were given a special category.

Like MANETs, VANETs are self-configuring and distributed Networks consisting of moving vehicles. Apart from these characteristics VANETs retain a number of distinguishing characteristics [13].

- **Very Dynamic Topology**

  The topology always changes because vehicles are moving at high speeds. For example, the average speed of vehicles on high ways is between 60 and 70 mph. Thus, a link established between two vehicles will be broken after almost 10 sec if the radio between the vehicles is 125 m. Therefore algorithms developed for VANETs must be capable of adapting to highly mobile nodes. In other words, theses algorithms must be capable of applying connection maintenance, frequent changes in neighborhood and high speed mobility since vehicles cannot stay in the range of an existing infrastructure for more than 10 to 20 sec.

- **Patterned Mobility**

  A specific mobility model is used by vehicles which can be affected by roads traffic lights, speed limits, and traffic conditions and drivers behaviors. Therefore the evaluation of routing protocols is affected by the mobility pattern used and the traces obtained from the pattern. Several mobility trace generators were developed in order to simulate and test VANET routing protocols

- **Frequently Disconnected Network**

  In frequently disconnected network, the link between two vehicles disappears quickly due to the highly dynamic topology. Also varying node density. As a result, robust routing

protocols are required in order to be able to adapt and react to frequent changes in topology and connectivity.

- **Unlimited Battery Power and Storage**

  Unlike nodes in sensor networks, nodes in VANETs have unlimited energy and storage. Therefore, energy consumption, power consumed in computing and duty cycle optimization is not as important to VANETs as in sensor networks.

Various applications have been developed for VANETs such as safety applications, commercial applications and convenience applications. These applications aim to provide solutions for real life issues or scenarios namely; lack of connectivity, fast communication, safety and infotainment [12]. Worth mentioning, different network models or architectures are adopted by the applications in order to achieve their goals

As follows, the research paper is structured. The associated work is addressed in section 2. For the proposed approach phases are described in a short note on the stairs is explained in section 3. The experimental findings and comparisons are discussed in section 4. Finally, in section 5, the concluding remarks are illustrated.

2. RELATED WORK

Much research has been done in the field of routing and security for trust based VANETs. Currently, researches on trust in VANETs can be classified into three directions: they are entity-centric trust, data-centric trust and combined trust. In addition, for the sake of evaluating trust objectively, researchers also do some work on trust metric [14]. Many researchers are conducting extensive studies on the protection of the security of VANETs. This is discussed in this section.

Xia, H., et al. (2019) [4] study the study trust properties and construct a novel trust inference model, where two trust attributes named subjective trust and recommendation trust, are selected to quantify the trust level of a specific vehicle. The SCGM (1, 1)-weighted Markov prediction algorithm based on fluctuation recognition is utilized to calculate the subjective trust accurately, meanwhile a new evaluation method of recommendation credibility based on the feedback mechanism is introduced for the calculation of recommendation trust and and design a light-weight trust-aware multicast routing protocol (i.e., LTMRP), which can establish secure and reliable communication paths by selecting trusted relay vehicles. To further improve the routing efficiency, two mechanisms including forwarding nodes reuse mechanism and trust-aware route handoff mechanism are proposed.

Sugumar, R., et al. (2016) [5] proposed to fulfil the security requirements like message privacy, integrity, and authentication. The authentication technique is said to be efficient if it detects compromised nodes accurately with less complexity, reduced authentication delay, and keying overhead. In the proposed work, a trust-based authentication scheme for cluster-based VANETs is proposed. The vehicles are clustered, and the trust degree of each node is estimated. The trust degree is a combination of direct trust degree and indirect trust degree. Based on this estimated trust degree, cluster heads are selected. Then, each vehicle is monitored by a set of verifiers, and the messages are digitally signed by the sender and encrypted using a public/ private key as distributed by a trusted authority and decrypted by the destination. This verifies the identity of sender as well as receiver thus providing authentication to the scheme.

