International Journal of
Computer & Software Engineering

Review Article Open Access

Survey: Trust Management in VANET

Nourelimane Bousmaha[1], Mohamed Maachaoui[2] and Rachid Chelouah[1,*]

University of Paris- Seine, ETIS laboratory, CNRS UMR8051, France
University of Paris- Seine, Quartz laboratory, EA 7393, France

Abstract

The Vehicular ad-hoc networks (VANET) are a subclass of MANET with vehicles as mobile nodes. The vehicles exchange data via vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication. The securities of data communications focus on deciding data trust. The concept of trust estimates the reliability of communications data. In particular, we have mainly focused on problems of mistrust or data trust in the VANET network. In this paper, we will study some models of trust and compare them, which will help to reduce the impact of trust problem and try to improve it.

Publication History:

Received: June 12, 2019
Accepted: January 20, 2020
Published: January 22, 2020

Keywords:

Vehicular Ad Hoc Networks(VANETs), Security, Trust model

Introduction

The vehicle ad hoc network (VANET) is composed of the mobile entity called vehicle and fixed entity known as Road Side Units (RSUs). The entities exchange of messages through the three modes of communication namely vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and hybrid communication [1]. The VANET intelligent applications depend on the exchange of messages between the entities source and destinations [2]. Consequently, these messages confront challenges evaluation trust of the data and entity to obtain insufficient attention. To protect and preserve the system from of these various attacks and the entities which commit it. The most common attacks in VANET are: Sybil attack, Newcomer attack, Black-hole attack, etc [3].

The security of the communication concentrates about trust in data exchange during communication, which is based on the concept of trust model to improve the security of communication. These trust models face some challenges must be considered against malicious vehicle that leads to the most critical and challenging security issues. The destination of the vehicle ensures that messages received come from the same source it claims. The biggest problem is that the vehicle must check the message integrity as fast as possible for avoiding the influence of real rate of data in the network. The movement of high-speed vehicles and the high density of traffic allow congestion on the road. Therefore, destination vehicles receive a lot of data but the problem of waiting for confirmation to detect falsifies the position and the actual times to respond [4-5].

The trust model permit mitigates these risks, which manage accurately trust between vehicles, used for making a decision as to follow the message or no. Working with a specific trust model it achieves security resiliency and robustness in the presence of malicious node sending false information to misguide other nodes. Trust management scheme will not allow malicious nodes to increase the trust value of untrustworthy message. The trust value obtained in the non-malicious environment will always be greater than the trust value obtained in the malicious environment [6-7].

Related Work

In this section, we will present the different trust models, which helps to ensure trust between entities and data, i.e. the reliability of messages and malicious entity blocking. These trust models can be classified into three categories of vehicle networks and listed as below: (A) entity-centric, (B) data-centric, and (C) combined.

Entity-oriented trust model

In this approach, we describe the models that are based on the reliability of the entity (vehicle), which is based on obtaining information about the sender and neighbor receivers. However, the change of vehicle position allows frequent interruptions, which makes difficult to have sufficient information about the neighbors.

The authors of [8] propose a VANET Dynamic Demilitarized Zone (VDDZ) trust model that uses a public key infrastructure and distributed cluster algorithm. As shown in Figure 5. The objectives of the trust model VDDZ is to exclude the entry of malicious or obscure vehicles in cluster, it prohibits using directly the communication of a cluster head (CH) with other member vehicles. This technique represents a set of registration authority (RA) vehicles located 1-hop away from the certification authority. This cluster algorithm uses two parameters:

1. The trust metric (Tm): allows calculating confidence it for each vehicle.
2. The mobility metrics: preserves security and stability of cluster head.

The Head cluster determines the trust level of vehicles in the cluster by a trust metric. The (Tm) is a continuous value between 0 and 1. Of course, new vehicles start with Tm = 0.1 and all vehicles with Tm <1 must behave well to increase their trust metric. Trusted vehicles are those with Tm = 1 [9], and this algorithm uses two types of messages:

1. The HELLO message, consisting of speed, identity, position, current status, Tm table and current neighbors.
2. BEACON ELECTION, consisting of an IP address, number of hops, relative mobility (RM) and number of trusted neighbors (NTN). Figure 1 describes a VDDZ.

[*]**Corresponding Author:** Dr. Rachid Chelouah, University of Paris- Seine, ETIS laboratory, CNRS UMR8051, France; E-mail: rc@eisti.eu

Citation: Bousmaha N, Maachaoui M, Chelouah R (2020) Survey: Trust Management in VANET. Int J Comput Softw Eng 5: 152. doi: https://doi.org/10.15344/2456-4451/2020/152

The Trust and Reputation Infrastructure-based model (TRIP) is presented in [10]. This model can detect malicious nodes that broadcast erroneous messages over the network. As shown in Figure 2, the malicious nodes are isolated by trust and reputation. Fuzzy sets [11] are sets where a member can have partial membership. This model utilizes fuzzy logic for to determine the trust values. Scores are evaluated based on three pieces of information:

1. Latest interactive experiences between the nodes,
2. The vehicles to neighbors,
3. Recommendations from other central authorities.

The confidence value of the vehicle is evaluated by three levels:

1. "TRUSTED" vehicles are accepted and their traffic warnings are broadcasted for other vehicles.
2. "+/- TRUSTED" vehicles are accepted and their messages are issued as trusted vehicles but it is not transferable.

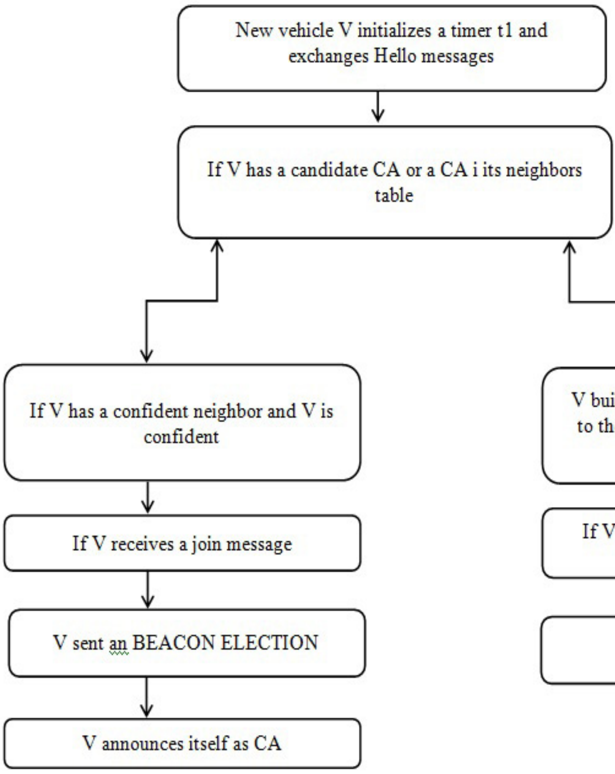
New vehicle V initializes a timer t1 and exchanges Hello messages
If V has a candidate CA or a CA i its neighbors table
If V has a confident neighbor and V is confident
If V receives a join message
V sent an BEACON ELECTION
V announces itself as CA
V builds its neighbors table according to the RM, NTN, and the number of hops
If V receives an ACCEPT message
V is member in a cluster

Figure 1: VDDZ.

