NB-FTBM Model for Entity Trust Evaluation in Vehicular Ad Hoc Network Security

S. Sumithra(✉) and R. Vadivel

Department of Information Technology, Bharathiar University, Coimbatore, India
sumiphdit@gmail.com, rvadivelit@buc.edu.in

Abstract. Vehicular Ad hoc network (VANET) is developed for exchanging valuable information among vehicles. Therefore they need to ensure the reliability of the vehicle which is sending data. Trustworthiness could be achieved based on two methods. The first method is creating entity trust and the second one is data trust. This research focuses on evaluating the trustworthiness of the sender entity (vehicle). This paper proposes NB-FTBM: Naive Bayesian Fuzzy Trust Boundary Model to find entity trust. NB-FTBM contains two modules namely Entity Identification (E-ID) and Entity Reputation (E-RP). The proposed model quickly identifies the entity identification score and entity reputation score of an entity. These scores fall under the trust boundary line. Based on this boundary level the entity is allowed to take the necessary decision for the information received. The main advantage of this approach is it takes the benefit of Naive Bayesian classifier along with fuzzy logic. The proposed trust model evaluates the trustworthiness of the metrics accurately.

Keywords: NB-Naive Bayesian · E-ID Entity Identification · E-RP Entity Reputation · Trust boundary · Fuzzy inference · FTB-Fuzzy Trust Boundary

1 Introduction

Vehicular Ad Hoc Network is a subclass of mobile Ad Hoc Networks (MANET). Participating vehicles, On-board Units (OBU) and Roadside Units (RSUs) are the VANET components. On-Board Units are responsible for the interaction between the vehicles [1]. VANET works on different architectures namely (i) Vehicle-to-Vehicle communication (V2V): In V2V architecture vehicle communicates only with other vehicles on the absence of roadside infrastructure. (ii) Vehicle-to-Infrastructure (V2I): In V2I architecture vehicles have to communicate with RSUs for information. RSUs are pre-build access pointers that provide necessary information [2]. (iii) Combined architecture: In combined architecture VANET nodes (vehicles) could communicate with both RSUs and other vehicles [3]. Even though

N. Kumar and R. Venkatesha Prasad (Eds.): UBICNET 2019, LNICST 276, pp. 173–187, 2019.
https://doi.org/10.1007/978-3-030-20615-4_13

VANET is a rapidly developing technology it is lacking in providing security [4]. How a vehicle could simply trust another vehicle which is sending some data about the traffic environment? Several security attacks are encountered in VANET. Illusion attack is one of the risky attacks. The attacker creates an illusion of a vehicle and pretends as a good vehicle to spread false information [5]. The victim vehicle believes the information without any condition. Thus based on the rumor data the victim vehicle takes a decision. As the result, the attacker's vehicle creates collision [6]. To avoid such an attack, VANET researchers have proposed several methods, but they still face many limitations. VANET scenario is very much complicated that raise several issues like dynamic network change and heterogeneous traffic environment. On considering these issues, reliability among the entities is achieved by creating trust value for each entity [7]. Key management and cryptographer techniques were former mechanisms established to provide security and trust among VANET nodes. Game theory based approaches worked well [8]. But due to the ephemeral nature of VANET, they fail in certain scenarios. Calculating the reputation score of an entity that is established based on the observations of the historical interactions of the vehicles. Trust management: In VANET, trust is defined as the belief of one node having with another node [9]. Trust management is the main method to ensure the trusted relationship between the vehicles in determining whether the traffic event reported by the sender vehicle is really happening or not. This method is also used to prevent false traffic warning message spreading. Comparing to other wireless networks, trust management is more complex in VANET.

The novelty of this research work is making use of two significant methodologies namely Naive Bayesian theorem and fuzzy logic. The Naive Bayesian theorem works with the independence assumptions between predictors. This theorem assumes the effect of the result by the predictor (X) on a given data-set (C) which is independent from the results of other predictors. Naive is also known as a conditional theorem. This is used for finding the trustworthiness of the evidence of an event. This method gives a clear view of how much we should trust a message coming from a strange vehicle [10].

The statistics and measurements of fuzzy based trust model in Vehicular Ad Hoc networks contain critical characteristics such as trustworthiness assessment for decisions given by a vehicle [11]. To overcome these entire issue, trust model developed based on the fuzzy logic mechanisms will be an effective solution. The development process of trust models lies on properties of trust metrics and various trust models [12]. On receiving incoming messages using an antenna which is fixed in RSUs and other vehicles, could gather input to the application system. Fuzzy based trust model uses the terms like low, high and medium. The final result or outcome of the trust model is the relationship between the data input to be gathered and only two possible values are obtained which are yes/no. Fuzzy logic are based on 'IF-Then' reasoning. The final outcome is expanded by considering each and every parameter that depends on application system type. Example: speed and distance between the vehicles.

