
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issues 3, pp. 451–462, DOI 10.12694:/scpe.v21i3.1743

A FRAMEWORK TO SYSTEMATICALLY ANALYSE THE TRUSTWORTHINESS OF NODES FOR SECURING IOV INTERACTIONS

INDU BHARDWAJ *, SIBARAM KHARA †, AND PRIESTLY SHAN ‡

Abstract. Trust plays essential role in any securing communications between Vehicles in IOV. This motivated us to design a trust model for IoV communication. In this paper, we initially review literature on IoV and Trust and present a hybrid trust model that separates the malicious and trusted nodes to secure the interaction of vehicle in IOV. Node segregation is done using value of statistics (S_t). If S_t of each node lies in the range of mean (m) plus/minus 2 standard deviation (SD) of PDR then nodes behaviour is considered as normal otherwise malicious. The simulation is conducted for different threshold values. Result depicts that PDR of trusted node is 0.63 that is much higher than the PDR of malicious node that is 0.15. Similarly, the Average no. of hops and trust dynamics of trusted nodes are higher than that of malicious node. So, on the basis of values of PDR, number of available hops and Trust dynamics, the malicious nodes can be clearly identified and discarded.

Key words: Internet of vehicles, Security, Trust Model, Challenges, Malicious Node

AMS subject classifications. 68M11

1. Introduction. The Internet of vehicle (IoV) [1] is a network in which vehicles, on-board sensors, road-side infrastructure and vehicular cloud are connected wirelessly to exchange traffic safely related information. It allows vehicles and infrastructure to be connected using internet connectivity [2]. In IoV, the concept of Internet of things (IoT) [3] is applied to the vehicles. It can be said that IoV is the joint version of VANET and IoT that enhances the road safety and security. The prime objective behind its implementation is to allow communication between different entities involved in it. In [4], IoV is defined as the dynamic mobile communication systems that enables communication between vehicles and public networks using V2V (vehicle-to-vehicle), V2R (vehicle-to-road), V2H (vehicle-to-human) and V2S (vehicle-to-sensor) interaction. Authors in [5], considers IoV as large-scale, distributed, wireless communication network for exchanging data between vehicle, road, human and internet, as per the agreed data interaction standards and communication protocols. To ensure the security of information exchanges in among the entities of IoV, the trust is established.

IoT is a swiftly developing system in which all entities of a network directly or indirectly connect to Internet. The evolution of IoT have revolutionized the vehicles to the great extent. For e.g. cars are equipped with navigation systems that gives information about traffic jams/ weather condition via internet and they also update the routing maps automatically. Some car models are equipped with vehicular communication network modules to communicate with other cars and alert the driver from invisible risk. They can find the car parking lots by themselves and react to any forthcoming accident.

Since IoV enables communication among various vehicles (which may also belong to malicious drivers/ pranksters), a serious interrogation arises on whether to trust vehicle or not. The idea of IoV network has brought various security, privacy and reliability issues that are imitated in a common term "trust" [6]. For example, IoV network is open and more vulnerable to attack by malicious users. Modelling trust is quite challenging in IoV network [7]. It is difficult to recognize which node is trusted and which is malicious.

Everybody recognizes what trust is, but nobody really knows how to define it to everyone's satisfaction. Trust is a feature that exist in every communication but it is hard to formulate trust. After reviewing the

*Faculty of Electronics & Communication Engineering, Galgotias University, Greater Noida, India (indubhardwaj2011@gmail.com)
†Sharda University, Greater Noida, India (sianba@rediffmail.com)
‡Galgotias University, Greater Noida, India (priestlyshan@gmail.com).

current trust models for vehicular network, we present an effective trust model for IOV to separate the trusted and non-trusted nodes.

The main contributions of this paper are the followings:

1. We propose a fuzzy logic-based approach to evaluate the trust of one-hop neighbors. The proposed approach takes into account three different factors, namely, cooperativeness, honestness, and responsibility factors. Since the fuzzy logic-based approach is able to handle the complex and uncertain behavior of vehicles, it is suitable for dynamic and lossy vehicular networks.
2. We propose a Q-learning approach to evaluate indirect trust of nodes that are not directly connected to a trustor node. An evaluation about a non-neighbor-node is conducted by averaging the evaluation reports.
3. We propose a fuzzy logic-based approach to evaluate the trust of one-hop neighbors. The proposed approach takes into account three different factors, namely, coop- erativeness, honestness, and responsibility factors. Since the fuzzy logic-based approach is able to handle the complex and uncertain behavior of vehicles, it is suitable for dynamic and lossy vehicular networks.
4. A threshold-based trust approach is proposed to evaluate the trustworthiness of the nodes. This approach authenticates the nodes by comparing their trust values with a pre-set trust threshold. Since threshold-based approach is able to validate nodes without involving complex computation. So, secure node interaction can be established in timely manner that suits to the dynamic and decentralized nature of IoV network.
5. A trust initialization and storage mechanism is provided by the proposed model. to handle the cold start problem and scalability issues faced by existing models.
6. A joint probability-based approach is presented to update the trust at online centres. The trust is calculated by evaluating the trust worthiness of data using various statistics collected during interaction.
7. Computer simulations used to evaluate the effectiveness of the proposed trust model in separating malicious nodes from the trusted nodes and discarding them. By using this model, the malicious nodes will no longer be able to harm the network.