Tripathi, K. N., & Sharma, S. C. (2019) [7] proposed a trust based model to detect rogue nodes in a vehicular network. Vehicular ad-hoc network (VANET), a part of the intelligence transportation system is the network created by vehicles. Security is the main issue in vehicular ad-hoc network. Many intruders try to use the vulnerability presents in the vehicular network. In VANET communication between two nodes, may involves multiple intermediate nodes to forward the data due to low transmission range. The intermediate nodes must be trustworthy enough to be a part of the communication process. Rogue or malicious nodes can accept the data and drop the data in between source to destination. The proposed model first estimates the trust value of the nodes and based on that identifies the rogue nodes in the network. We select only trustworthy nodes to relay the data in the routing process. The simulation result shows that the proposed model enhances network performance significantly.

Zhang, D., et al. (2018) [8] proposed a software- defined trust based deep reinforcement learning framework (TDRL-RP), deploying a deep Q-learning algorithm into a logically centralized controller of software-defined networking (SDN). Vehicular ad hoc networks (VANETs) have become a promising technology in smart transportation systems with rising interest of expedient, safe, and high- efficient transportation. Dynamicity and infrastructure-less of VANETs make it vulnerable to malicious nodes and result in performance degradation. Specifically, the SDN controller is used as an agent to learn the highest routing path trust value of a VANET environment by convolution neural network, where the trust model is designed to evaluate neighbors' behaviour of forwarding packets. Simulation results are presented to show the effectiveness of the proposed TDRL-RP framework

Li, W., & Song, H. (2015) [9] introduces an attack-resistant trust management scheme (ART) for VANETs that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. The trustworthiness of VANETs could be improved by addressing holistically both data trust, which is defined as the assessment of whether or not and to what extent the reported traffic data are trustworthy, and node trust, which is defined as how trustworthy the nodes in VANETs are. Specially, data trust is evaluated based on the data sensed and collected from multiple vehicles; node trust is assessed in two dimensions, i.e., functional trust and recommendation trust, which indicate how likely a node can fulfil its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively. The proposed trust management theme is applicable to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness.

In comparison to most of these works, should discuss briefly about published matter that technically relates to your proposed work. A short summary of what you can include in the Related Works section: Work that proposes a different method to solve the same problem.

3. THE PROPOSED SCHEME

According to [1], the applications in VANETs are categorized into safety and non-safety applications. The basis of these applications is the exchange of data among entities. Therefore, due to the lack of centralized services as well as the open, distributed, and dynamic nature of VANETs [2], many attacks like denial of service, message suppression, and propagation of false message can affect the performance of applications. Security is one of the

main issues in VANETs, and trust is a key element of security [3]. Hence, since VANETs are based upon data exchange among vehicles, trustworthiness of data is of great importance. In addition, data communication between trusted vehicles directly affects.