Contribution of the Research. As the contribution, we propose an NB-FTBM approach which is based on Naive Bayesian classifier and fuzzy logic. This methodology is separated into three phases namely ETM-Entity Trust Model, FTBM-Fuzzy Trust Boundary Model, and Naive Bayesian Decision making model. The novelty of this research work is combing two significant machine learning techniques to achieve accuracy. The proposed method is enhanced from existing method in time and accuracy management. All the existing methodologies do not concentrate on the time constraint in VANET. The fraction of second could cause enormous damage in Vehicular Ad Hoc Network. The proposed method gives an effective solution by using fuzzy logic and Naive Bayesian classifier.

The paper is organized as follows. Section 2 reviews the challenges faced by VANET, security issues, applications and related methodologies for the security of VANET. Entity Trust Model (ETM) module is presented in Sect. 3. Section 4 reveals the Fuzzy Trust Boundary Model (FTBM). In Sect. 5, the decision making of NB-FTBM is presented. Performance Evaluation of the overall simulation is shown in Sect. 6.

2 Related Work

Since vehicular Ad hoc network is a high mobility based network, it is very complicated in nature. VANET nodes (vehicles) are always movable and rarely stable. Due to this complex feature, security is very important for VANET [12]. Network topology changes frequently. Golle et al. present an approach which aims to address the limitation of detecting and correcting malicious data in vehicular Ad Hoc network [13]. The key concept of the model of their approach is in maintaining a model of VANET at every node [14]. This approach contains all the knowledge that a vehicle has about VANET. Receiving message can then be evaluated the agent's model of VANET. When the entire message received and agrees with high probability, then the vehicle accepts the trustworthiness of message [15]. In case of incoming data, that is not convenient with the model, the vehicles rely on an empirical that tries to restore the consistency through finding the easiest possible and different ranks of trustworthiness [16]. The event message that consists with highest trust score is then accepted by the vehicle. The major strength of this mechanism is that provides tight security against unwanted messages. This may spread malicious data and collapse the network [17]. In opposite to the traditional point of view of entity-centric trust, Raya et al. proposed a new method. Trust metrics depend on the attributes associated with the vehicles. Bayesian inference and DSF-Dempster Shafer Theory tells about evaluating the various shreds of evidence regarding an event. Lin et al. [18] have analyzed the benefits obtained by self-interesting vehicles in vehicular network. This model considers the scenario where vehicles can achieve congestion data from other vehicles through gossiping. This way is more appropriated in ephemeral ad hoc networks. Data level trust evaluation deals with establishing the trustworthiness of the message reported by the entities instead of the entity trust [19]. This model defines various trust parameters which categories the

trust relationships for vehicles [20]. There are two different behaviors of vehicles. First one is, vehicles want to maximize their own utility and the second one is, vehicles cause disorder in the network. This is one of the main security threat formed in VANET. The authors realized these issues which resulted in highly complexity and potentially more damaging situations that arise in VANET. These authors also identified the importance to establish trust in VANETs through reputation mechanisms [21]. This is the main module in the proposed work. Regarding security issues in VANET, several authors have studied the security challenges [22,23]. Patwardhan et al. The author [9] developed a reputation based system in order to discover the reliability and accuracy of data accumulated in a distributed manner, pushes devices too quickly adapt the changing conditions. The entity trust model focuses on evaluating the trustworthiness of vehicles with the aim of measuring their daily behavior and selfishness or malicious vehicles to make sure the reliable dissemination of messages among the vehicles [24,25]. The existing entity-centric based trust models compute reputation or trust values based on the trust metrics [26]. Trust metrics are the parameters that tell about the reputation and trust score of the vehicle. The recommendation given by another vehicle is also taken into account [27]. This approach sometimes spreads false recommendations. This approach otherwise called direct trust.

3 Entity Trust Model (ETM)

The proposed work mainly focuses on the entity-centric trust. Entity-centric trust models focus on the trustworthiness of the vehicles. To achieve this, the entity trust model needs sufficient information about the vehicle which is sending data. In the proposed work entity trust is obtained by analyzing two submodules. The identity of the vehicle and the reputation of the vehicle and they are represented as E-ID and E-RP respectively. The block of the data received contains the necessary parameters that are used for measuring the entity trust value. NB-FTBM model has stronger robustness because it adapts more than one framework for calculating trust.

3.1 Entity Identification (E-ID) Module

Entity identification is the submodule of the entity trust model. The proposed model focuses on calculating the trustworthiness of the sender vehicle (S_v). When the receiver vehicle (R_v) receives the block of information it starts analyzing for entity identification (E-ID). E-ID contains the following trust parameters.