The rest of the paper is organized as follows. Section 2 includes the review and categorization of existing trust models on basis of their types, methodologies used and the network type. It also presents various challenges in modelling trust in IOV network. Section 3 includes the proposed trust model along with a descriptive discussion. Section 4 includes the simulation scenario and the results based on analytic study and simulation. At last, Section 5 concludes the paper and presents future scope.

2. Related Work.

2.1. Definition of Trust. Trust has different definitions in different contexts and subjects. But the importance of trust is same in every aspect. There is no particular definition of trust in vehicular network. Most of trust definitions are taken from the social sciences. However the trust has direct relation with the network security and basic concept of trust can be used to enhance the security of the network [8,9]. The trust is generally considered as a belief that one entity has about other entities depending upon the past experiences, data about the nature of entity, and on recommendations from other trusted entities. Authors in [10] stated that trust is a prime component in forming a trusted environment for VANET which endorses security in the network. In study [11], trust is an expectation and the belief about upcoming behaviour, depending upon past experiences. Authors in [12], defines trust as a relation among different entities established depending on the observations of past interactions.

2.2. Existing Trust Models. Research on development of trust model have been previously explored by various researchers in the field of MANET, VANET. But there are limited models which are proposed till now for IoV environment.

Authors in [13] presents a Multi-faceted approach to model the trustworthiness of data. This model is decentralized, task specific, scalable but it has not addressed the robustness. Gomez et al. model called TRIP [14] to differentiate malicious nodes from trusted nodes. It is a scalable model but it did not consider overhead introduced. Fangyu Gai [15] presented Ratee-Based Trust Management scheme model where each node maintains its own reputation rated by other during previous interactions. In extension to the work in [15],

Table 2.1
Types of trust models and their references

Types of Model	**Study**
Entity Based Model	[13], [14], [15], [16]
Data-based models	[17], [18], [19], [20] , [22], [23]
Hybrid Models	[10], [12], [21], [24],

Table 2.2
Various methodologies used in trust models and their references

Methodology	**Study**
Weighting	[10], [12], [21]
Ratings	[15], [16] , [19]
Probability	[18]
Bayesian network	[17], [22], [23]
Fuzzy logic	[14], [20]
Observations/Opinion gathering	[13], [24]

authors proposed a trust model for Social IoV [16]. This model is also ratee based This model also includes the Certification authority server and public key cryptography to avoid any alteration in the trust information by the ratee.

Study [17] includes a data based trust model for VANET to evaluate the trustworthiness of messages related to road safety. It used data trust instead of entity trust and utilizes Bayesian Inference approach in voting algorithm to enhance the robustness of network. Work in [18], presented a scheme to compute the reputations based on Hidden Markov Model (HMM). The proposed scheme evaluates the message reliability and predicts the legitimacy for broadcast messages. Authors in [19] proposed an announcement scheme for VANET based on reputations. Reputation value is evaluated by using a aggregation algorithm that is based on binary feedback ratings.

Study [20] includes an experience -based fuzzy trust model for securing the vehicular network. The proposed model executes various security checks to confirm the accuracy of received information. Yao et al. [21] proposed hybrid model including entity-centric trust evaluation based on weight and data-centric trust evaluation on the basis of experiences and the utility theory. L. Cong [22] et al. proposed data-based trust model to evaluate the correctness of vehicle to vehicle incident reports. This model computes the trust score by using behavior history of the incident report accuracy for a vehicle. Shu Yang et. al [23] proposed a trust model to elect anomaly nodes in IOV environment by forming cluster heads. Authors also provided mutual supervision model to handle tempering behaviors. Chen & Wei provided RSU and beacon-based trust management model[24] that prevents sending of false messages. Author in [12] proposed a Beacon-based trust management (BTM) model which computes entity trust from beacon messages. Merrihan Badr Monir et al. [10] combined experience and Role based trust to give Categorized trust based message reporting scheme for VANET.

According to the literature review, trust models are divided in three categories:

1. Entity trust model - evaluates the trustworthiness of the entity.
2. Data trust model - calculates the trustworthiness of data sent by entity.
3. Hybrid trust models – performs trustworthiness of data as well as entity.

Table 2.1 Summarizes trust models existing in each category. These trust models used different methodologies to model trust in network. Table 2.2 summarises various methodologies used in existing trust models. The methodologies used in for modelling trust are weights, ratings, probability, Bayesian network, fuzzy logic, and opinion gathering. From table 2.2, it can be clearly seen that Weights, ratings and Bayesian network are commonly used for trust modelling whereas probability approach is least used methods. Only one out of 14 trust models studied in literature used probabilistic approach in VANET. So, in our work we will focus on probabilistic approach to model evaluate the trust value. Table 2.3 shows the types of network for which the existing trust models are proposed. Out of 14 trust models studied in the literature, most of the trust models are designed for VANET and few are proposed for IoV environment. In our work we will focus on modelling trust for IoV network.

TABLE 2.3
Types of network and their references

Network	Study
VANET	[10], [12], [13], [14], [17], [18], [19], [20], [21], [22], [24]
IoV	[15], [16], [23]

2.3. Challenges in Trust management and Properties of Trust Model. Managing trust in IoV environment is quite important so that as to prevent malicious node to spread traffic-related false or tempered information. False information circulated by malicious nodes may create traffic jams and collision on roads. Dissemination of false information sometimes may result in dire consequences like loss of life. It is very challenging in IoV environment to manage trust in IoV network is various characteristics.

