Trust Management Evaluation in Vehicular Ad-hoc Networks(VANET)

Saeed Jafari, Master Student of Electrical Engineering (Cryptography and Security)

***Abstract*—The development of communication technologies and information processing have persuaded the developers of the transportation systems to use the capacities of communication technology in vehicles and monitoring units of this system. There is a growing trend toward using artificial intelligence (AI) in the transportation system to address human errors. Vehicular Ad-hoc Network (VANET) is one of the communication technologies used in the intelligent transportation system. However, if either the communication channels do not provide the desired functionality or attackers interfere in this system, this can cause condensible road hazards and risk people life. Therefore, designers of the VANET must guarantee the correct operation of the network in the event of a technical failure or an attack.**
Given the potential peril, it is necessary to design a model to calculate the value of trust of nodes to each other and the value of trust of nodes to the received message. In this article, we review and analyze five approaches to build and manage trust in VANET. Finally, we provide a quantitative comparison of these approaches.

***Index Terms*—Connected Vehicles, Trust Management, Trust Model, Smart Cities, Vehicular Ad-hoc network (VANET).**

I. Introduction

Using the fastest and safest vehicles has always been one of the challenges of human life. The growth rate of 200,000 road casualties from 2000 to 2018 doubles the need for addressing the security of the transportation system. Various connections have been defined between the components of the transportation system, which can be classified into four categories: vehicle-to-vehicle communication(V2V), vehicle-to-pedestrian communication(V2P), vehicle-to-grid(V2G), and vehicle-to-infrastructure(V2I). Vehicular connectivity is installed in the transportation system to cover the driver's blind spots while driving, prevent collisions, control traffic congestion,... . However, if the communication channels do not provide the desired function or attackers can interfere in this system, they can potentially create road hazards and damage to humans. Therefore, designers of the VANET must guarantee the correct operation of the network in the event of a technical failure or attack.

In VANET, malicious nodes may subconsciously or consciously send the wrong message in the network and endanger human life. Also, some nodes may report no message at all, which decreases drives trust. Therefore, designing a model to kick out malicious nodes from the network is necessary.
Most studies in this field have focused on sending and delivering messages reliably on VANET, and measuring the validity of message content is out of attention. In addition, authentication methods do not address this issue because high mobility, rapidly changing network topology, limited bandwidth and processing power available, and privacy of vehicles in these networks make authentication costly. In VANET, a mechanism has been established to determine the validity of the content of the received messages and to calculate the probability that VANET nodes are truthful. This mechanism called trust management defects false messages to increase the security of VANET. Cryptographic-based methods do not have the capabilities to deal with internal attackers, so if one of the trusted nodes in VANET, which is based on a secure encryption approach, starts sending a fake message, there is no ability to detect that the message is fake. Also, the overhead of cryptographic-based solution increases due to the distributed structure and dynamic topology.
In general, trust models in VANET can be divided into three categories; Data-centric Trust Models, Entity-centric Trust Models, and Combined Trust Models (Fig. 1).

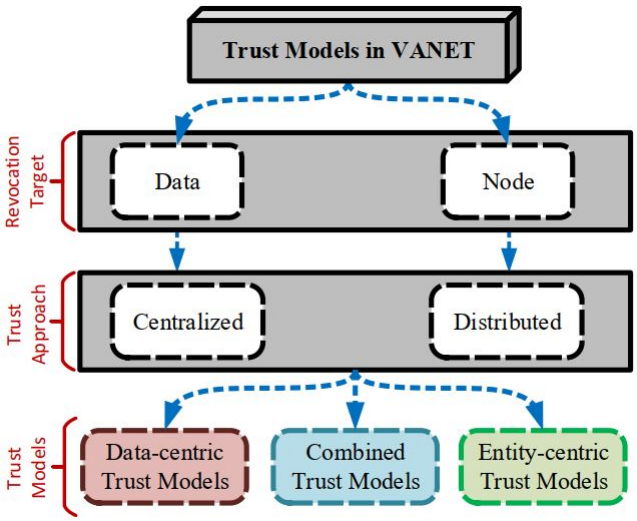

Fig. 1. Categories of Trust Models in VANET.[1]

In the rest of this paper, we discuss these solutions and provide a comparison in their functionality.