The Distance Between S_v and R_v. Inter-vehicle distance (D) is the distance between transmitter and receiver vehicles. Each and every vehicle in VANET should compute the distance of it and neighbor vehicle based on velocity and propagation delay. Vehicles are equipped with GPS (Global positioning system) which is a transceiver that obtains positional data (Longitude, and Latitude) and direction. The proposed work makes use of the Haversine formula for obtaining the distance between S_v and R_v. The Haversine formula is used to determine the

great circle distance between two points on a sphere providing their longitude and latitude. These values are given by GPS receiver in the form of degrees, minutes and seconds. The Haversine distance formula is given below:

LON_v is the longitude of the vehicle at one point denoted as α.
$\Delta\alpha$ is the difference between $\alpha 1$ and $\alpha 2$

$$\Delta\alpha = \alpha 2 - \alpha 1 \tag{1}$$

LAT_v is the latitude of the vehicle at one point denoted as β.
$\Delta\beta$ is the difference between $\beta 1$ and $\beta 2$

$$\Delta\beta = \beta 1 - \beta 2 \tag{2}$$

$$A = (sin(\Delta\beta/2)^2 + cos(\beta 1).cos(\beta 2).sin(\Delta\alpha/2)^2) \tag{3}$$

$$C = 2.atan2(\sqrt{A}, \sqrt{1-A}) \tag{4}$$

$$D = R \times C \tag{5}$$

where R is the radius of the earth and R = 6371 km. For sender vehicle S_v, the latitude and longitude values are given by GPS, whereas for receiver vehicle R_v the latitude and longitude values are sent through the data block to the S_v.

Bearings/Direction of S_v. The direction of the vehicle is the number of degrees east or west of north or south. There are eight major directions that are commonly used. The first four directions are cardinal directions. Another four directions are. Southeast – SE, Northeast – NE, Northwest – NW, Southwest – SW. These are named as primary Inter-Cardinal directions. The combination of Cardinal and Primary Inter-Cardinal Directions are called as Bearings. Finding the bearing is reading the angle between two points.

Let R_e be the radius of the earth to get the bearing of the vehicle.
Lon_v - Longitude of the vehicle at one point and it is denoted as α.
Lat_v - Latitude of the vehicle at one point which is denoted as β.
B_v - Bearing of the vehicle which is denoted as λ.

Due to the participation of two intercommunicating vehicles, both vehicles have longitude and latitude coordinates which are denoted as ($\alpha 1$, $\alpha 2$, and $\beta 1$, $\beta 2$) respectively. Similarly Bearings for both intercommunicating vehicles denoted as ($\lambda 1$, $\lambda 2$). The following equation finds the bearing factor for S_v and R_v.

$$\lambda = atan2(X, Y) \tag{6}$$

$$X = cos\beta 2.sin\Delta\alpha \tag{7}$$

where $\Delta\alpha = \alpha 2 - \alpha 1$

$$Y = cos\beta 1.sin\beta 2 - sin\beta 1.cos\beta 2.cos\Delta\alpha \tag{8}$$

Velocity on Which S_v is Traveling. Velocity is the measure of how fast a particular vehicle is moving in a particular direction. Finding the velocity of the vehicles

gives more accurate trust results. Even though velocity details are appended along with the event message, it is necessary to find the trustworthiness of the information. Sender vehicle S_v sends the position information appended with the event message as the longitude and latitude coordinates. The receiver vehicle R_v estimates the distance of the sender vehicle S_v at the instance of propagation time. Therefore D_1 and D_2 are obtained at the time interval T_i and T_f respectively. VANET node is frequently moving in nature. Due to this feature, the distance is estimated from one point of time to another point in time. Distance traveled by S_v is denoted as $\Omega 1$.

$$\Omega = D_2 - D_1 \tag{9}$$

Now compute the velocity V_s with respect to distance traveled and propagation time.

$$V_s = \Omega(T_f - T_i) \tag{10}$$

The Average Velocity AVE_v is the speed of the vehicle traveled in a particular elapsed time.

$$AVE_v = \frac{P_f - P_i}{T_f - T_i} \tag{11}$$

where P_i = Initial position, P_f = Final position, T_i = Initial time, T_f = Final time.

3.2 Entity Reputation (E-RP) Module

Entity reputation module contains three sub parts to find the reputation value of the vehicle. Role of the vehicle tells about the type of vehicle. Recommendation of the vehicle is gathered from RSU in order to get more about the reputation. Response from other vehicles gives positive or negative reputation.

Role of the Vehicle. The role of the vehicle is generated automatically during the registration of the vehicle. Regional Transport Office (RTO) takes care of assigning the role of each vehicle and it is stored centrally. RSUs can access the centrally stored role of the vehicle. Each time the vehicle send data to another vehicle, the role detail of the vehicle is sent along with the data. The receiver vehicle should compare the received role and verify the role of the sender vehicle through RSU. There are different roles for a vehicle such as a highway patrol, ambulance, road engineering vehicles, sanitation vehicles, taxi, goods, and personal vehicles.