Trust verification in real-time: Vehicles randomly enter and leave IoV environment and move at very high speed so it is challenging to build up the trust in timely fashion. As vehicles interact for small time, it is difficult to judge which node is untrusted and up-to which extent.

Dynamicity: vehicular nodes are continuously moving so it is not necessary that the behaviour of trusted node will remain same always. Besides that, conditions of road are highly unpredictable [25]. Trust model developed for IoV should be able to handle these varying situations and characteristics of Network.

Large scale network: Number of vehicles in IoV are very large. Also, this situation become worse in the peak rush hours. This situation may arise problem like network congestion as vehicles are interacting through shared channel, and data overload – as vehicles may receive lot of data at one time from other vehicles stuck in a congested area.

Decentralization: There is no centralized infrastructure in IoV environment. Nodes can come and leave the network at any time. If a node interacts with a vehicle now, it is not guaranteed to interact with the same vehicle in the future.

According to the above characteristics of IoV and challenges in modelling trust, trust model should have following characteristics:

Fast computation: In order to evaluate trustworthiness of entity and data in real time for making quick decisions in IoV, trust model should have less complex so that trust computation can be fast. low complexity with also result in low computation overhead.

Distributed trust computation: Computation of trust in distributed manner is more suited for IoV due to its open, dynamic and self-organizing characteristics. When every node will calculate trust, there will be no need of central server to calculate the trustworthiness of nodes. Moreover, the system will have less chances of complete failure.

Scalable: Since the traffic is unpredictable so, the trust model should be scalable enough to handle the large number of nodes avoiding network congestion.

Literature review concludes that most of the existing trust model has been proposed for VANET. Trust modelling in IoV is still in infant stage. In our literature review, only three models out 14 models reviewed are proposed for IOV out of which two are entity trust model [15, 16] and one is data trust model [23]. There is no hybrid trust model proposed so far for IoV. Besides that, the existing IoV trust models suffers two main problem a) Scalability - when the number of nodes in network increases then it becomes difficult for each node to maintains the trust values of all. b) Cold start problem: this problem arises when a new joined node wants to communicate other nodes. Other nodes do not find the trust value to authenticate new node. In addition to this, we have identified some character that a trust model should have to overcome the above-mentioned challenges in IoV. To address these issues, we have proposed a framework for probability distribution-based hybrid trust model for IoV that initially computes the trustworthiness of nodes and then that of data exchanged between them by calculating trust. The proposed model is designed to solve the scalability issues and cold start problem and achieve the desired characteristics of trust model.

3. Proposed Model. The proposed trust model for IoV is event driven. Trust values are stored online at trusted centres and updated after every event. System works as distributed protocol in which nodes computes the trust value of other node with which it interacted after every interaction. In this model, each node will be assigned a initial trust value of 0.5 whenever it joins the network. This will solve the cold start problem of

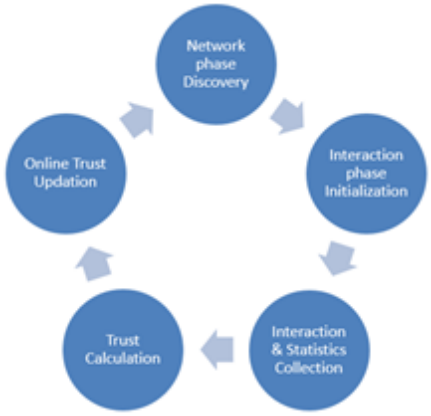

FIG. 3.1. *Trust Modelling Process*

the existing trust models. The nodes store the trust value of only limited set of nodes with whom it interacted recently. Besides this all other trust values will be stored at the online trusted centre. This will make the network more scalable in the sense that when the number of nodes increase during peak hours then nodes need not maintain the trust value of all other nodes as the trust values will be maintained at online centres. This will solve the problems associated with limited storage at node. This model Suits well to be decentralized architecture of IOV as there is no centralized authority for trust computation. Each entity in network has the capability to compute the trust value itself after interaction and update it online.

3.1. Trust Modelling. IOV has several advantages like internet connection, fast computations etc. over VANET that make it more useful for securing vehicular communication. Nonetheless, IOV is openly accessible and has huge data set involved in computation. Moreover, IOV is quite dynamic network where vehicles are joining and leaving the network continuously to cope up with these properties of IOV, we propose a trust model to secure communication in IOV. Trust modelling process used in proposed model is shown in Figure 3.1.

In an IOV trust model sender vehicle has to locate another vehicle with whom it wants to interact to get or provide the service as per the requirement of situation. If there are multiple requests then receiver node initialize the network phase discovery with the node having good reputation (high trust value). Once the network phase is over the interaction between node takes place. During this interaction, statistics is collected by RSU which is further used to calculate the new trust value of sender and receiver node. The trust is finally updated at online centers.

3.2. The Proposed Trust Model. The trust model proposed to secure communication in IOV is depicted as flow chart in Figure 3.2. The Proposed model is event driven. The process starts when A tries to interact with any node B to provide any service or get service from it. Node A initiates RSU to find location of Node B. To achieve this, RSU initially looks up to the past trust value of Node A saved at online centre to judge to trustworthiness of A. If trust value of A is available, RSU checks whether A's trust is greater than past threshold (T_0). If A fulfils the condition for minimum level of trust threshold, it is considered as legitimate node. If the A's trust value is less than T_0 then A can't interact with B.