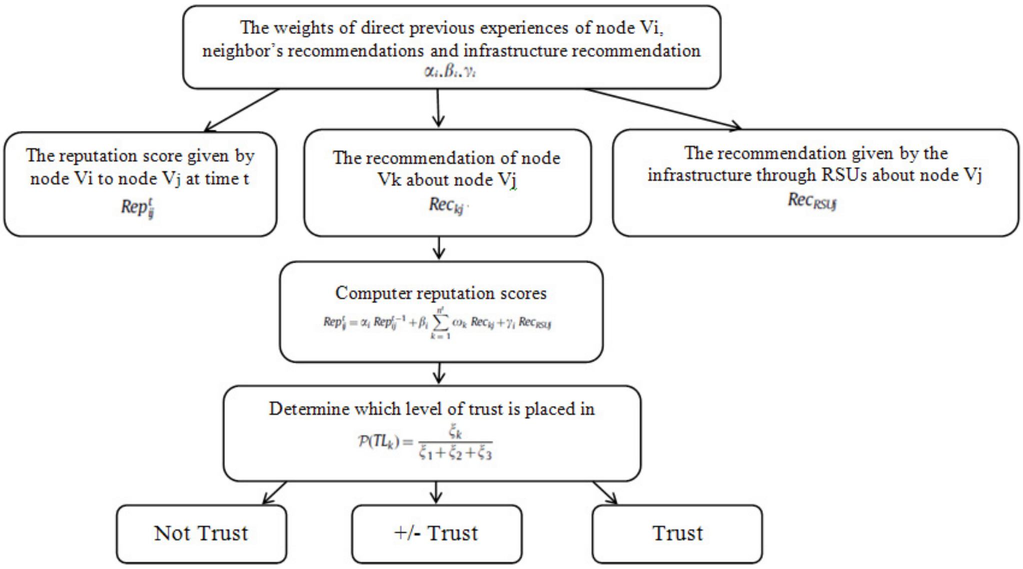
The weights of direct previous experiences of node Vi, neighbor's recommendations and infrastructure recommendation
$\alpha_i.\beta_i.\gamma_i$
The reputation score given by node Vi to node Vj at time t
Rep_{ij}^t
The recommendation of node Vk about node Vj
Rec_{kj}
The recommendation given by the infrastructure through RSUs about node Vj
Rec_{RSUj}
Computer reputation scores
$Rep_{ij}^t = \alpha_i\, Rep_{ij}^{t-1} + \beta_i \sum_{k=1}^{n'} \omega_k\, Rec_{kj} + \gamma_i\, Rec_{RSUj}$
Determine which level of trust is placed in
$\mathcal{P}(TL_k) = \frac{\xi_k}{\xi_1+\xi_2+\xi_3}$
Not Trust
+/- Trust
Trust

Figure 2: TRIP.

3. "NOT TRUSTED" vehicles are rejected and their messages warn the presence of a malicious vehicle

Zhouw et al. [12], proposed a Dynamic Trust Token (DTT) mechanism that focuses on finding uncooperative network nodes and ensuring the integrity of the package upon delivery. This mechanism uses symmetric and asymmetric cryptographic algorithms and Neighborhood WatchDog algorithm to protect the integrity of the packets. In this algorithm, packet monitoring increases during communication for security packet. The initiator must be trusted and the event package is right when it is generated. This packet transmits for routing to neighbors during a transmission session. Each transmission session (TS) is framed in a time interval, which increases the latency for receiving in the network. The disadvantage of this mechanism does not excite changes on malicious behavior, do not prevent malicious nodes. Figure 3 describes a DTT.

In [13], the authors propose a solution called Multi-faceted Approach to Modeling Agent Trust permit the reliability of the agent to behave honest behavior. Thus, the trust of an agent is based on two parts priority-based trust and the majority-based trust. In addition, the priority based is used to select in preference between other agents/vehicles. Following this, it divided in two parts on trust based on experience-based, role-based. The role-based is basic some vehicles have high trust such as the police for to relies on the identification of agents (vehicles). Trust based on experience is used with the past interaction. The majority opinion is also used to group the selected comments. Moreover, each node calculates the trust values through previous experiences.

An agent may passively wait for other agents to report on an event. In fact, every agent contains in database, with the aim of containing list of past interaction them. But usually, the agent sends a request to a list of neighboring trusted agents to inquire. But it may be necessary to verify this information by interviewing other trusted agents. The agent must aggregate the shipper's reports and the officer will decide whether to believe a particular report and take the corresponding action. Figure 4 shows Multi-faceted.

Jorgeh et al. propose in [14] the trust establishment that utilizes watchdog algorithm with intrusion detection techniques. The watchdog technique can be described to detect routing perturbation attacks in ad hoc networks. It aims to guarantee protocol independent, and a useful instrument for intrusion detections in ad hoc networks.

The objective of the watchdog is to monitor packets in order to take into consideration routing rule. The watchdog of a particular node transmits data to the node's neighbors in order to observe the routing protocols. The watchdog computes all the received packets for defining a node that exhibits a malicious behavior. A neighbor trust determines the received packets for forwarding and those effectively forwarded by the neighbor node. Drawback of this technique is to differentiate the loss of a packet that due to an attack or a collision. Figure 5 describes a watchdog.

Data-oriented trust model

Confidence modeling is about data reliability. Data-centric trust can be termed event-based trust. This model estimates the level of