II. Vehicular Ad-hoc Network (VANET) and Trust Management

A. Data-centric Trust Models

Entity-centric Trust Models emphasize the reliability of vehicles or nodes that send messages. Therefore, by the neighbor's recommendations, sufficient information about the

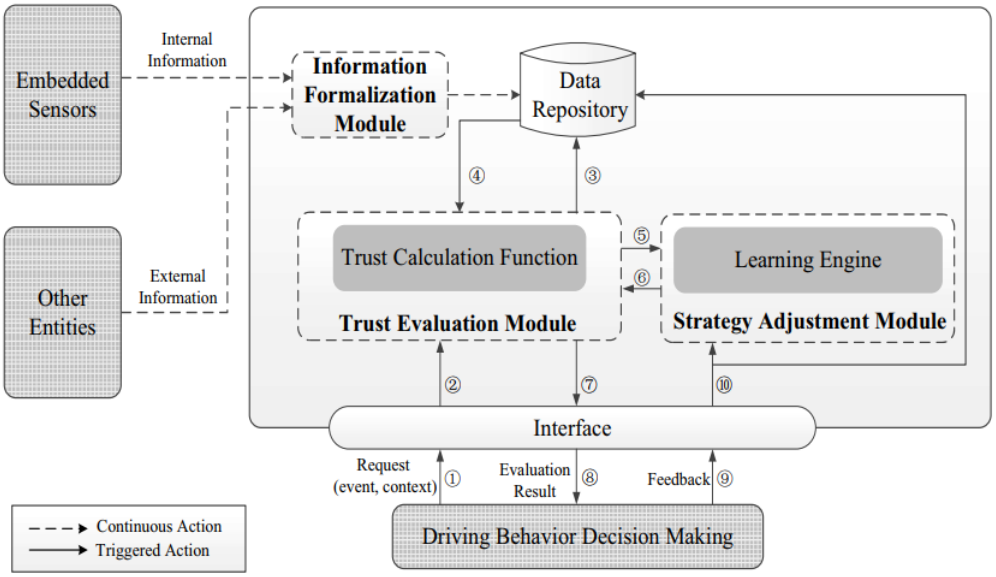

Fig. 2. The framework of the scheme proposed in reference [2]

origin of the message is collected for accurate assessment, which is very complicated due to the very dynamic nature of VANET.

Reference [2] proposed a context awareness trust management model to evaluate the value of trust for received message by internal and external information. In this study, the value of trust is calculated based on information received from sensors(internal information) and information received from other entities(external information). It also divides network entities into three categories: Trusted Authorities(TA), Roadside Units(RSUs), and Vehicles. The TA is responsible for registering vehicles and roadside units and serves as the certificate authority(CA). Roadside units are responsible for establishing inter-regional communications and receiving information from vehicles. Vehicles are also responsible for recording events and sending them to the network.It is assumed that all entities are equipped with a clock and GPS.

In regular system operations, a trust calculation is required for event e with content c (e, c). Assuming that e_f is the reality of the event e, e_e is the event recorded by the car sensors, and e_r is the event that the cars publish on the network (the superscript v represents the information recorded by car v). According to Table 1, there were four modes for the behavior of cars in the network.

TABLE I
BEHAVIOR OF A VEHICLE.

type	C1	C2	C3	C4
behavior	$e_f = e_p^v$ $e_p^v = e_r^v$	$e_f = e_p^v$ $e_p^v \neq e_r^v$	$e_f \neq e_p^v$ $e_p^v = e_r^v$	$e_f \neq e_p^v$ $e_p^v \neq e_r^v$
vehicle	honest	malicious	defective	malicious and defective

After introducing the entities and the vehicle modes, we will review the trust framework proposed in [2]. As shown in Fig. 2, the trust evaluation system has input and output. The system's input is information captured by sensors and received from other entities. The system's output is the decision made based on input. Input information is stored in standard format in the data repository. Due to limited storage space, information will be eliminated at the end of the event or after a specified time. Since we may not have external information about a particular event or the car sensors may be damaged, both internal and external information sources are used to calculate the trust and the weight of information changes depending on the conditions of use.