Once RSU finds A as trusted Node, it initiates the procedure to find location of B. After locating B, RSU repeats the same procedure to judge trustworthiness of Node B. If B also meets the minimum trust requirement set for a node to be a legitimate node, the interaction between A & B starts. If B's Trust value is less than T_0 then node A cannot interact with node B. During interaction between both trusted nodes A & B, RSU collects the trust statistics like Packet Delivery Ratio (PDR). PDR is given by the following equation

$$PDR_t = \frac{\text{Total packet received}}{\text{Total packet transmitted}} \tag{3.1}$$

If the value of statistics (S_t) of each node lies in the range of mean (m) plus/minus 2 standard deviation

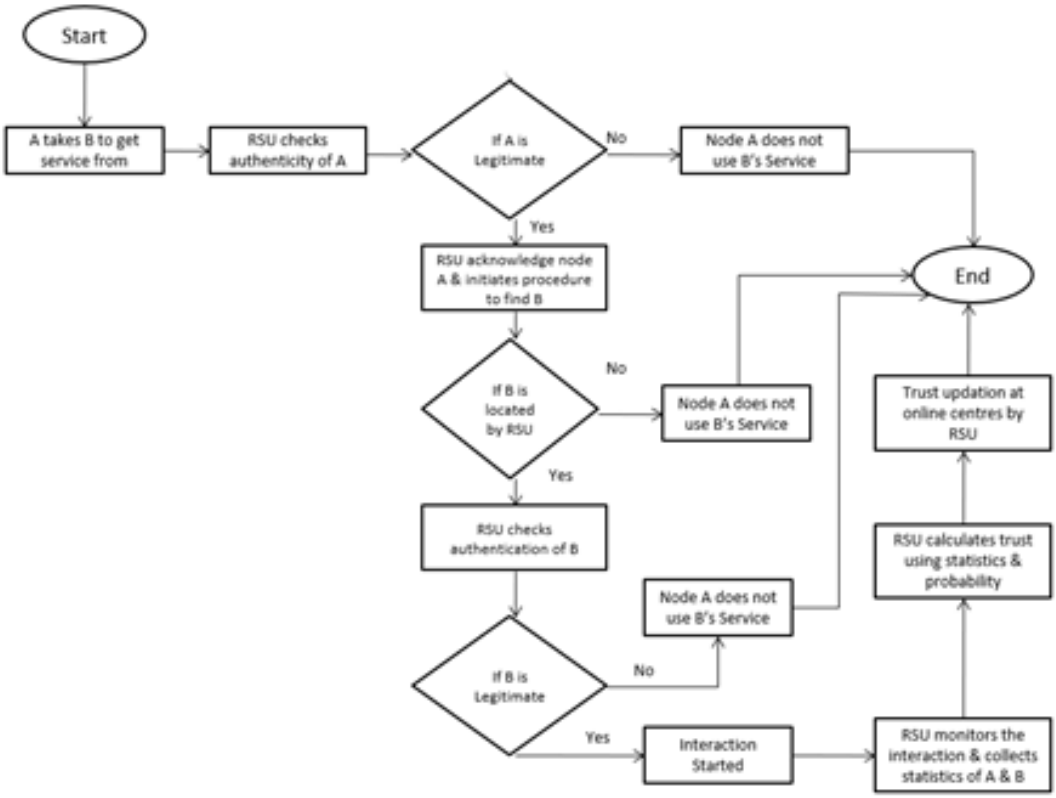

FIG. 3.2. *Flow Diagram of the Proposed Trust model for IoV*

(SD) of PDR then nodes behaviour is considered as normal otherwise malicious. Once the interaction between A & B is over, RSU calculates the new trust value for both node A & B by using conditional probability. RSU then updates the new calculated trust value at online centres.

$$if \left\{ \begin{array}{l} S_t > \ m + 2SD \\ S_t < \ m - 2SD \end{array} \right\} \quad Malicious\ Behaviour \tag{3.2}$$

and

$$if \left\{ \begin{array}{l} S_t \leq \ m + 2SD \\ S_t \geq \ m - 2SD \end{array} \right\} \quad Trusted\ Behaviour \tag{3.3}$$

Each time the successful / failed communication will take place between nodes the trust will be recalculated using conditional probability and updated (increased in case of successful interaction & decreased in case of failed interaction). It is to be noted that the above algorithm is inspired by interaction of humans in real life. We want to take services from trusted service provider and after taking service we update the feedback (trust value in this algorithm).

4. Results and Discussion.

4.1. Simulation Scenario. This section presents the simulation scenario our proposed trust model for IOV. The main aim of conducting this simulation is to study how efficiently the proposed trust model works in presence of non-trusted nodes in IoV environment. To achieve this the Simulation is conducted on SUMO (1.4.0 version) and MATLAB (2016a version). SUMO is used as traffic simulator for generating the traffic patterns and MATLAB is used as event simulator. Figure 4.1 shows the traffic scenario of real-world map for

FIG. 4.1. *Traffic Scenario - Open Street Map for a Manhattan City*

Manhattan city generated using SUMO. The figure 4.1 includes top-view of traffic scenario near intersection of two roads having buildings. The objects in green color are vehicles moving on roads.