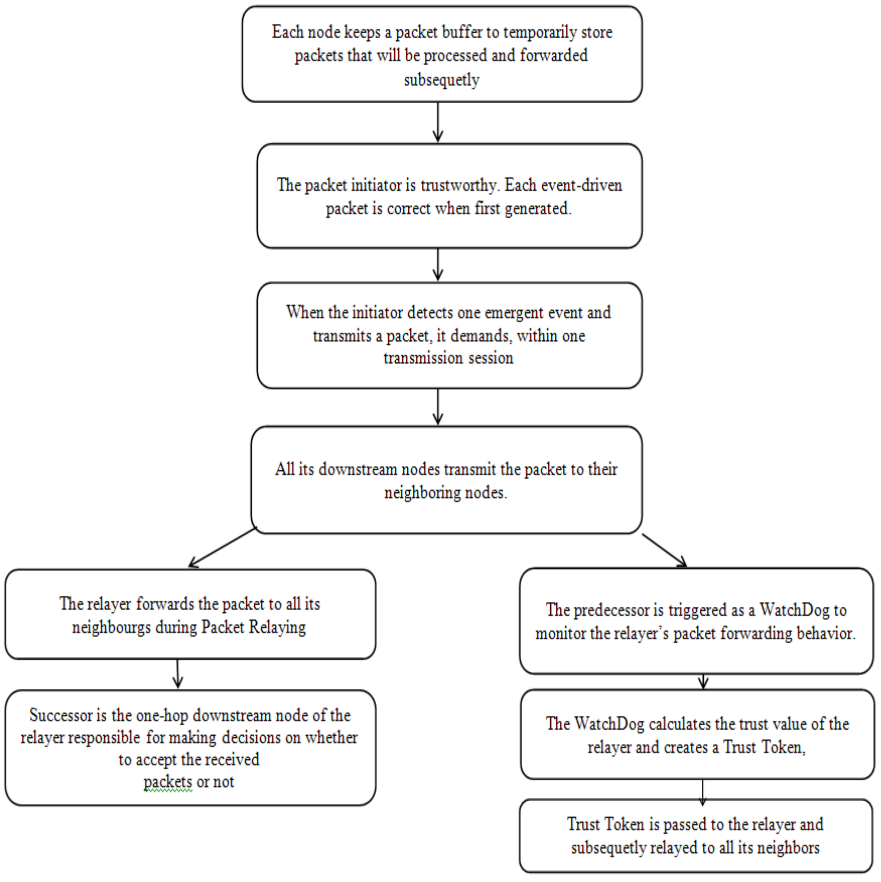
Each node keeps a packet buffer to temporarily store packets that will be processed and forwarded subsequetly
The packet initiator is trustworthy. Each event-driven packet is correct when first generated.
When the initiator detects one emergent event and transmits a packet, it demands, within one transmission session
All its downstream nodes transmit the packet to their neighboring nodes.
The relayer forwards the packet to all its neighbourgs during Packet Relaying
Successor is the one-hop downstream node of the relayer responsible for making decisions on whether to accept the received packets or not
The predecessor is triggered as a WatchDog to monitor the relayer's packet forwarding behavior.
The WatchDog calculates the trust value of the relayer and creates a Trust Token,
Trust Token is passed to the relayer and subsequetly relayed to all its neighbors

Figure 3: DTT.

trust of each sender and receiver. As a result, the high traffic density increases the amount of data, which leads to a risk of long latency for data transfer and network disconnections.

In the study [15], the authors propose a model of trust based on clustering with Ant Colony Routing (TACR), Clustering is created by the algorithm based on position, direction and velocity. There are two cases for the Cluster Head (CH) selection:

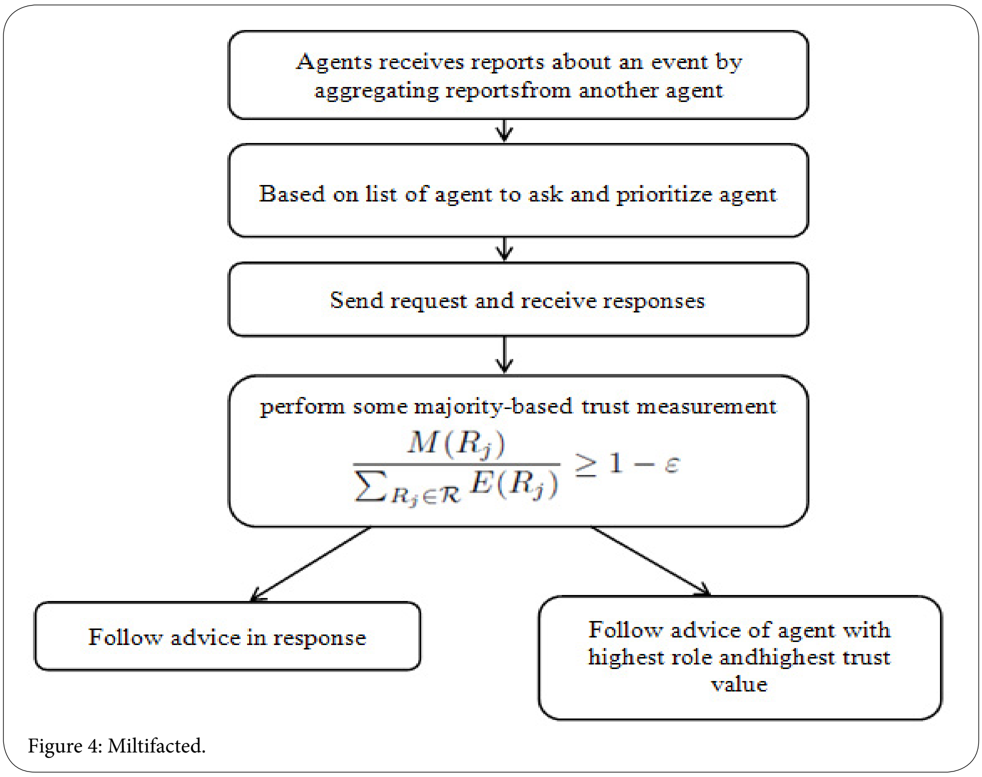
Agents receives reports about an event by aggregating reportsfrom another agent
Based on list of agent to ask and prioritize agent
Send request and receive responses
perform some majority-based trust measurement
$\frac{M(R_j)}{\sum_{R_j \in \mathcal{R}} E(R_j)} \geq 1 - \varepsilon$
Follow advice in response
Follow advice of agent with highest role andhighest trust value

Figure 4: Miltifacted.

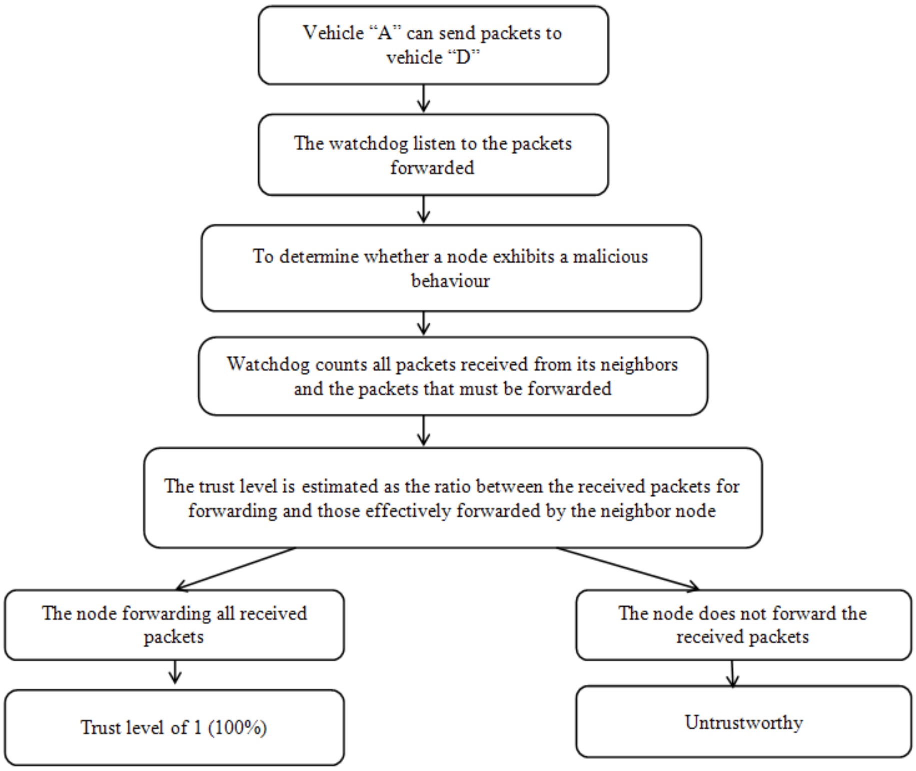
Vehicle "A" can send packets to vehicle "D"
The watchdog listen to the packets forwarded
To determine whether a node exhibits a malicious behaviour
Watchdog counts all packets received from its neighbors and the packets that must be forwarded
The trust level is estimated as the ratio between the received packets for forwarding and those effectively forwarded by the neighbor node
The node forwarding all received packets
The node does not forward the received packets
Trust level of 1 (100%)
Untrustworthy

Figure 5: Whatchdog.