Recommendation from RSU. The regional transport office could control the RSUs to manage a database containing all the vehicle users with good or malicious statements. RSUs could store current data storage and processing technologies. It is assumed that every vehicle may store and manage hundreds of trust scores and recommendations equipped with a cache memory in the build.

Response from Neighbor Vehicles. To fully evaluate the reputation of the vehicle, the response from other neighbor vehicles is also considered, because the trustworthiness of an entity depends on the neighbor's reaction. The receiver vehicle R_v checks for the set of response from other vehicles.

Response from neighbor = N_R(Event). The degree of the response will be explained during trust evaluation.

4 Fuzzy Trust Boundary Model

The fuzzy mechanism is a universal approximates. Fuzzy systems are isomorphic between two algebras namely abstract algebra and linear algebra. Fuzzy logic is based on fundamental algebraic theorem called STONE-WEIERSTRASS theorem. This theorem states that every continuous function defined on a closed interval [a,b] can be uniformly approximated as closely as desired by a polynomial function. The flow of the proposed NB-FTBM approach is shown (See Fig. 1). The basic aim of this fuzzy trust model is to categorize the boundary level of the trustworthiness of the parameters. These are otherwise called fuzzy membership functions (MF). MF can hold different levels such as high, medium, low, trust or false, very good, better and poor. The fuzzy membership functions have been defined using the experts domain knowledge. To calculate the trust values of the entity parameters considered in this paper, a new mechanism is introduced namely Fuzzy Trust Boundary Model (NB-FTBM). Many degrees of membership is allowed. Membership function can be represented as:

$$MF = \mu_A(x) \tag{12}$$

This is the Membership Function associated with fuzzy set A such that the MF maps every element of the universe of discourse x to the interval [0,1].

$$\mu_A : X \rightarrow [0, 1] \tag{13}$$

The proposed NB-FTBM model uses Gaussian membership function. Gaussian MF specifies up to three parameters.

4.1 E-ID Trust Boundary

Trust Boundary for Distance and Bearing (TBDB). Algorithm 1 describes the method to find the distance and bearing of the sender vehicle.

$\mu_A(D_s)$ = Membership function of Distance.

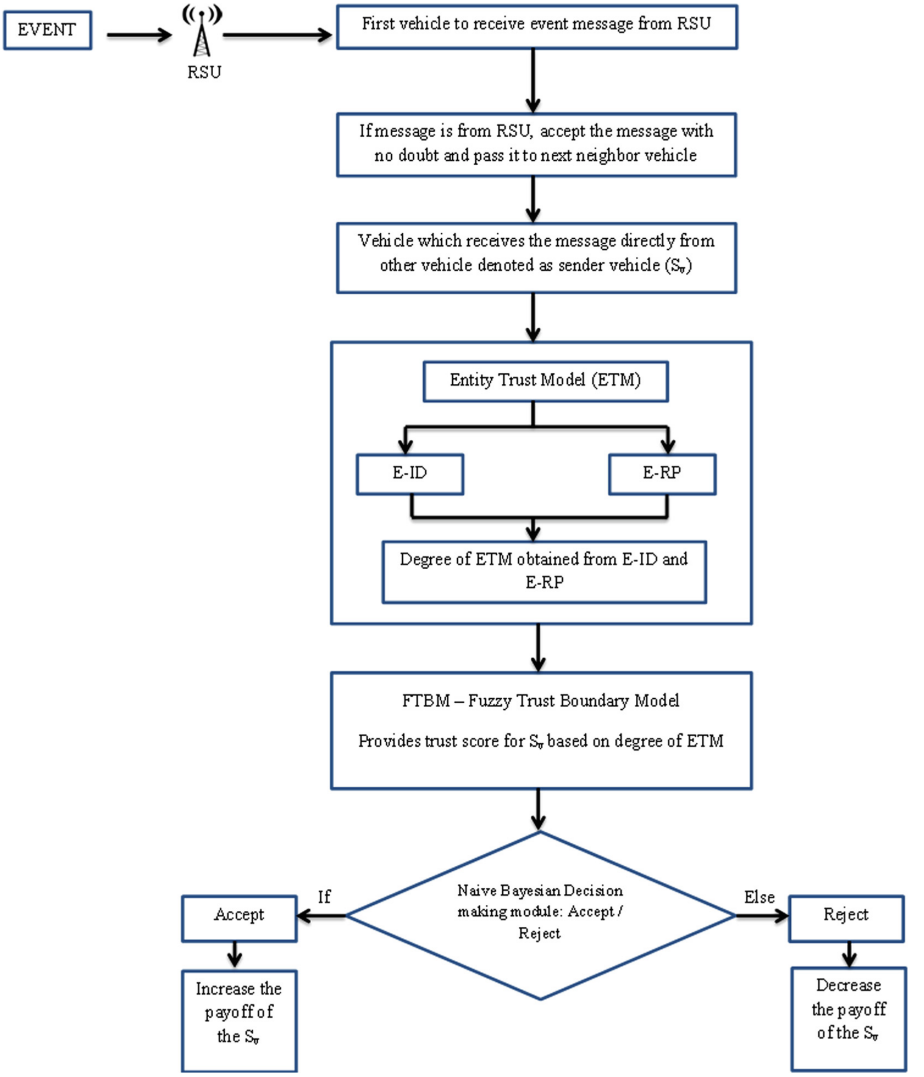

Fig. 1. NB-FTBM diagrammatic representation.