In experimental setup, the status of each node is changing dynamically. The input parameters provided to the simulation are listed in Table 4.1. Simulation is conducted by randomly setting some of the nodes as abnormal nodes. Initially, all nodes are assigned with equal trust value of 0.5. But with passage of time trust value of normal nodes increases with every successful interaction and that of abnormal node will decrease due to their malicious behavior.

To simulate this model, an IoV environment consisting of 30-100 nodes is considered in which 10% are malicious nodes. These nodes randomly move in 1000*1000 meters square area and has range of 250m for communication. The total time of simulation is taken 180 mins (3 hrs). The performance of proposed trust model is evaluated using three metrics i.e. number of available hops, PDR and trust value as metrics.

Simulation is conducted for three different value of threshold to study the impact of threshold value on evaluation metrics like PDR, average number of available hops. This study of different threshold will show how the value of evaluation metrics (PDR, number of available hops) vary for trusted and untrusted node under normal threshold policy (θ= 0.65), slightly strict (θ= 0.70) and highly strict threshold policy (θ = 0.75).

4.2. Analytical Evaluation.

Fast computation: Instead of cryptography, the proposed model makes use of trust values for validating the trustworthiness nodes. This reduces the computation complexity and overhead involved in key management. This makes the computations fast.

Distributed trust computation: The proposed model does not involve any central authority to calculate the trustworthiness of nodes. Every entity in the network is connected to internet and able to calculate and update the trust value of nodes after every interaction. The distributed trust computation reduces the chances of complete system failure and is more suited for IoV due to its open, dynamic and self-organizing characteristics.

Scalable: Any node in the network need not maintain the trust of all the nodes in the network rather only for small set of nodes with which node plans to have interaction. So, the proposed trust model is scalable enough to handle the large number of nodes avoiding network congestion. It also solves cold start

TABLE 4.1
Parameters for simulation

Simulation Parameters	**Values**
Monitoring Area	1000 × 1000 meters
Number of nodes (n)	30-100
Communication Range	250 meters
Packet Interval	2 ms
Length of Data Packet	923 bits
Symbol rate	256KB/S
Bit rate	512KB/S
Simulation time	180 (s)
No Malicious Nodes	10%
Routing Protocol	A-STAR
Mac Layer Protocol	802.11p
Trust Range	[0,1]
Initial trust value of each node	0.5

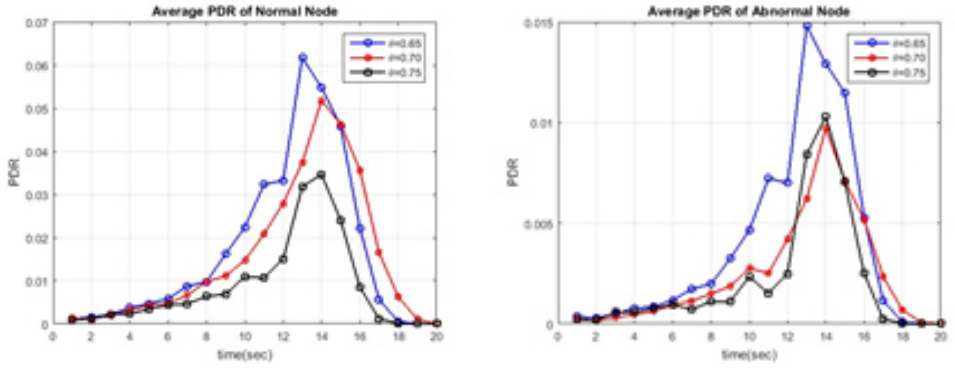

FIG. 4.2. *Average PDR for normal node (left) and abnormal (right) nodes*

problem by assigning minimum trust to each node initially.

4.3. Simulation-based Evaluation. The simulation shows easily how the proposed model can filter trusted and malicious nodes se depending upon the Packet delivery ratio, number of available hops curves. The network simulation is conducted for three different values of threshold values.

4.3.1. Packet delivery ratio. It is the ratio of number of packets received successful to the total number of packets sent. As we know that malicious nodes will not forward all the received packet so estimation of its PDR will be less as compared to that of trusted node. The curves show how the packet delivery ratio of normal and malicious nodes varies with time. The results show that average PDR value for trusted as well as malicious nodes, varies continuously with increase in time. Ideally the value of PDR should be as high as possible for better performance of network. The graphs presented in figure 4.2 depicts that average PDR of normal nodes is high approx. i.e. 0.063 in threshold $T_0 = 0.65$ as compared with the average PDR of abnormal nodes i.e. 0.015 at threshold $T_0 = 0.65$.

4.3.2. Effect of threshold policies on PDR. Table 4.2 shows the values of Average PDR of trusted nodes for different thresholds ($\theta = 0.75,0.70,0.65$) at different instants of time starting from t= 0 sec to 20 sec. Initially at t=0, the Average PDR of trusted nodes is zero for each value of θ. As the times increases from t=0 to t=14 seconds, the average PDR value of trusted nodes is increasing for each threshold and After t=14, Average PDR values are decreasing for each threshold value till t=20. It means the maximum PDR achieved at t=14 sec for all the thresholds. For θ=0.65 is 96% which is very high as compare to the maximum PDR achieved for θ=0.75 i.e. 64%.