In this system, first, a request to calculate the trust value of the event (e, c) is issued by the decision-making unit, and the request is given to the trust evaluation module through the interface. From the data repository, all information that is close enough to (e, c) in terms of time and location is then delivered to the trust evaluation module. This information is passed to the learning engine unit, and then the resulting strategy returns to the trust evaluation module. Then the result is given to the decision-making unit through the interface. Finally, feedback goes back to the learning engine unit as a reward for reinforcing learning.

Finally, in [2] concluded without adding any overhead to the network, as long as the manipulated nodes are less than 50%, the proposed framework works with good accuracy.

B. Entity-centric Trust Models

Data-centric Trust Models generally focus on the accuracy of the information shared in the VANET. In Data-centric Trust Models, the accuracy of each incident is assessed using input information; Therefore, delay in receiving or losing information can affect the time and accuracy of the decision. In this method, two goals are more critical; Identifying the existence of malicious nodes and encouraging all nodes to

cooperate in the trust model.
Reference [3] proposed the Vcash model, which is based on the idea of market trading. In this model, vehicles have to sense traffic data and send them to roadside units(RSUs). RSUs are trustable units that collect all information and verify them. After verification, RSUs would announce events to covered vehicles and near RSUs. This model divides traffic events into Bogus event mode and Selfish mode. Bogus event mode refers to the event that there are one or more malicious nodes that broadcast the wrong message in the vehicular network. Selfish mode illustrates that one or more nodes in the network do not participate in the trust model. In the trust model proposed in [3], several nearby RSUs are identified as a zoning market. In this local market, cars have some initial cash and invest in a particular event, which can be profitable.
If an event is profitable, the vehicle's initial credit is added, and if an event is not profitable, their invested credit is deducted. Most cars invest in the event known as the existing event and are sent by the RSUs to the other vehicles. RSUs charge a fee for each vehicle announcement and distribute them among those invested in the event. This is how an event can be profitable. For scalability, a central server is defined that transferring vehicle cash information from one RSU to another RSUs (if the vehicle travels to another region). This unit plays the role of a bank in the marketing model. Fig. 3 shows the model infrastructure and Fig. 4 shows the marketing model of the trust model.

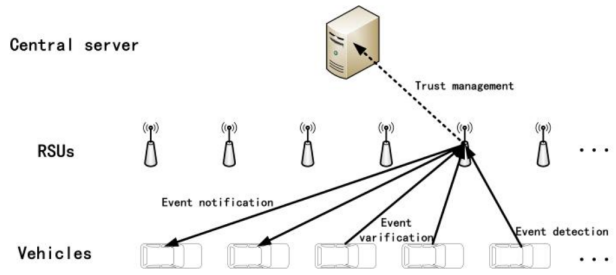

Fig. 3. Framework infrastructure, Vcash. [3]

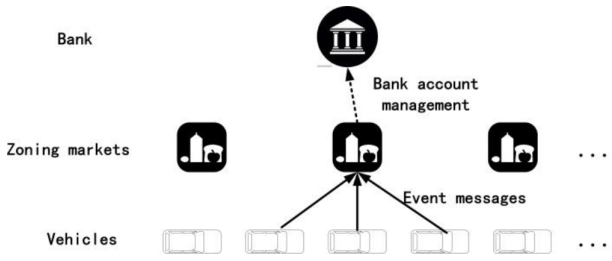

Fig. 4. Framework functionality, Vcash. [3]

This model has good conditions to satisfy the goals set for the Entity-centric Trust Models. Because RSUs charge for vehicle notification messages, a vehicle can not be in a mode that always receives event information and does not report any events. As a result, the model can deal with the selfish mode. Also, if a node sends the wrong message, it will invest

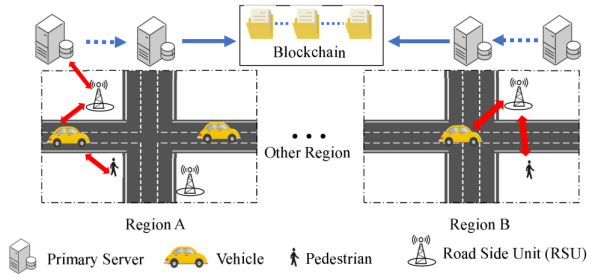

Fig. 5. System model of ATM. [4]