1. If the RSU is present it will be chosen as CH,
2. In case if RSU is absent of, the algorithm searches and select the slowest vehicle of the cluster, as this guarantees coverage for a maximum period.

The goal of the cluster head (CH) is to guarantee the real-time dissemination of data with the value of trust between the sender and the recipient. The new vehicle starts with the normal value trust.

The trust value is calculated directly and indirectly; the direct trust is obtained for each vehicle by transactions with neighboring vehicles. It depends on several parameters: Traffic RuIe Obey (TRO), Data Packets Forwarded (DPF), Data Packet / Message Precession (DPP), Control Packet Forwarded (CPF), Control Packet / Message Precession (CPP). The indirect trust used at the Cluster-Head level to calculate the trust value of strange vehicles generates messages. Indirect trust value does not allow malicious vehicles to send messages across the network. Figure 6 describes a TACR.

The authors present in [16] a model of trust centered on the entity that allows discovering the black-hole attacks and the reliability of the data transmission. As shown in Figure 7, trust is based on three parameters: Direct trust, Recommendations and Comprehensive trust.

The value of direct trust is calculated according to the data transfer rate and the weight of the data, which must fulfill these three conditions: Traffic Safety, Traffic Efficiency and Infotainment Data, which have different impacts on the data traffic. The value of the recommendation trust is determined by the direct trust value of the source node to its neighbors and by the global trust value of other neighbors with the destination node. Comprehensive trust is a combination of two parameters of direct trust and trust recommendation that has a different impact on network nodes already in use. The direct trust will not be important the recommendation trust. The node strange is request to use the recommendation. This model builds to apply security on the GPSR routing protocol and increase the rate the transmission of success data.

The authors of [17] propose an information-driven Real-time Message Content Validation (RMCV) trust model that allows each vehicle to evaluate the reliability of a large number of messages received in VANETs. They use several factors that have a huge impact: evaluating the reliability of messages, such as content similarity, content conflicts, and similarity of the message routing path.

As shown in Figure 8, the RMCV scheme includes an information-oriented trust model; it also includes a message classification

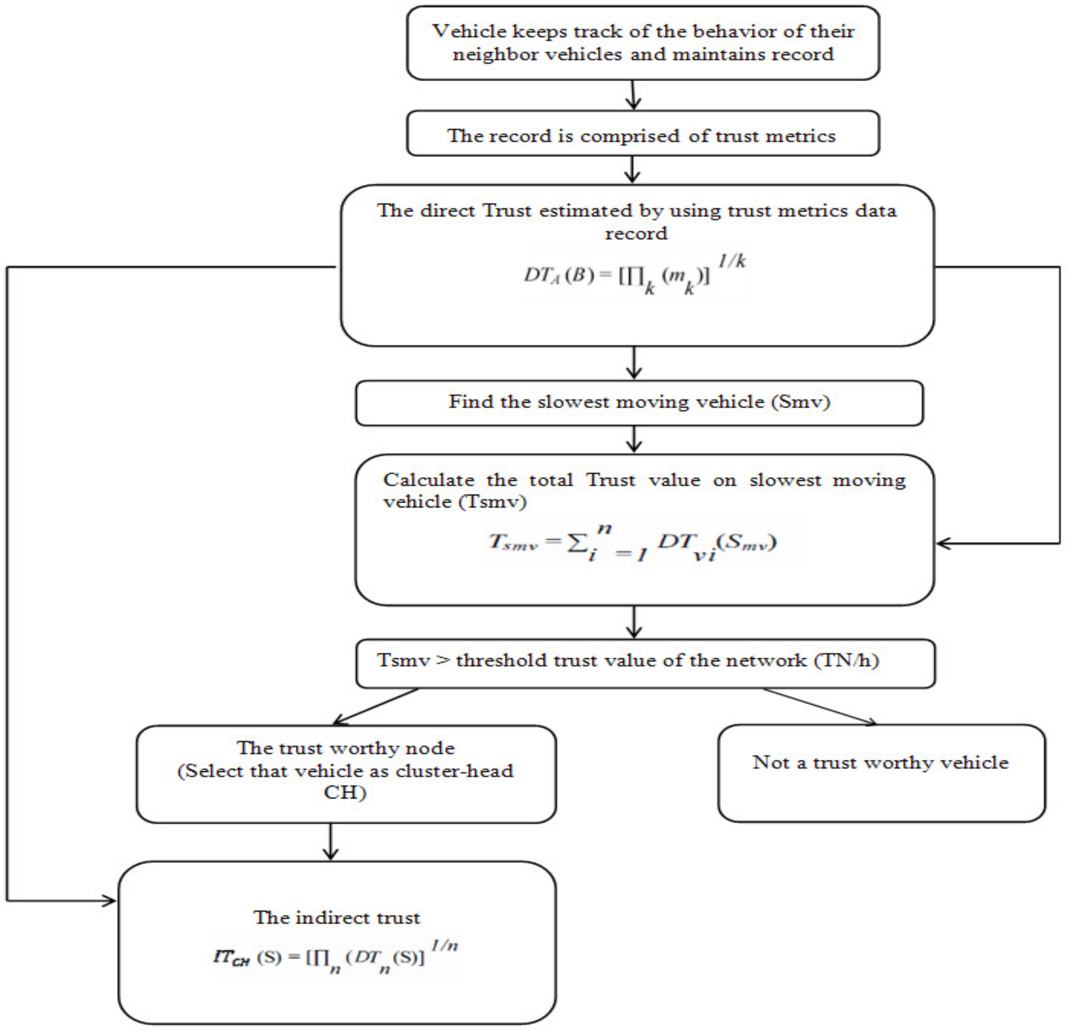
Vehicle keeps track of the behavior of their neighbor vehicles and maintains record
The record is comprised of trust metrics
The direct Trust estimated by using trust metrics data record
$DT_A(B) = [\prod_k (m_k)]^{1/k}$
Find the slowest moving vehicle (Smv)
Calculate the total Trust value on slowest moving vehicle (Tsmv)
$T_{smv} = \sum_{i=1}^{n} DT_{vi}(S_{mv})$
Tsmv > threshold trust value of the network (TN/h)
The trust worthy node (Select that vehicle as cluster-head CH)
Not a trust worthy vehicle
The indirect trust
$IT_{CH}(S) = [\prod_n (DT_n(S)]^{1/n}$

Figure 6: TACR.

component to identify messages describing the same event. The potentially high number of received messages can be grouped together using clustering algorithms. First-level clustering generates a collection of messages describing the same event based on the content. The purpose of the second level is to identify conflicting information about the same event.