The PDR reading at almost every instant of time is less for higher threshold values, for e.g. at t=10, PDR

TABLE 4.2
PDR value of trusted nodes at different threshold

θ \ t	0	2	4	6	8	10	12	14	16	18	20	Max
0.75	0	0.31	0.32	0.35	0.37	0.41	0.45	0.64	0.38	0.30	0.30	0.64
0.70	0	0.30	0.33	0.36	0.40	0.44	0.58	0.82	0.52	0.30	0.31	0.82
0.65	0	0.31	0.35	0.38	0.63	0.84	0.80	0.96	0.81	0.38	0.33	0.96

TABLE 4.3
PDR value of non-trusted nodes at different threshold

θ\t	0	2	4	6	8	10	12	14	16	18	20	Max
0.75	0	0.00	0.00	0.00	0.00	0.00	0.0025	0.0100	0.0025	0	0	0.0100
0.70	0	0.00	0.00	0.00	0.00	0.00	0.0030	0.0103	0.0052	0.0001	0	0.0103
0.65	0	0.00	0.00	0.00	0.00	0.00	0.0042	0.0135	0.0053	0.0007	0	0.0135

for θ=0.65 is 0.84, which decreases for θ=0.70 i.e. 0.44 and further decreases for θ=0.75 i.e. 0.41. Similarly, at t=20 seconds, PDR for θ=0.65 is 0.33, which decreases for θ=0.70 i.e. 0.31 and further decreases for θ=0.75 i.e. 0.30. This discussion on PDR values concludes that the PDR for trusted nodes decreases significantly (i.e. from 96% to 64%) with increase in trust threshold (i.e. from 0.65 to o.75). This is due to the reason that if threshold policy is strict then sometimes trusted nodes may be considered as untrusted.

Table 4.3 shows the values of PDR of non-trusted nodes for different thresholds (θ = 0.75,0.70,0.65) at different instants of time starting from t= 0 sec to 20 sec. Initially at t=0, the Average PDR of non- trusted nodes is zero for each value of θ. It remains zero from t=0 to t=10 seconds irrespective of threshold value. After t=10 seconds, the average PDR value of non-trusted nodes increases for each threshold till t=14 seconds and After t=14 seconds, Average PDR values are decreasing for each threshold value till t=20 seconds. It means that the maximum PDR achieved at t=14 seconds for θ=0.65 is 1.35% which is comparable to the maximum PDR achieved for θ=0.75 i.e 1.0%. For each non zero values of PDR (from t=12 to t=18), it is observed that, the PDR reading at every instant of time is less for higher threshold values. For e.g. at t=12, PDR for θ=0.65 is 0.42, which decreases for θ=0.70 i.e. 0.003 and further decreases for θ=0.75. This discussion on PDR values concludes that with increase in trust threshold, the PDR for non- trusted nodes decreases but not significantly. Reason behind this is that malicious nodes has nothing much to do with threshold policies as their main motive is to affect PDR.

4.3.3. Average number of available hops to the non-trusted node. We estimated the average number of available hops to the trusted nodes with the progression of time for different trust threshold. Fig 4.3 depicts that as the time progresses, the available number of hops to the trusted nodes increases because of their good behaviour. More number of hops helps them in getting shortest path. So, behaving good is rewarding.

It is evident from the figure 5 that as the time progresses the number of average hops to the non-trusted nodes approaches to zero. Within first 10 seconds the average number of hops drops significantly. This drop is more prevalent in stricter threshold policy (θ=0.75).

4.3.4. Effect of threshold policies on Available number of hops. Table 4.4 shows the values of number of hops available of trusted nodes for different thresholds (θ = 0.75,0.70,0.65) at different instants of time starting from t= 0 sec to 20 sec. Initially at t=0, the no. of available hops for trusted nodes is zero for each value of θ. As the times increases from t=0 to t=20 seconds, the available no. of hops for trusted nodes increases continuously for each threshold value due to their good behaviour in the interactions. Hops readings at every instant for different values of threshold shows that available number of hops is comparatively less for higher threshold values. for e.g. at t=10, hops available for θ=0.65 is 27, which decreases for θ=0.70 i.e. 18 and further decreases for θ=0.75 i.e. 15. Moreover, Average no. of hops available for θ=0.65 is 26 which is very high as compare to the that for θ=0.75 i.e. 17. This discussion concludes that the growth of average available hops is higher when θ is less (θ=0.65) and smallest during the strict policy. This is due to the reason that under strict threshold policies the trusted node sometimes may be misunderstood as non-trusted.

Table 4.5 shows the values of number of hops available of non-trusted nodes for different thresholds (θ =

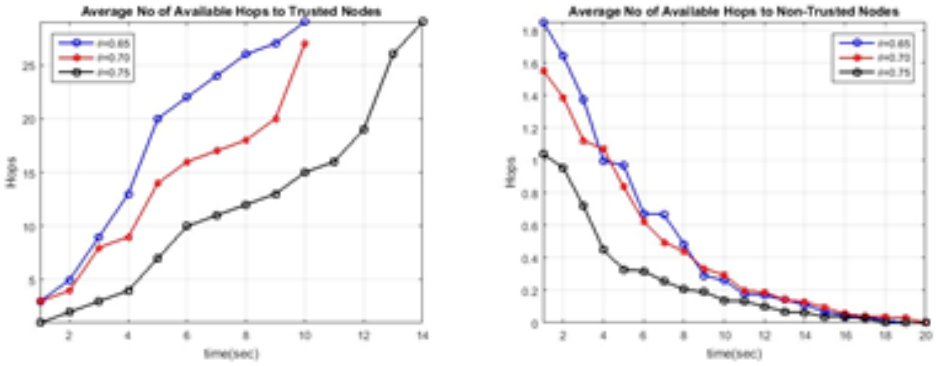

FIG. 4.3. *Average number of Available hops to trusted (left) and non-trusted (right) nodes*