Trust Boundary for Velocity (TBV). Using the value of distance traveled, velocity is measured. By the initial position, final position and initial time, the final time of the vehicle, the average velocity is calculated. Algorithm 2 tells about the velocity of the sender vehicle.

$\mu_A(V_s)$ = Membership function of velocity.

Algorithm 1. Distance and Bearings.

Input: LON, LAT (sender and receiver), radius (earth), a, c
Output: Distance (D) of sender and receiver, Bearing (B) of sender and receiver
dLatitude ← LAT_{v2} - LAT_{v1}
dLatitude ← LON_{v2} - LON_{v1}
a ←(sin (dLatitude/2)^2) + cos(LAT_{v1}).cos (LAT_{v2}).sin(dLatitude/2)^2)
c ← 2 × atan2 ($\sqrt{a}$, $\sqrt{1-a}$)
D ← radius × c
B ← atan2 (X,Y)
X ← cos Lat 2. Sin (dLongitude)
Y ← cost Lat1 . sin Lat2 – sin Lat1 . cos Lon2 . cos (dLatitude)

Algorithm 2. Velocity.

Input: Dis_1 ← distance at initial time, Dis_2 ← distance at final time $Time_i$ ← initial time, $Time_f$ ← final time
Pos_i ← initial position, Pos_f ← final position
Output: $Velocity_s$ ← velocity of sender vehicle
Ave_v ← Average velocity
Dis_t ← Distance traveled
Dis_t ← Dis_2- Dis_1
$Velocity_s$ ← Dis_t ($Time_f$ - $Time_i$)
Ave_v ← (Pos_f - Pos_i) / ($Time_f$ - $Time_i$)

4.2 E-RP Trust Boundary

Entity reputation module contains the role of the vehicle, recommendation provided by RSU for reputation and the response from the neighbor vehicles for the event message.

The Degree of the Role (DROL). The degree of the role of the vehicle is measured in three types which are High, medium and low. The role of a vehicle is said to be a high degree if it is a highway patrol or an ambulance. The role of a vehicle is said to be a medium degree if it is a road engineering vehicle, sanitation vehicle or goods vehicle. The role of a vehicle is said to be low degree if it is a taxi or personal vehicle.

$RL_s \rightarrow$ Role of the sender vehicle.
D_R (S_v) → Degree of Role μ_A (RL_s) = Membership function of Role

$$D_R(S_v) \rightarrow \begin{cases} 1, & S_v = High \\ 0.5, & S_v = Medium \end{cases} \tag{14}$$

The Degree of Recommendation (DREC). The degree of recommendation is the reputation grade that is been given by the RSU based on the performance of the vehicle. RTO-Regional Transport Office is responsible for holding this database. To find out the trustworthiness of the vehicle this information is very much

useful. During each and every interaction between the vehicles, its payoff will increase or decrease. A good successful interaction provides increment payoff for the vehicle. An unsatisfied and failure interaction provides payoff decrements for the vehicle.

$RSU_R \in [0,1] \rightarrow$ Recommendation from RSU,
$\mu_A(RSU_R) \rightarrow$ Membership function of Recommendation from RSU.
$Rec_d(S_v) \rightarrow$ Degree of Recommendation

$$Rec_d(S_v) \rightarrow \begin{cases} 1, & S_v = Reputed \\ 0, & S_v = Non - Reputed \end{cases} \tag{15}$$

The Degree of Neighbor Response (DNR). The receiver vehicle should analyze the response of other vehicles for the same event message. The response from neighbor vehicles will bring out the actual trustworthiness of the vehicle and message. This parameter is also applicable for evaluating the trustworthiness of event data. The degree of response carries two membership function namely accepts or reject.

$N_R(Event) \rightarrow$ Response from neighbor
$\mu_A(N_R) \rightarrow$ Membership function of neighbor response

$$Res_d(N) \rightarrow \frac{Accept - Reject}{Tot_R(Event)} \tag{16}$$

where $Tot_R(Event)$ = Total number of Response for an event, Accept = Number of accepts, Reject = Number of rejects.