The information-oriented trust model is to determine which collection should be approved. The confidence score of each message will be calculated at the level of each vehicle.

There are group of messages that are associated with the same event, similar messages are generally considered as mutually supportive group. This is an important factor in judging the reliability of a message. Modeling the effects of these two important parameters can be used to determine:

1. The maximum distance of the content between two messages in the same cluster.
2. The number of messages in the cluster.

The authors of [18] propose trust model based on identity anonymous vehicular ad hoc networks, this model also allows detecting false location and time information.

The intrusion-aware trust model is based on three phases:

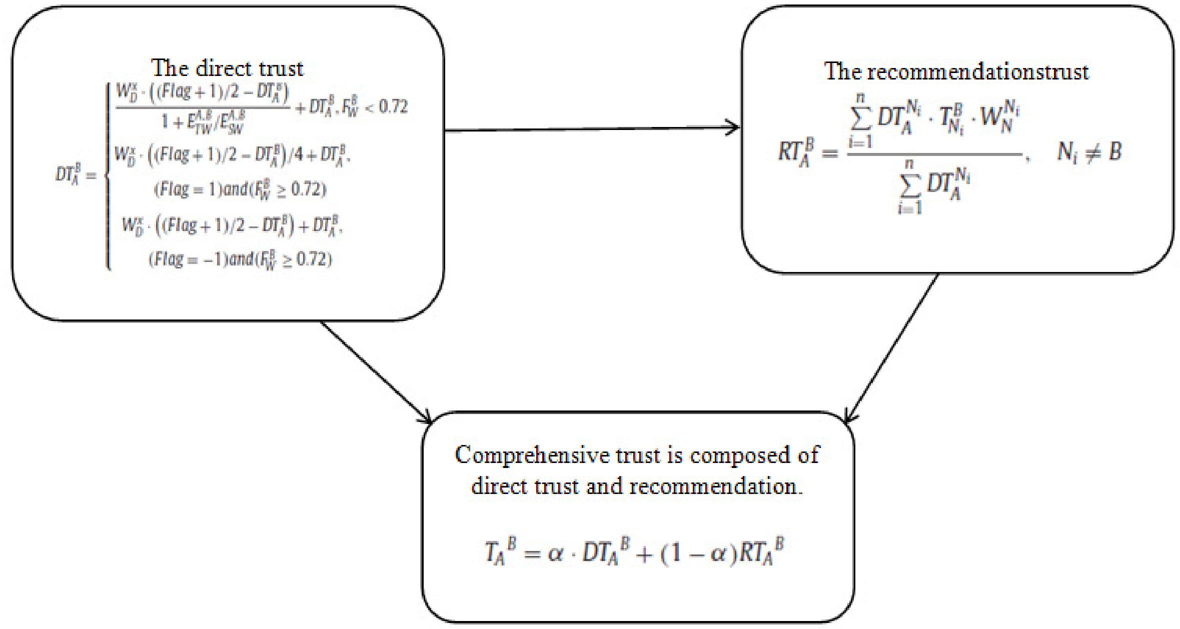
The direct trust
$DT_A^B = \begin{cases} \frac{W_D^x \cdot ((Flag+1)/2 - DT_A^B)}{1+E_{TW}^{A,B}/E_{SW}^{A,B}} + DT_A^B, F_W^B < 0.72 \\ W_D^x \cdot ((Flag+1)/2 - DT_A^B)/4 + DT_A^B, \\ (Flag=1) and (F_W^B \geq 0.72) \\ W_D^x \cdot ((Flag+1)/2 - DT_A^B) + DT_A^B, \\ (Flag=-1) and (F_W^B \geq 0.72) \end{cases}$
The recommendationstrust
$RT_A^B = \frac{\sum_{i=1}^{n} DT_A^{N_i} \cdot T_{N_i}^B \cdot W_N^{N_i}}{\sum_{i=1}^{n} DT_A^{N_i}}, \quad N_i \neq B$
Comprehensive trust is composed of direct trust and recommendation.
$T_A{}^B = \alpha \cdot DT_A{}^B + (1-\alpha) RT_A{}^B$

Figure 7: Black hole.

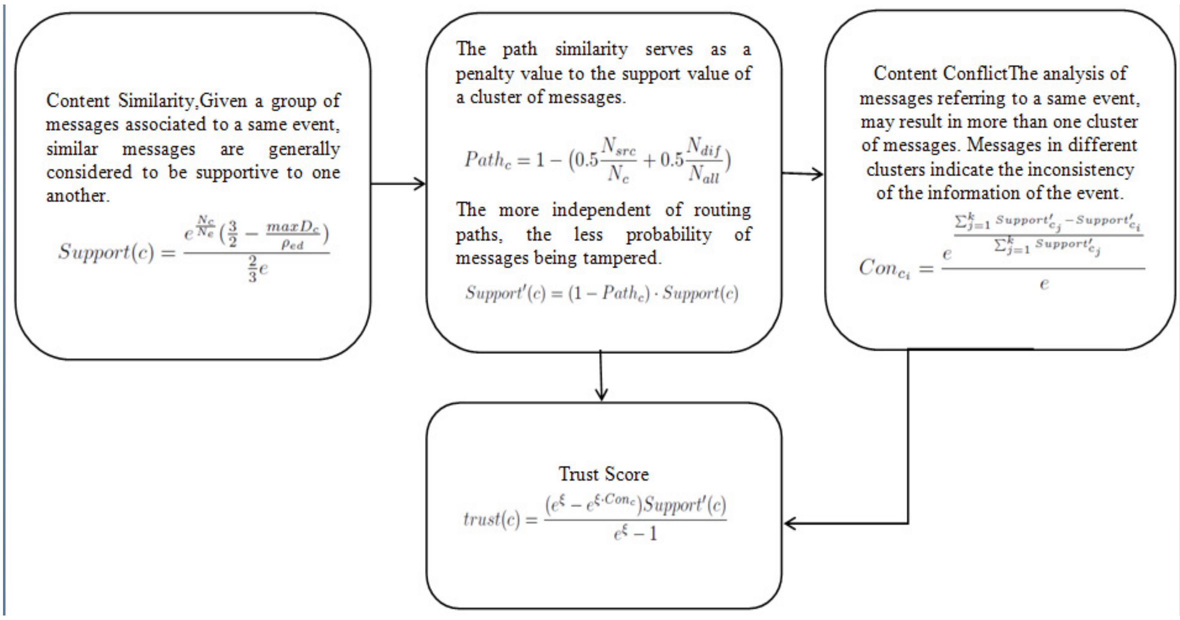
Content Similarity,Given a group of messages associated to a same event, similar messages are generally considered to be supportive to one another.
$Support(c) = \frac{e^{\frac{N_c}{N_e}}(\frac{3}{2} - \frac{maxD_c}{\rho_{ed}})}{\frac{2}{3}e}$
The path similarity serves as a penalty value to the support value of a cluster of messages.
$Path_c = 1 - (0.5\frac{N_{src}}{N_c} + 0.5\frac{N_{dif}}{N_{all}})$
The more independent of routing paths, the less probability of messages being tampered.
$Support'(c) = (1 - Path_c) \cdot Support(c)$
Content ConflictThe analysis of messages referring to a same event, may result in more than one cluster of messages. Messages in different clusters indicate the inconsistency of the information of the event.
$Con_{c_i} = \frac{e^{\frac{\sum_{j=1}^{k} Support'_{c_j} - Support'_{c_i}}{\sum_{j=1}^{k} Support'_{c_j}}}}{e}$
Trust Score
$trust(c) = \frac{(e^{\xi} - e^{\xi \cdot Con_c})Support'(c)}{e^{\xi} - 1}$