TABLE 4.4
Number of hops available for trusted nodes at different threshold

θ\Time	0	2	4	6	8	10	12	14	16	18	20	Avg.
0.75	0	2	4	10	12	15	19	29	28	32	36	17
0.70	0	2	4	9	16	18	27	30	33	38	42	20
0.65	0	3	9	20	24	27	30	33	41	45	50	26

0.75,0.70,0.65) at different instants of time starting from t= 0 sec to 20 sec. Initially the malicious node shows some available no. of hops to mislead the other nodes. But, as the times increases from t=0 to t=20 seconds, the available no. of hops for non-trusted nodes decreases continuously for each threshold value and becomes Zero at t=20. This is due to their misbehaviour in the interactions. Hops reading at each instant of time for different values of threshold shows that available number of hops is comparatively less for higher threshold values. for e.g. at t=14, hops available for θ=0.65 is 0.11, which decreases for θ=0.70 i.e. 0.13 and further decreases for θ=0.75 i.e. 0.06. The growth of average available hops is higher i.e. 0.438 when θ is less (θ=0.65) and smallest according to the equation during the strict policy θ=0.75. This discussion concludes that the growth of average available hops is higher when θ is less (θ=0.65) and smallest during the strict policy but the value is almost negligible in both cases.

4.3.5. Trust Dynamics. Trust dynamic of a node shows the trust worthiness of nodes. The trust dynamics changes dynamically after completion of each interaction. The trust value varies between 0 to 1. Figure 4.3.5 shows the combined graph of trust dynamics for trusted as well as abnormal nodes. The result depicts that the trust values of trusted nodes are continually increasing with time and that of abnormal node is gracefully decreasing with passage of time.

Every successful interaction contributes further increase in the trust value of trusted node. The reduction in trust value of malicious node is due to its misbehaviour. Initially there is not much difference in the trust dynamics of normal and abnormal node but as the time increases and more events are encountered the difference increases to great extent that helps in clearly separating the abnormal nodes from normal nodes and discarding them.

5. Conclusion and Future Scope. Modelling trust in IoV network is quite challenging. This paper presents various challenges faced by researchers in modelling trust for IOV network and the characteristics of the trust model. Additionally, we have proposed probability-based hybrid trust model that is combination of entity based and data-based trust models. The entity-based trustworthiness is evaluated by using pre-set threshold policy and data- based trustworthiness is evaluated by collecting the statistics during communication. The model used joint probability distribution to separate the malicious and trust nodes. If the measure statistics lies in the range of mean plus/minus twice of standard deviation then it is considered as trusted otherwise untrusted. The model also resolves the cold start problem by providing initial trust value to each node. The analytic evaluation of proposed model shows the model is scalable and involves fast and distributed trust

TABLE 4.5
Number of hops available for non-trusted nodes at different threshold

θ\Time	0	2	4	6	8	10	12	14	16	18	20	Avg.
0.75	1.06	0.95	0.45	0.32	0.21	0.14	0.10	0.06	0.03	0.00	0.00	0.226
0.70	1.55	1.39	1.07	0.62	0.44	0.29	0.19	0.13	0.06	0.04	0.00	0.423
0.65	1.8	1.64	1.00	0.67	0.49	0.23	0.17	0.11	0.05	0.02	0.00	0.438

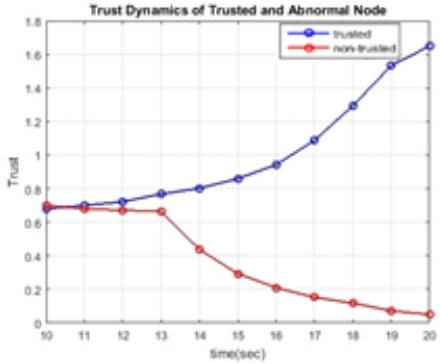

FIG. 4.4. *Trust dynamics trusted and non-trusted nodes wrt time*

computations, so is well suited for IoV. The experimental results for proposed model depict that PDR of trusted node is 0.63 that is much higher than the PDR of malicious node that is 0.15. Additionally, the average number of available hops, and trust value of trusted nodes are also significantly higher than that of non-trusted node. Thus, the malicious nodes can be clearly identified and discarded on the basic of value of PDR, available hops and Trust dynamics. The effects of threshold on evaluation metrics shows PDR and available number of nodes for both trusted and non-trusted nodes decrease with increase in threshold (θ). But this decrease is less significant in non-trusted nodes.

In future, the work might be extended to investigate the following aspects:

1. The current model secures the traffic information exchanged between vehicles. This model might be extended to secure the data transactions in other application scenarios of IoV network.
2. In proposed model, a vehicle and its driver are considered as a single node. Our model might be extended to identify the malicious behaviours of drivers and vehicles separately and discard it.
3. The proposed system might be extended by using better techniques to improve the robustness of the model.
4. In this paper, we present a separate approach to evaluate the trustworthiness of entity and data. A single approach might be used to compute the trustworthiness of both data as well as entity to make the computation much faster than that in this model.