5 Decision making in NB-FTBM

The fuzzifier in fuzzy logic transforms the Crisp values (input values) into equal linguistic values. In NB-FTBM model the input parameters are gathered by the receiver vehicle (R_v) using the data message from the sender vehicle (S_v). The input parameters are fuzzified with the use of membership functions. The fuzzy inference engine for E-ID and E-RP is assessed. After calculating the fuzzy inference engine for E-ID and E-RP, they start to evaluate the fuzzy rules for decision making. In the proposed model the membership function of each parameter is obtained. E-ID and E-RP membership functions used to set three fuzzy rules namely high, medium and low. The final fuzzy rules are constructed based on the number of input parameters. The final fuzzy inference engine to make a decision based on the event message (See Table 1).

5.1 Naive Bayesian theorem

Table 2 provides the dataset or class for Naive Bayesian classifier. The novelty of this research work is making use of two significant methodologies namely Naive Bayesian theorem and fuzzy logic. This theorem assumes the effect of the result of the predictor (X) on a given dataset (C) is independent from the results of other predictors. Naive is also known as a conditional theorem. This is used for finding the trustworthiness of the evidence of an event. This method gives a clear view of how much we should trust a message coming from a strange vehicle.

$$P(C \mid X) = \frac{P(C \mid X)P(C)}{P(X)} \tag{17}$$

where P(Decision) = P(Accept) OR P(Reject)

According to dataset, P(Accept) = 5/9, P(Reject) = 4/9

Probability of Acceptance	Probability of Rejection
P(E-ID = High | Decision = Accept) = $\frac{3}{5}$	P(E-ID = Low | Decision = Reject) = $\frac{2}{4}$
P(E-RP = High | Decision = Accept) = 3/5	P(E-RP = Low | Decision = Reject) = 2/4
P(X | Decision = Accept) P(Decision = Accept)	P(X | Decision = Reject) P(Decision = Reject)
$\frac{3}{5} \times \frac{3}{5} \times \frac{5}{9} = 0.2$	$\frac{2}{4} \times \frac{2}{4} \times \frac{4}{9} = 0.111$

$$\text{P(X)} = \text{P(E-ID = High)} \times \text{P(E-RP = High)}$$
$$\text{P(X)} = \frac{5}{9} \times \frac{5}{9} = 0.30864$$
$$\text{P(Decision = Accept} \mid \text{X)} = 0.2/0.30864 = 0.648$$
$$\text{P(Decision = Reject} \mid \text{X)} = 0.111/0.30864 = 0.3596$$
$$0.648 > 0.3596$$

Therefore Acceptance probability is greater than Reject and the decision made is to accept the event message ad reacts.

Table 1. Fuzzy inference engine for decision making using E-ID and E-RP.

S.no	E-ID	E-RP	Decision
1	Low	Low	Reject
2	Low	Medium	Reject
3	Low	High	Accept
4	Medium	Low	Reject
5	Medium	Medium	Reject
6	Medium	High	Accept
7	High	Low	Accept
8	High	Medium	Accept
9	High	High	Accept

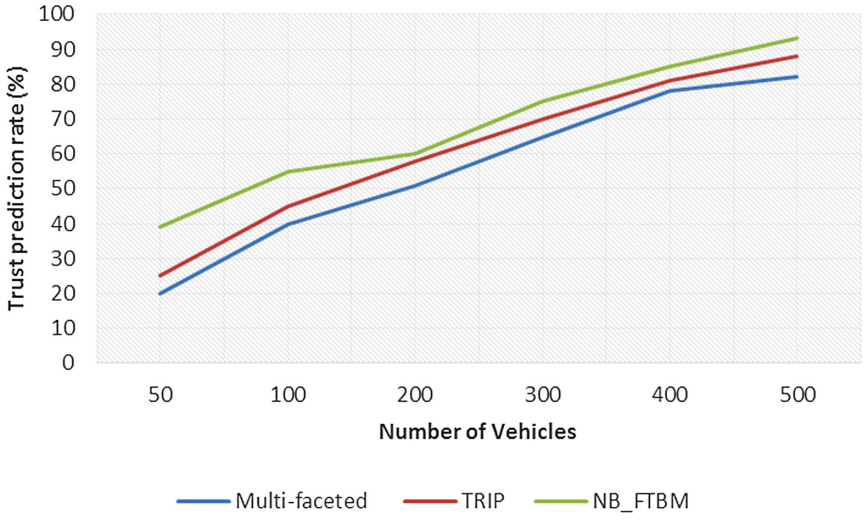

Fig. 2. The accuracy level of trust prediction

6 Performance Evaluation

To demonstrate the performance of NB-FTBM model, the following scenario is used. The proposed algorithms are implemented in network simulator 2 (NS2). The Simulation of Urban Mobility (SUMO) traffic simulator is used along with NS2. The proposed NB-FTBM model concentrates on the highway and urban scenarios. Simulation area is set up to 3 km × 3 km. the maximum speed of a vehicle is set to 100 km/h. Node density of the simulator area is 500 vehicles.