Figure 8: RMCV.

1. The first phase estimates the confidence value for every received message.
2. The second phase estimates the trust value for every single message.
3. The last phase makes the decisions on the message, mainly based on their highest trust value.

As shown in Figure 9, the trust value is measured by using the following four parameters: The location closeness, time closeness, location verification and time stamp verification.

The parameters can be calculated without knowing the source identities. The trust value is based on the total number of sender nodes and confidence value. The decision logic is based on two steps:

1. In the first step, the system takes the messages that have the highest trust value.
2. The second step, the system makes the decision to approve that message if the trust value of the selected message is greater than the minimum acceptable threshold.

In [19], the authors proposed a trust model namely Road side unit Aided Trust Establishment scheme (RATE). The RSUs has been considered to execute the trust establishment, which separatethe data-consuming vehicles from those submitting information. This model uses the Ant Colony Optimization ACO algorithm, which evaluate trustworthiness of data. The ACO main objective combines the direct observed data with feedback information.In addition; the vehicles create the observations and confidence according to the detection of an event. The estimation of the Observation Factor is based on the most recent reporting frequency of the evidence. The observation factor is calculated according to the confidence of the observer on this piece of evidence and the weight corresponding to reporter's identity. The feedback factor denotes the directory's practically verified usefulness. The management of feedback depends on three stages: initialization, aging and promotion.

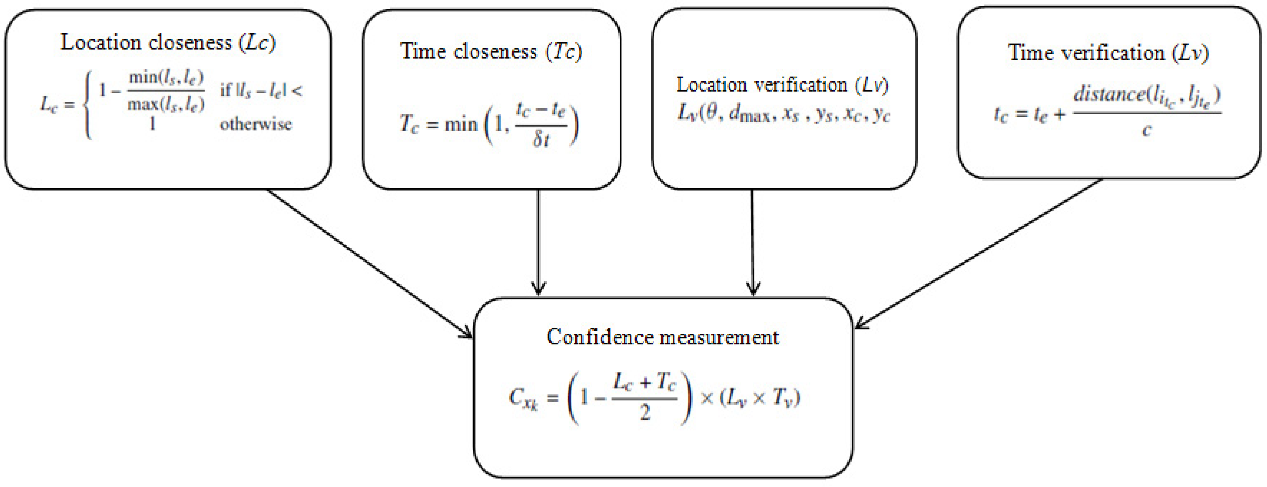
Location closeness (Lc)
$L_c = \begin{cases} 1 - \frac{\min(l_s, l_e)}{\max(l_s, l_e)} & \text{if } \|l_s - l_e\| < \\ 1 & \text{otherwise} \end{cases}$
Time closeness (Tc)
$T_c = \min\left(1, \frac{t_c - t_e}{\delta t}\right)$
Location verification (Lv)
$L_v(\theta, d_{\max}, x_s, y_s, x_c, y_c$
Time verification (Lv)
$t_c = t_e + \frac{distance(l_{i_{t_c}}, l_{j_{t_e}})}{c}$
Confidence measurement
$C_{x_k} = \left(1 - \frac{L_c + T_c}{2}\right) \times (L_v \times T_v)$

Figure 9: INTRUSION AWARE.

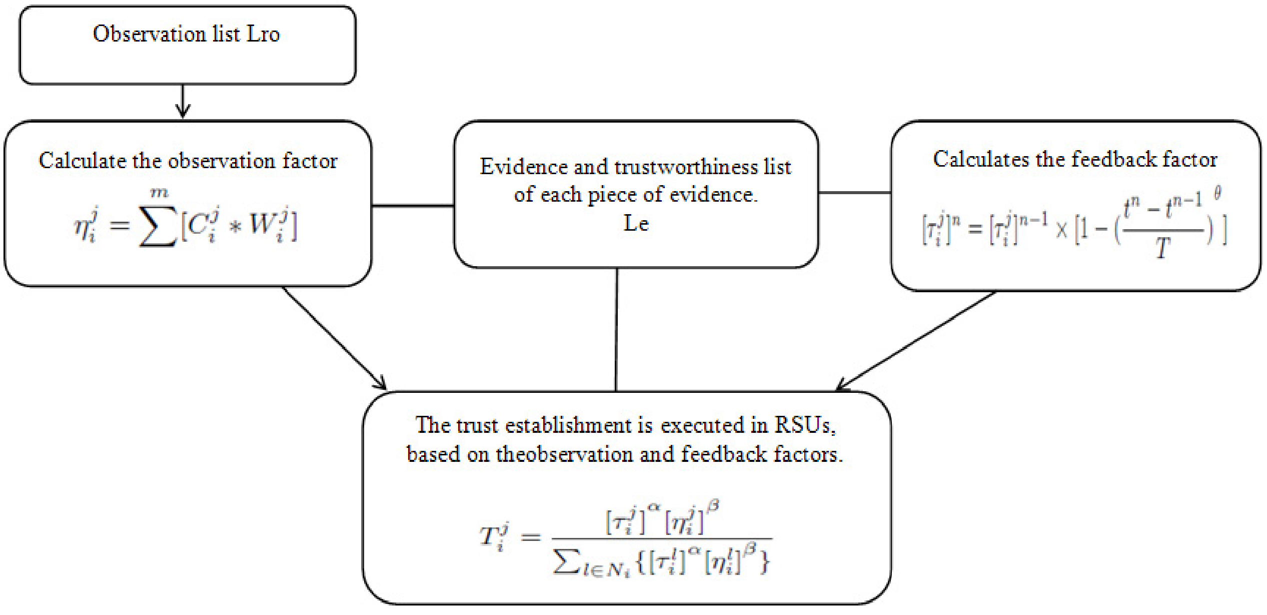
Observation list Lro
Calculate the observation factor
$\eta_i^j = \sum^m [C_i^j * W_i^j]$
Evidence and trustworthiness list of each piece of evidence. Le
Calculates the feedback factor
$[\tau_i^j]^n = [\tau_i^j]^{n-1} \times [1 - (\frac{t^n - t^{n-1}}{T})^\theta]$
The trust establishment is executed in RSUs, based on theobservation and feedback factors.
$T_i^j = \frac{[\tau_i^j]^\alpha [\eta_i^j]^\beta}{\sum_{l \in N_i} \{[\tau_i^l]^\alpha [\eta_i^l]^\beta\}}$