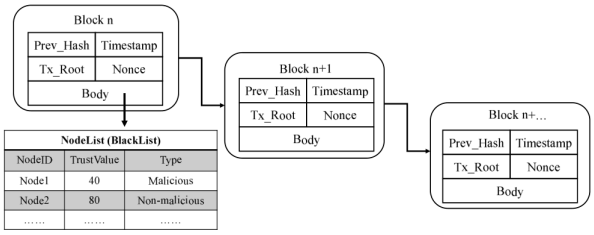

Fig. 6. The structure of blockchain, ATM. [4]

in the event that it is not profitable, and its financial credit will be deducted. If the car continues to send the wrong message, its credit will be exhausted, and it will no longer be able to send the message in the network.

Reference [4] reports ATM, a trust management model for finding malicious nodes. In [4], trust models are divided into centralized and decentralized trust models, and discuss the advantages and disadvantages of each model and try to provide a model of a combination of centralized and decentralized methods. Although the classification of this article for trust models is different from ours, the work done in this article is to find malicious nodes, so it falls into the category of Entity-centric Trust Models.
In [4], the activities of the adversary can be summarized in 3 types activity; Packet dropping misbehavior, spoofing attacks, and active cooperation among attackers. Blockchain, primary server, nodes, and RSUs are the main components of this model(Fig. 5). In this model, nodes are vehicles and pedestrians (equipped with smart devices). RSUs collect information from nodes and deliver it to the primary servers after confirmation. Due to the limited memory and low computing power of RSUs, we use primary servers to update blockchain information. The blockchain uses the Proof-of-Work consensus structure, and each block contains a list of nodes and information about the amount of trust and the type of nodes. (Fig. 6)
In [4], calculating the trust value is done in four steps. In the first step, a probe is sent to the neighboring nodes, and they are asked to send this message to RSU. If it is not malicious, In [4], calculating the trust value is done in four steps. In the first step, a probe is sent to the neighboring nodes, and they are asked to send this message to RSU. If the neighboring node is not malicious, it delivers the

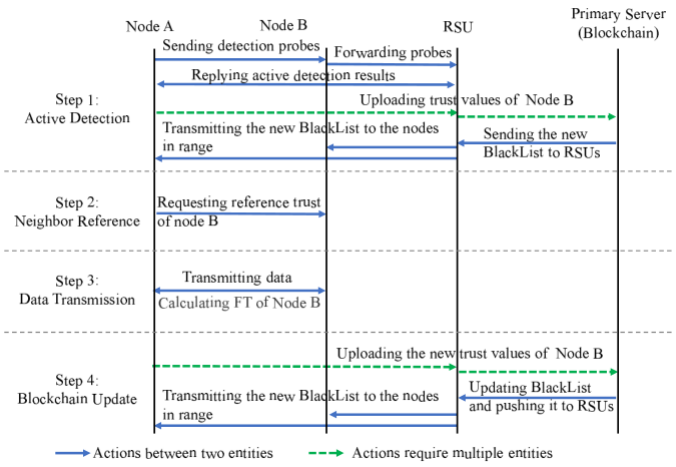

Fig. 7. An example of illustrating the procedure of ATM. [4]

received message to the nearest RSU, and RSU returns it to the original node. By calculating the time of sending and the integrity of the received information, a value of trust is calculated in this step. In the second step, the primary node requests the amount of trust history from the existing common neighbors, and in this step, another value of trust is calculated. In the third step, a trust value is calculated based on the throughput for the transmitted information for the neighboring node. Then the average of the values obtained in the previous steps will be the final trust value. In the fourth step, vehicles send these values to the RSU. The RSUs send to the primary servers to update the blockchain values. Fig. 7 shows an example of how to calculate trust in this framework. In the results section,[4] claims that as the probes are sent by vehicles, the detection speed of the offending nodes will increase. However, this is while the network load is increasing. They also claim high accuracy for detecting faulty nodes.