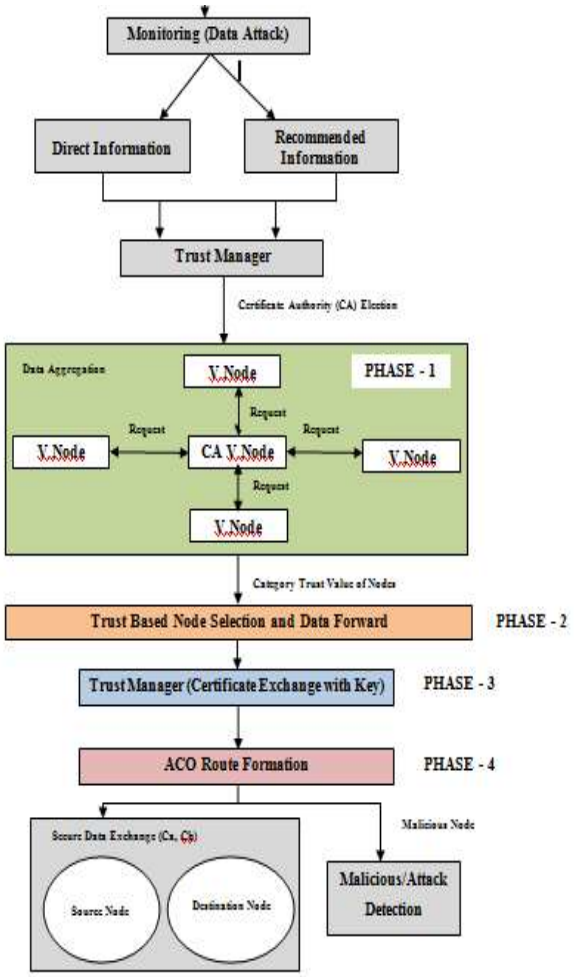

Figure 1: - Structure of Proposed Work

Moreover, the quality of safety/non-safety applications in VANETs largely depends upon the trustworthiness of data [10], and trust plays a vital role in the security and quality of a vehicular network. Thereby, comprehensive studies on trust and reviewing existing trust models are necessary. However, the lack of a review on trust in VANETs to sum up the best available research on specific questions is sensible, which must be done by synthesizing the results of existing studies [15].

Trust is the belief that someone or something is reliable, honest etc. The meaning of trust varies with different context. In networks trust is the important part of relationship among nodes. In our trust model, Trust Initiator is the node that is evaluating the trust [18]. Trusty refers to the node whose trust is being evaluated. Recommenders are the expectation of the Trust Initiator nodes those can give honest and unbiased recommendation on a specific Trusty.

In this work, we propose a trust-based model and evaluation framework to support the effective evaluation of information sent by peers and the immediate control of false information in a VANET.

Phase 1: - Data Aggregation

In our trust evaluation model TVAODV, the trust evaluation is performed by each node locally. The trust information table must be maintained by each node and the table may contain the information about trusty node's ID, Direct Trust Value, Recommendation trust Value and Combined trust value. The trust information may be refreshed periodically. The information will be expired if it is not refreshed within the period of time t as assumed by the network and the corresponding trust value will become Zero i.e. the initial value.

Phase 2: - Trust Based Node Selection

If a source node or monitored node gets both direct trust and recommendation trust of the trusty node then it will evaluates the trust value. Based on the trust value the intermediate nodes are selected and these nodes are used to establish the communication between the source and destination.

Phase 3: - Certificate based Security Model

Security is the main concern of any other network because of if attacks apply in networks than users suffer and quality of service is down when we talk about VANET which is highly moveable or infrastructure of VANET change frequently in this network security is main concern because if it's flexible and secure passengers feel convenient to travel. Trust is the most important area, to build trust between vehicles we apply behavior based technique. Hashing is used for encryption and decryption, hashing is not secure technique because of its keys easily hacked by hackers. Overcome this problem we gave RSU based centralized and AES based security technique.

Phase 4: - Route Discovery using ACO

Route discovery process starts if a source node needs a valid route to some destination nodes. The source node will sense its entire neighbor and take those are having the evaluated Trust Decision (TD) value satisfied the trust requirements. Source node will then broadcast the Route REQuest (RREQ) packet to all such neighbors. The neighboring nodes also does the same process to broadcast its RREQ packet to their neighbor and so on until the destination node reached or an intermediate node with afresh enough route plus TD with satisfied trust requirement to reach the destination node is found. This route formation is done using Ant Colony Optimization (ACO) Algorithm. This algorithm is used to find the shortest path between the source and destination like the ants are found the food in shortest way.

4. PERFORMANCE EVALUATION

Development of an appropriate trust model requires a set of characteristics and parameters that should be taken into account when designing. These parameters are based on the challenges in a VANET environment. In [11], several parameters as requirements of a trust model have been identified. They mentioned that a suitable trust model should be accurate, scalable, simple and fast, resilient to security and privacy threats, and independent of mobility patterns.

In order to evaluate the performance of the comparative algorithms, it is essential to define the parameters for which the algorithms must be tested. Since the security features of each algorithm as their strength against different attacks are already known. The selected performance factor here is the performance of the proposed work [17]. In this study, to perform qualitative comparison, have selected the following parameters as the trust model's requirements.

Table 4.1: - Parameters for the rescue operation scenario

Parameters	Values
Mobility model	RPGM
Distribution of nodes	5 in each group 10 groups
Simulation Area	1000 * 1000 m
Probability of group change	0.05
Maximum distance to group center	100 m
Node speed	Max speed: 2 m/s Min speed : 1 m/s

This scenario represents groups of workers operating in a relatively small area. For example, in an avalanche rescue operation we may have set of nodes communicating within a small area. We consider a relatively denser set of nodes than the battlefield scenario. The nodes have lesser probability of changing a group (0.05) as compared to the battlefield scenario. The parameters defined for this scenario are shown in table 4.1.