Simulation Results and Discussion. The parameters or trust metrics for evaluating the trust for an entity or vehicle are distance, bearings, velocity, recommendation from RSU, role of the vehicle and response from other vehicles. Time and Accuracy are the performance parameters to calculate the improvisation between the existing methodologies and the proposed NB-FTBM method. In the Simulation of the proposed method, we employ two main constraints. One is elapsed time for predicting trust and other one is accuracy of trust calculation. The existing approaches hardly concentrate on time and accuracy. The proposed NB-FTBM model is compared with Multifaceted and TRIP mechanisms of entity-centric trust evaluation. The simulation time is set up to 300 s. Based on the time intervals the accuracy level of trust prediction is done.

Simulation Assumptions. When a VANET node encounters a malicious node sending false information, the received information is simply discarded. The prevention mechanism is not analyzed in this paper when a node is been attacked. We assume that over 40% of vehicles are set as malicious nodes from total number of vehicles. In the first Simulation at the level of 50 vehicles in during the simulation, the multifaceted approach could reach 20% of accuracy level.

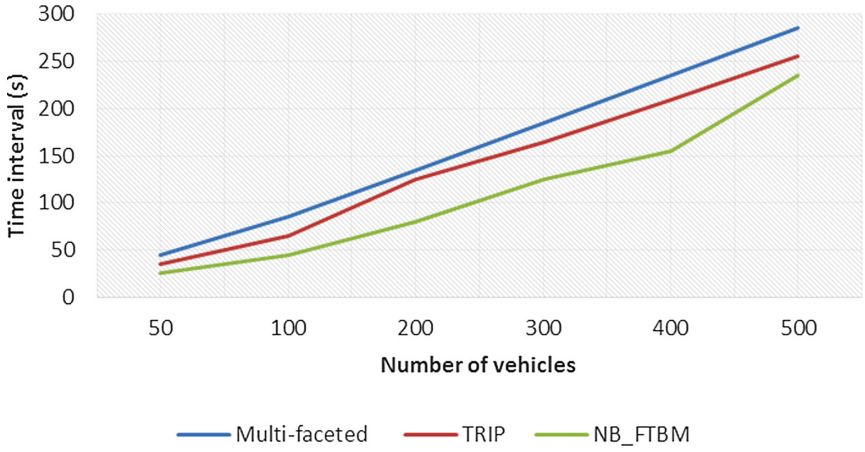

Fig. 3. Elapsed time interval

Table 2. Simulation parameters.

Parameter type	Value
Map scenario	Coimbatore (P N. Puthur to Gandhi park)
Network simulator	NS2 2.34
Traffic simulator	SUMO
Routing protocol	DHRP
Transmission range	250 m
Simulation time	300 s
Traffic density	500 vehicles
Vehicle speed	40 km/hr
Simulation area	3 km × 3 km
Packet size	512 bytes

The TRIP model could achieve 25% of accuracy level. The proposed model achieves 40% of accuracy level of trust prediction. At the end of simulation with 500 vehicles, NB-FTBM model achieves nearly 90% of accuracy level. (see Fig. 2). In the second Simulation, the simulation runs for 300 s. The Simulation shows how fast the trust evaluation approaches predict the trustworthiness of the entities. The x-axis shows the number of vehicles which increase according to the simulation. The y-axis shows the elapsed times which vary by seconds (see Fig. 3). As the simulations time increases, the traffic density is also increased. On comparing the elapsed time used for trust calculation the proposed method consumes less time than other two methods of entity-centric trust evaluation in VANET. The threat is entering only via vehicle to vehicle communication.

The malicious behavior from RSU is out of the research scope from this paper. The assumptions for the simulation scenario are set only for malicious vehicles or nodes. The RSUs malicious behavior rarely happens because the RSUs are handled by Government.

7 Conclusion

Naive Bayesian Fuzzy Trust Boundary Model has been proposed to evaluate the entity trust among VANET nodes. Due to the unstable nature of VANET environment, malicious behavior such as illusion attacks spread false information. NB-FTBM results in providing better security by detecting the malicious node. On comparing with TRIP method and Multifaceted method, NB-FTBM is improvised based on accuracy level of trust prediction with less elapsed time. From this research work we observed that, Vehicle identity and vehicle reputation plays a major role in providing trustworthiness among the vehicles. Trustworthiness is an essential constraint for achieving the full benefits of VANET. In future VANET researchers could use more efficient machine learning concepts for providing security. In this paper the comparison is made between elapsed time and accuracy. We could further add more comparison metrics. Malicious Attack prevention mechanism is not spoken in this paper. In future preventing malicious activity could be taken into account. Other than these thoughts and ideas, we have to ensure that the threat is not entering from RSUs.