Reference [5] suggests a blockchain-based decentralized trust management model. In this model, information is stored in the blockchain, and the consensus mechanism is a combination of proof-of-work(PoW) and proof-of-stake(PoS) mechanisms. The main components of this model are RSUs and Vehicles. Vehicles are equipped with sensors and automatically notify nearby vehicles when an event occurs. In this system, vehicles are responsible to vote the received messages from their neighbors after observing the incident and after that, they have to send result to RSUs.
RSUs collect ratings for occurring events and calculate the reporter's trust value based on all ratings for their reported event. Due to hardware limitations and topological changes, these values are stored in the blockchain network so that if a vehicle travels to another region, its trust results can be used there as well. Based on the rating uploaded by the vehicles in the RSUs, an offset value is calculated for the value of each vehicle's trust. In this system, the calculated offset has a value between $+1$ and -1.

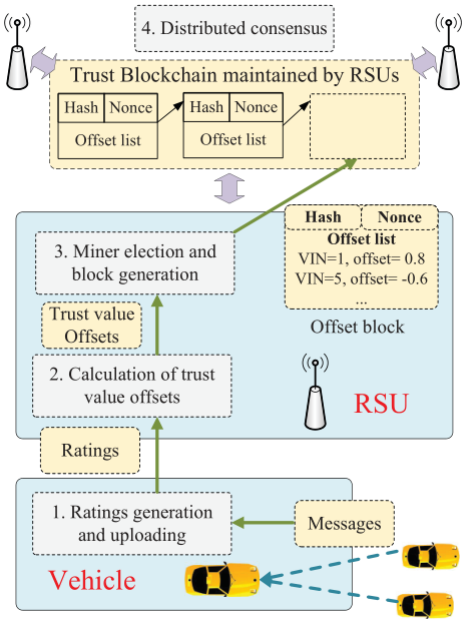

Fig. 8. System design of blockchain-based decentralized trust management. [5]

Consensus or how to choose a miner to propose a new block in the blockchain is an important part of blockchain-based systems. Reference [5] presents a combination of PoW and PoS consensus mechanisms. In the proposed model, the miners compete to release a new block according to the PoW approach. However, the complexity of the network is adjustable and is inversely related to the stakes. The more stakes RSUs have, the less difficult it will be for the network to find the right nance in the PoW approach. Stakes in this system are the sum of absolute offsets calculated in RSUs. To win the block publishing competition, we have to solve equation 1.

$$Hash(ID_{RSU}, time, PreHash, Nonce) \leq S_i \qquad (1)$$

$$S_i : \overbrace{000...0}^{N_z} \underbrace{1111...111}_{N_m} \qquad (2)$$

In Equation 2, if the stakes increase, the number n decreases, resulting in less network complexity. This is because the higher sum of the absolute offsets for an RSUs (more stake), the more trusts are transferred and with the more chances and in less time they have to release in the blockchain network. Fig. 8 is an overview of the trust management model presented in the reference [5].

C. Combined Trust Models

In combined trust models, the validity of incoming messages assets by node reputation and messages content.

Reference [1] proposes a combined trust model. In this model, the value of trust is affected by both the node reputation

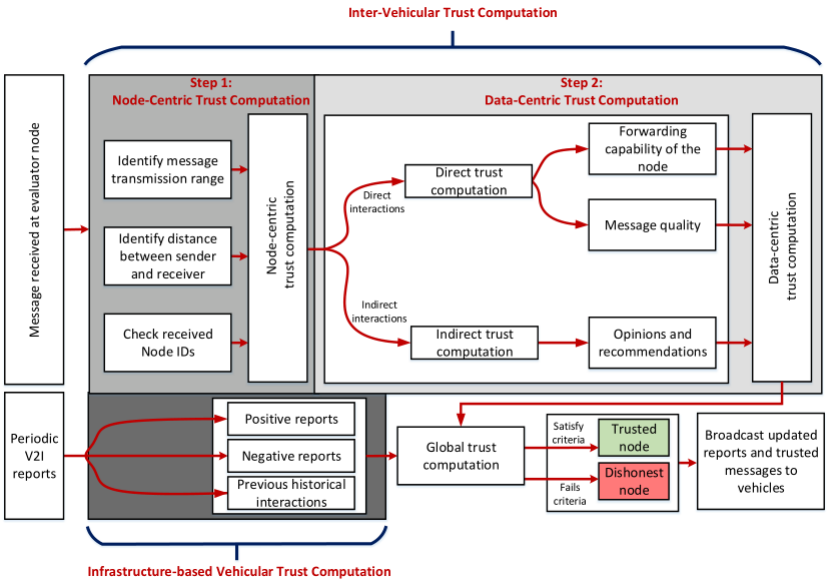

Fig. 9. Operation of the Proposed Trust Model, MARINE. [1]