REFERENCES

[1] O. KAIWARTYA ET AL., Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects, IEEE Access, vol. 4, pp. 5356–5373, 2016.
[2] L. ANGELES AND L. ANGELES, Internet of Vehicles?: From Intelligent Grid to Autonomous Cars and Vehicular Clouds, IEEE World Forum Internet Things, pp. 241–246, 2014.
[3] A. EL BEKKALI, M. BOULMALF, M. ESSAAIDI, AND G. MEZZOUR, Securing the Internet of Things (IoT), Proc. - 2018 Int. Conf. Wirel. Networks Mob. Commun. WINCOM 2018, vol. 44, pp. 51–58, 2019.
[4] L. M. ANG, K. P. SENG, G. K. IJEMARU, AND A. M. ZUNGERU, Deployment of IoV for Smart Cities: Applications, Architecture, and Challenges, IEEE Access, vol. 7, pp. 6473–6492, 2019.
[5] R. SILVA AND R. IQBAL, Ethical Implications of Social Internet of Vehicles Systems, IEEE Internet Things J., vol. 6, no. 1, pp. 517–531, 2019.
[6] K. ZAIDI AND M. RAJARAJAN, Vehicular internet: Security & privacy challenges and opportunities, Futur. Internet, vol. 7, no. 3, pp. 257–275, 2015.

[7] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, Trust management in social Internet of vehicles?: Factors , challenges , blockchain , and fog solutions, Int. J. Distrib. Sens. Networks, vol. 15, no. 1, 2019.
[8] D. D. K. Nigahat, A review of blackhole attack in mobile adhoc network, Int. J. Eng. Sci. Res. Technol., vol. 6, no. 4, pp. 314–319, 2017.
[9] S. Mandala, K. Jenni, M. A. Ngadi, M. Kamat, and Y. Coulibaly, Quantifying the severity of blackhole attack in wireless mobile Adhoc networks, Commun. Comput. Inf. Sci., vol. 467, pp. 57–67, 2014.
[10] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, A Categorized Trust-Based Message Reporting Scheme for VANETs, Commun. Comput. Inf. Sci., vol. 381 CCIS, no. 5, pp. 65–83, 2013.
[11] N. Bismeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters, IEEE Veh. Netw. Conf. VNC, pp. 78–85, 2012.
[12] Y. M. Chen and Y. C. Wei, A beacon-based trust management system for enhancing user centric location privacy in VANETs, J. Commun. Networks, vol. 15, no. 2, pp. 153–163, 2013.
[13] J. Finnson, J. Zhang, T. Tran, U. M. Farooq, and R. Cohen, A framework for modeling trustworthiness of users in mobile vehicular ad-hoc networks and its validation through simulated traffic flow, in springer book series Lecture Notes on Computer Science, 2012.
[14] F. Gómez Mármol and G. Martínez Pérez, TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks, J. Netw. Comput. Appl., vol. 35, no. 3, pp. 934–941, 2012.
[15] F. Gai, J. Zhang, Z. Peidong, and X. Jiang, Ratee-Based Trust Management System for Internet of Vehicles, in Part of the Lecture Notes in Computer Science Springer book series, springer, 2017.
[16] F. Gai, J. Zhang, P. Zhu, and X. Jiang, Trust on the Ratee?: A Trust Management System for Social Internet of Vehicles, Wirel. Commun. Mob. Comput., vol. 2017, 2017.
[17] G. Wang and Y. Wu, BIBRM: A Bayesian Inference Based Road Message Trust Model in Vehicular Ad Hoc Networks, in IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014.
[18] A. Shrivastava, K. Sharma, and B. K. Chaurasia, HMM for Reaputation Computation in VANET, in IEEE International Conference on Computing, Communication and Automation (ICCCA2016), 2016, pp. 667–670.
[19] Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang, A Reputation-Based Announcement Scheme for VANETs, in IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, 2012, vol. 61, no. 9, pp. 4095–4108.
[20] S. A. Soleymani et al., A Secure Trust Model based on Fuzzy Logic in Vehicular Ad Hoc Networks with Fog Computing, in IEEE., 2017, vol. 3536, no. c, pp. 1–10.
[21] X. Yao, X. Zhang, H. Ning, and P. Li, Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks, vol. 55, pp. 107–118, 2016.
[22] C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, A trust model for vehicular network-based incident reports, in IEEE 5th International Symposium on Wireless Vehicular Communications, WiVeC 2013, 2013.
[23] S. Yang, Z. Liu, J. Li, S. Wang, and F. Yang, Anomaly detection for internet of vehicles: A trust management scheme with affinity propagation, Mob. Inf. Syst., vol. 2016, 2016.
[24] Y.-M. C. Yu-Chih Wei, Reliability and Efficiency Improvement for Trust Management Model in VANETs, in Human Centric Technology and Service in Smart Space, springer, 2012, pp. 105–112.
[25] J. Zhang, Trust Management for VANETs: Challenges, Desired Properties and Future Directions, Int. J. Distrib. Syst. Technol., pp. 48–62, 2012.

Edited by: Anand Nayyar
Received: Apr 26, 2020
Accepted: May 13, 2020