Figure 10: RATE.

Citation: Bousmaha N, Maachaoui M, Chelouah R (2020) Survey: Trust Management in VANET. Int J Comput Softw Eng 5: 152. doi: https://doi.org/10.15344/2456-4451/2020/152

The RSU receives observation reports. RATE has put them in the recently received observation list (Lro). The RSU allow testing the recent observation reports in (Lro). The observation factor estimation is based on all the confidence and weight. The confidence is established by the distance from the vehicle to the event k (Dk), maximum detection range of the vehicle (Dmax), the number of sensors that can detects the event (Nks), and total number of sensors equipped in the vehicle (Nmax). Besides, the weight of vehicle is determined by the type of vehicle. Figure 10 describes a RATE.

Cong et al. [20] proposed trust model based on the estimated trust of the originator or forwarder, which aims to determine the accuracy of V2V incident reports. In this model, the trust score is estimated by using the behavior history of incident report accuracy for the vehicle, based on this, a trust model is used by Vehicle Behaviour Information collection Infrastructure (VBII) to provide a central authority incident reports received from other vehicles. To ensure the viability of the process we consider three assumptions:

1. The latency: describes the period of delay of traffic incidents in real-time.
2. The vehicles observe the behavior of other vehicles to transfer the information to the central authority.
3. The identifier system for vehicles that contains other vehicles information.

As shown in Figure 11, the vehicle takes trusted decisions from the information received based on the confidence score. The trust score of the report originator and forwarders allows taking two decisions:

1. The vehicle makes the decision on whether accepting or not the data message from other vehicles.
2. In the case where the vehicle decides to accept the received information, an endorsement opinion must be attached.

Combined-oriented trust model

This model depends on the estimation of the reliability of the data based on the trust of the entity. It checks the confidence of the received data, using its previous experience of reliability received from other vehicles in the network.

In [21], the authors present the hybrid trust modelthe basic distributed public key infrastructure and algorithm Fuzzy. Thetrust depend two aspects to follow:The cooperation between vehicles disseminates the reliability data. Consequently, the cooperation

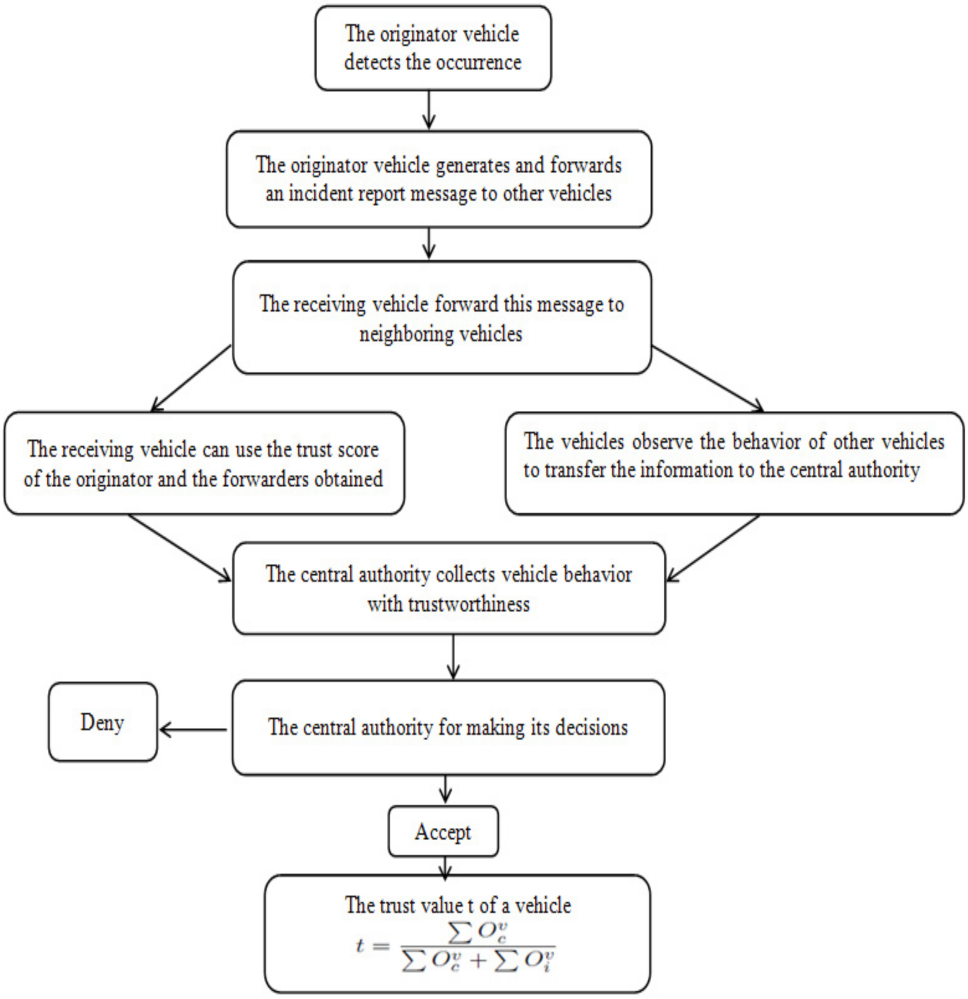
The originator vehicle detects the occurrence
The originator vehicle generates and forwards an incident report message to other vehicles
The receiving vehicle forward this message to neighboring vehicles
The receiving vehicle can use the trust score of the originator and the forwarders obtained
The vehicles observe the behavior of other vehicles to transfer the information to the central authority
The central authority collects vehicle behavior with trustworthiness
Deny
The central authority for making its decisions
Accept
The trust value t of a vehicle
$t = \frac{\sum O_c^v}{\sum O_c^v + \sum O_i^v}$

Figure 11: Incident Reports.

depends on the estimate to receive a warning message by the reputation of the same event. The surveillance the behavior of vehicles used Fuzzy algorithm, which can filter malicious vehicles.The trust estimates that level by the trust metric (Tm), which consists of interval value in [0, 1].The vehicle assess trustworthiness arrive 1. The trust level is refreshed with every change in cluster. The Certification Authority (CA) is responsible for creation the certificate among the member of the cluster. Figure 12 describes a Fuzzy.