4.1. Packet Delivery fraction (PDF)

It is found that for the battlefield scenario, ACO outperforms both ART and TDRL-RP protocols in terms of packet delivery fraction for pause times of 100-400 sec as shown in figure 4.1. For higher pause times (greater than 500 sec), all the three protocols converge to give a PDF of almost 100% because the nodes are almost static and hence the congestion in the network decreases.

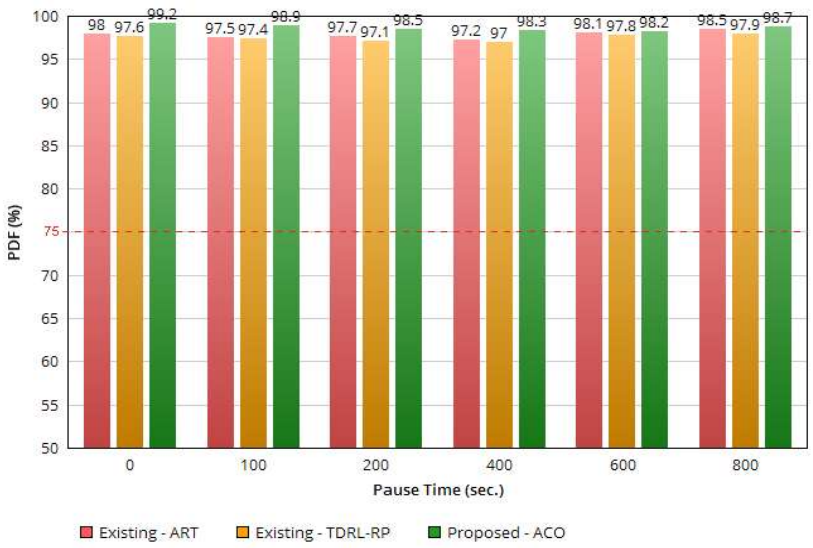

Fig. 4.1: - Analysis of PDF

4.2. End-to-End Delay

Now the impact on the most important metric, the average end to end delay is studied. As shown in figures 4.2, exhibits a lower delay than ART & TDRL-RP.

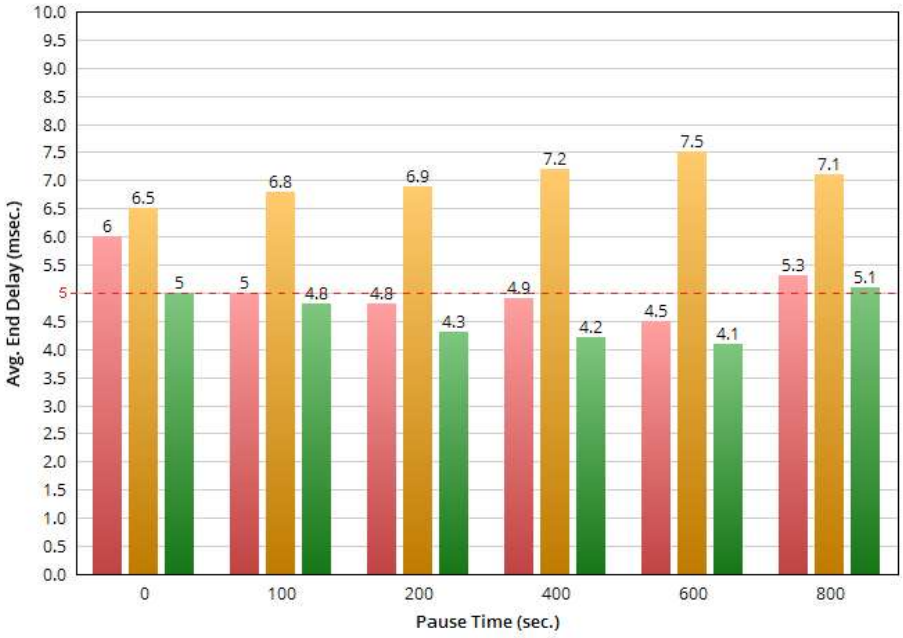

Fig.4.2: - Analysis of End-to-End Delay

ACO exhibits a lower delay than ART and TDRL-RP across all the three scenarios as seen from the graphs, which bolsters the fact that a reactive protocol tends to be faster than the proactive protocols under varying loads