and the message content. In this model, the network infrastructure sends some information for vehicles; this information is the model's resource. In the proposed model, the distance between sender and receiver is essential, and if this distance exceeds a specific range message would be dropped.
The final value of trust is affected by two values. In other words, to calculate the value of trust, we go through two steps. The first step is infrastructure-based vehicular trust computation, and the second step is inter-vehicular trust computation. In the infrastructure-based vehicular trust computation step, the amount of trust is calculated based on the reports received by the infrastructure and historical interaction records.
In the inter-vehicular trust computation step, the trust value is calculated at two levels. The first level is the node-based check and checks the message sender at the permissible distance. If the vehicle is at the proper distance, we will review the content of the message. At this stage, the content of the message will be analyzed according to the neighbors' opinions about the message content and the quality of the message content. The calculated values are combined, and the global trust value is calculated. If this value is less than a specific value, the message will be deleted and not broadcast.
The simulation results show that the model presented in reference [1] has a good performance in a network with up to 35% of Man-in-the-Middle(MiTM) attackers and appears successful in tests.

III. Conclusion

In this study, we reviewed five references related to the trust management in VANETs. For each case, we summarized the proposed methods and categorized them into Data-centric Trust Models, Entity-centric Trust Models, and Combined Trust Models categories.

In the rest of this section, we define some criteria by which we compare the discussed methods.

- **Decentralized**: The proposed model is decentralized or belongs to the category of centralized models.
- **Distance**: Indicates whether the event reporter distance will affect the final amount of calculated trust.
- **Time**: Indicates whether the time difference will affect the final amount of calculated trust for events.
- **Event Type**: Indicates that in the proposed trust model, the type of event would be reported or not.
- **Neighbor Recommendation**: Indicates whether cars would use their neighbors' recommendations to evaluate the message trust or node trust.
- **Vehicle Rule**: Indicates whether roles are defined in the proposed model for vehicles or that they all play an equal role.
- **Historical Interactions**: Indicates whether the historical interactions are used in calculating the amount of trust or not.

TABLE II
COMPARISON OF TRUST MODELS

Refrence:Metric	**Decentralized**	**Distance**	**Time**	**Neighbor Recommendation**	**Event Type**	**Vehicle Rule**	**Historical Interactions**
TROVE [2]	✓	x	x	✓	✓	x	x
Vcash [3]	x	x	x	✓	✓	x	x
Blockchain-based [4]	✓	x	✓	✓	✓	x	✓
ATM [5]	✓	x	x	✓	x	x	✓
MARINE [1]	x	✓	x	✓	✓	x	✓

REFERENCES

[1] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain and F. Hussain, "MARINE: Man-in-the-middle attack resistant trust model in connected vehicles", IEEE Internet Things J., vol. 7, no. 4, pp. 3310-3322, Apr. 2020.

[2] J. Guo et al., "TROVE: A context awareness trust model for VANETs using reinforcement learning", IEEE Internet Things J., vol. 7, no. 7, pp. 6647-6662, Jul. 2020.

[3] Z. Tian, X. Gao, S. Su and J. Qiu, "Vcash: A novel reputation framework for identifying denial of traffic service in Internet of Connected Vehicles", IEEE Internet Things J., vol. 7, no. 5, pp. 3901-3909, 2020.

[4] F. Li, Z. Guo, C. Zhang, W. Li and Y. Wang, "ATM: An Active-Detection Trust Mechanism for VANETs Based on Blockchain", IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 4011-4021, May 2021.

[5] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks", IEEE Internet Things J., Vol. 6, April 2019.

Saeed Jafari received the B.S. degree from Isfahan University of Technology in 2019, and he is currently a master student of Electrical Engineering (Cryptography and Security) in the University of Tehran, and his current research focuses on trust management, Cyber-Physical Systems,and Internet of things security.