References

1. Sharef, B.T., Alsaqour, R.A., Ismail, M.: Vehicular communication ad hoc routing protocols: a survey. J. Netw. Comput. Appl. **40**, 363–396 (2014)
2. Mehdi, M.M., Raza, I., Hussain, S.A.: A game theory based trust model for vehicular ad hoc networks (VANETs). J. Comput. Netw. **121**, 152–172 (2017)
3. Seuwou, P., Patel, D., Ubakanma, G.: Vehicular ad hoc network applications and security: a study into the economic and the legal implications. Int. J. Electr. Secur. Digit. Forensics **6**(2), 115–129 (2014)
4. Hubaux, J.P., Capkun, S.: The security and privacy of smart vehicles. IEEE Secur. Priv. Mag. **2**(3), 49–55 (2004)
5. Sumra, I.A., Hasbullah, H.B.: Trust levels of vehicular ad hoc network (VANET). Int. J. Inf. Technol. Electr. Eng. 3(5) (2014). ISSN: 2306–708X
6. Gerlach, M., Fokus, F.: Trust for vehicular applications. In: Proceedings of the 8th International Symposium on Autonomous Decentralized Systems, pp. 295–304 (2007)
7. Khainar, V.D., Kotecha, K.: Performance of vehicle-to-vehicle communication using IEEE 802.11p in vehicular ad hoc network environment. Int. J. Netw. Secur. Appl. **5**(2), 143–170 (2013)
8. Sharmaa, V., Srinivasan, K., Chaoc, H.-C., Huag, K.-L., Cheng, W.-H.: Intelligent deployment of UAVs in 5G heterogeneous communication environment for improved coverage. J. Netw. Comput. Appl. **85**, 94–105 (2017)
9. Pham, T.N.D., Yeo, C.K.: Adaptive trust and privacy management framework for vehicular networks. Veh. Commun. **13**, 1–12 (2018)

10. Karagiannis, D., Argyriou, A.: Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning. Veh. Commun. **13**, 56–63 (2018)
11. Jalalia, M., Aghaee, N.G.: A fuzzy reputation system in vehicular ad hoc networks. Procedia Comput. Sci. **5**, 951–956 (2011)
12. Regan, K., Poupart, P., Cohen, R.: Bayesian reputation modeling in e-marketing places sensitive to subjective, deception and change. In: Proceedings in the 21st Conference. Artificial Intelligence, pp. 1206–1212 (2006)
13. Li, X., Liu, J., Li, X.: RGTE: a reputation based global trust establishment in VANETs. In: IEEE 5th International Conference (2013)
14. Ma, S., Wolfson, O., Lin, J.: A survey on trust management for intelligent transportation system. In: IWCTS', November 2011
15. Raya, M., Papadimitrator, P., Gligor, V., Hubaux, J.: On data-centric trust establishment in ephemeral Adhoc networks. In: IEEE INFOCOM 2008-The 27th Conference on Computer Communications, April 2008
16. Huynh, T., Jennings, N., Shabalt, N.: An integrated trust and reputation model for open multiagent systems. Auton. Agent. Multiagent Syst. **13**, 119–154 (2006)
17. Minhas, U.F., Zhang, J., Trans, T., Cohen, R.: Towards expanded trust management for agents in vehicular ad hoc networks. Int. J. Comput. Intell. Theor. Pract. (IJCITP) **5**(1), 3–15 (2010)
18. Chen, C., Zhang, J., Cohen, R., Ho, P.H.: A trust-based message propagation and evaluation framework in VANETs. In: Proceedings of International Conference on Information Technology Convergence and Services (2010)
19. Li, F., Wang, Y.: Routing in vehicular ad hoc networks: a survey. IEEE Veh. Technol. Mag. **2**(2), 12–22 (2007)
20. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
21. Boukerche, A., Xu, L., El-Khatib, K.: Trust-based security for wireless ad hoc and sensor networks. Comput. Commun. **30**(11–12), 2413–2427 (2007)
22. Nassar, L., Karray, F., Kamel, M.S.: VANET IR-CAS for commercial SA: information retrieval context-aware system for VANET commercial service announcement. Int. J. Intell. Transp. Syst. **13**(1), 37–49 (2015)
23. Wang, S., Yao, N.: LIAP: a local identity-based anonymous message authentication protocol in VANETs. Comput. Commun. **112**, 154–164 (2017)
24. Shaikh, R.A.: Fuzzy risk-based decision method for vehicular ad hoc networks. Int. J. Adv. Comput. Sci. Appl. **7**(9), 54–62 (2016)
25. Liu, Z., Ma, J., Jiang, Z., et al.: LSOT: a lightweight self-organized trust model in VANETs. J. Mob. Inf. Syst. **2016**, 1–15 (2016). Article id 7628231
26. Harika, E., Satyananda Reddy, C.: A trust management scheme for securing transport networks. Int. J. Comput. Appl. **180**(8), 38–42 (2017)
27. Chen, Y.M., Wei, Y.C.: A beacon-based trust management system for enhancing user-centric location privacy in VANETs. J. Commun. Netw. **15**(2), 153–163 (2013)