The above results state clearly that the proposed ACO algorithm achieves better performance in the VANET environment. The simulation results presented had shown that ACO has a better performance than the existing ART and TDRL-RP algorithms used. Since ACO does not have any known security vulnerabilities so far, this makes it an excellent candidate to be considered a standard encryption algorithm.

5. CONCLUSION

The trust model enables vehicles to distinguish trustworthy vehicles or messages from untrustworthy ones. It leads to reducing the risk of vehicles being misguided by other malicious vehicles. Due to the importance of data and its quality in VANETs as well as the impact of trustworthiness on the quality of applications, this study has conducted a systematic review of current research that aim at managing trust in vehicular *ad hoc* networks. To concluded that none of the proposed trust models have achieved all the desired properties. Therefore, we developed a framework including probability module, plausibility module, trust measurement module, and decision making module.

6. REFERENCES

[1] Yin, J., ElBatt, T., Yeung, G., Ryu, B., Habermas, S., Krishnan, H., & Talty, T. (2004, October). Performance evaluation of safety applications over DSRC vehicular ad hoc networks. In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks (pp. 1-9).

[2] Yan, G., Olariu, S., & Weigle, M. C. (2008). Providing VANET security through active position detection. Computer communications, 31(12), 2883-2897.

[3] Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. Journal of computer security, 15(1), 39-68.

[4] Xia, H., Zhang, S. S., Li, Y., Pan, Z. K., Peng, X., & Cheng, X. Z. (2019). An attack-resistant trust inference model for securing routing in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 68(7), 7108-7120.

[5] Sugumar, R., Rengarajan, A., & Jayakumar, C. (2018). Trust based authentication technique for cluster based vehicular ad hoc networks (VANET). Wireless Networks, 24(2), 373-382.

[6] Zhang, D., Yu, F. R., Wei, Z., & Boukerche, A. (2016). Trust-based secure routing in software-defined vehicular ad hoc networks. arXiv preprint arXiv:1611.04012.

[7] Tripathi, K. N., & Sharma, S. C. (2019). A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS). International Journal of System Assurance Engineering and Management, 1-15.

[8] Zhang, D., Yu, F. R., & Yang, R. (2018, December). A machine learning approach for software-defined vehicular ad hoc networks with trust management. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[9] Li, W., & Song, H. (2015). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE transactions on intelligent transportation systems, 17(4), 960-969.

[10] Gurung, S., Lin, D., Squicciarini, A., & Bertino, E. (2013, June). Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In International conference on network and system security (pp. 94-108). Springer, Berlin, Heidelberg.

[11] Mármol, F. G., & Pérez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of network and computer applications, 35(3), 934-941.

[12] Tan, S., Li, X., & Dong, Q. (2015). Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Networks, 30, 84-98.

[13] Lim, K., & Manivannan, D. (2016). An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. Vehicular Communications, 4, 30-37.

[14] Mehdi, M. M., Raza, I., & Hussain, S. A. (2017). A game theory based trust model for Vehicular Ad hoc Networks (VANETs). Computer Networks, 121, 152-172.

[15] Gazdar, T., Benslimane, A., Rachedi, A., & Belghith, A. (2012, June). A trust-based architecture for managing certificates in vehicular ad hoc networks. In 2012 International Conference on Communications and Information Technology (ICCIT) (pp. 180-185). IEEE.

[16] Oubabas, S., Aoudjit, R., Rodrigues, J. J., & Talbi, S. (2018). Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme. Vehicular Communications, 13, 128-138.

[17] Fan, N., & Wu, C. Q. (2019). On trust models for communication security in vehicular ad-hoc networks. Ad Hoc Networks, 90, 101740.