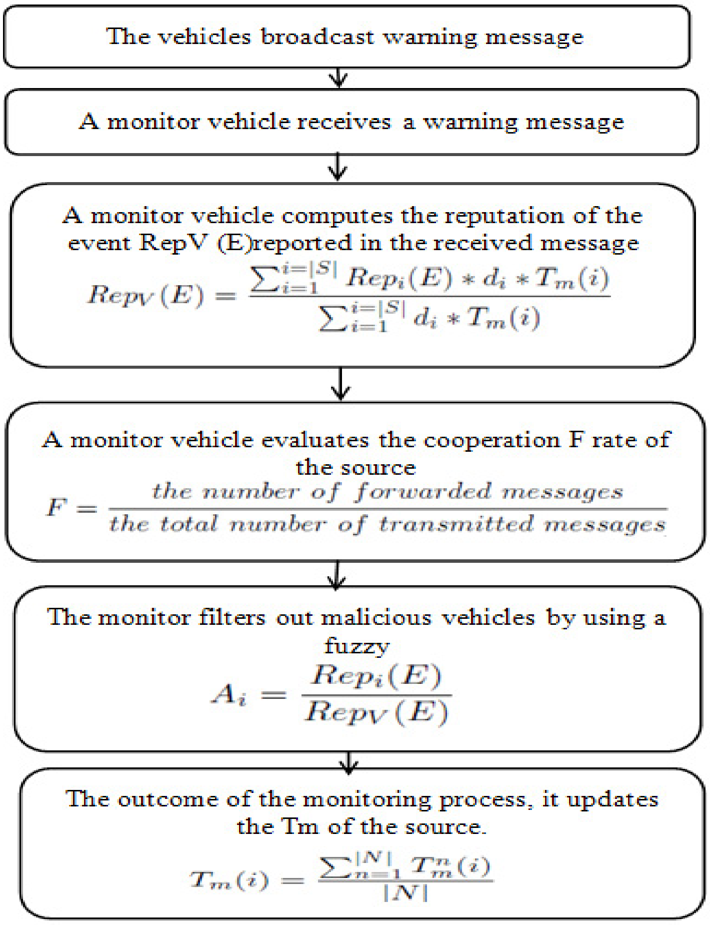
The vehicles broadcast warning message
A monitor vehicle receives a warning message
A monitor vehicle computes the reputation of the event RepV (E)reported in the received message
$Rep_V(E) = \frac{\sum_{i=1}^{i=|S|} Rep_i(E) * d_i * T_m(i)}{\sum_{i=1}^{i=|S|} d_i * T_m(i)}$
A monitor vehicle evaluates the cooperation F rate of the source
$F = \frac{the\ number\ of\ forwarded\ messages}{the\ total\ number\ of\ transmitted\ messages}$
The monitor filters out malicious vehicles by using a fuzzy
$A_i = \frac{Rep_i(E)}{Rep_V(E)}$
The outcome of the monitoring process, it updates the Tm of the source.
$T_m(i) = \frac{\sum_{n=1}^{|N|} T_m^n(i)}{|N|}$

Figure 12: Fuzzy.

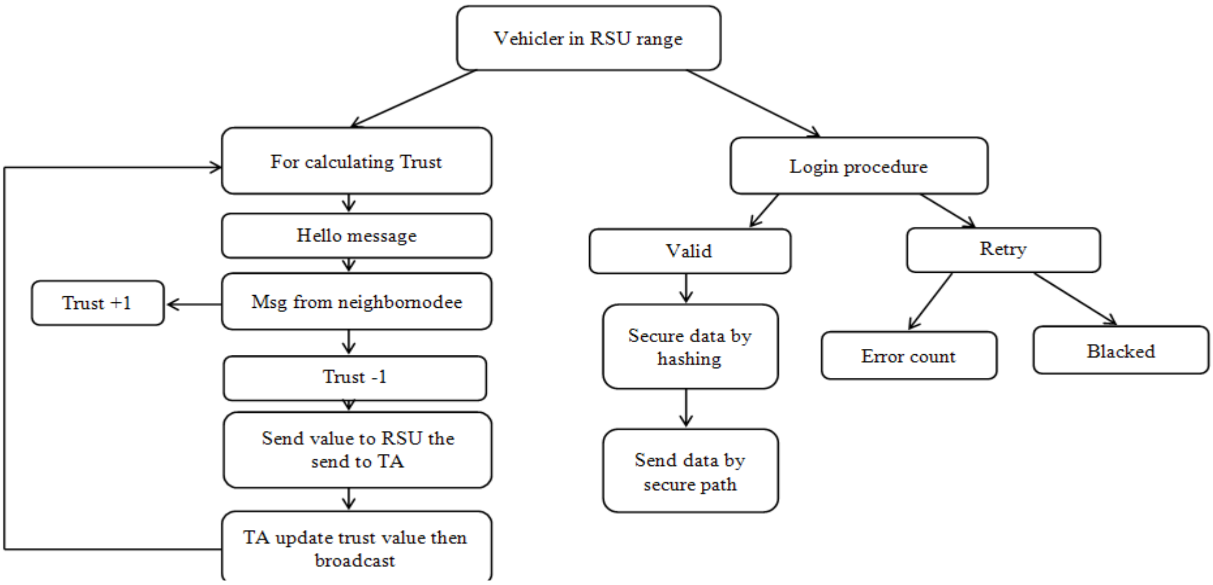

Figure 13: Hashing.

The authors in [22], propose a mechanism for estimating the trust value based on the behavior of each vehicle, which concerns data integrity protection through the hashing technique and use a trusted path. The value of the trust evaluates the periodic message broadcast with its acknowledgment.This mechanism allows the evaluation of the trust value by each vehicle, which will calculate the confidence value and transmits it to the AS via RSU. Then the AS will save the trust values and broadcast them immediately into the network via the RSU.This mechanism allows the evaluation of the trust value by each vehicle, which calculates the confidence value to transmit the value to AS via RSU. AS depends on saving the confidence values immediately broadcast in the network through RSU. This mechanism identifies the valid RSU node to apply the hash technique on the data, every vehicle containing a value of confidence using this value to discover trusted paths to transmit information via trusted nodes. The disadvantage of this mechanism is that it does not check the behavior of periodic messages. Figure 13 describes a Hashing.

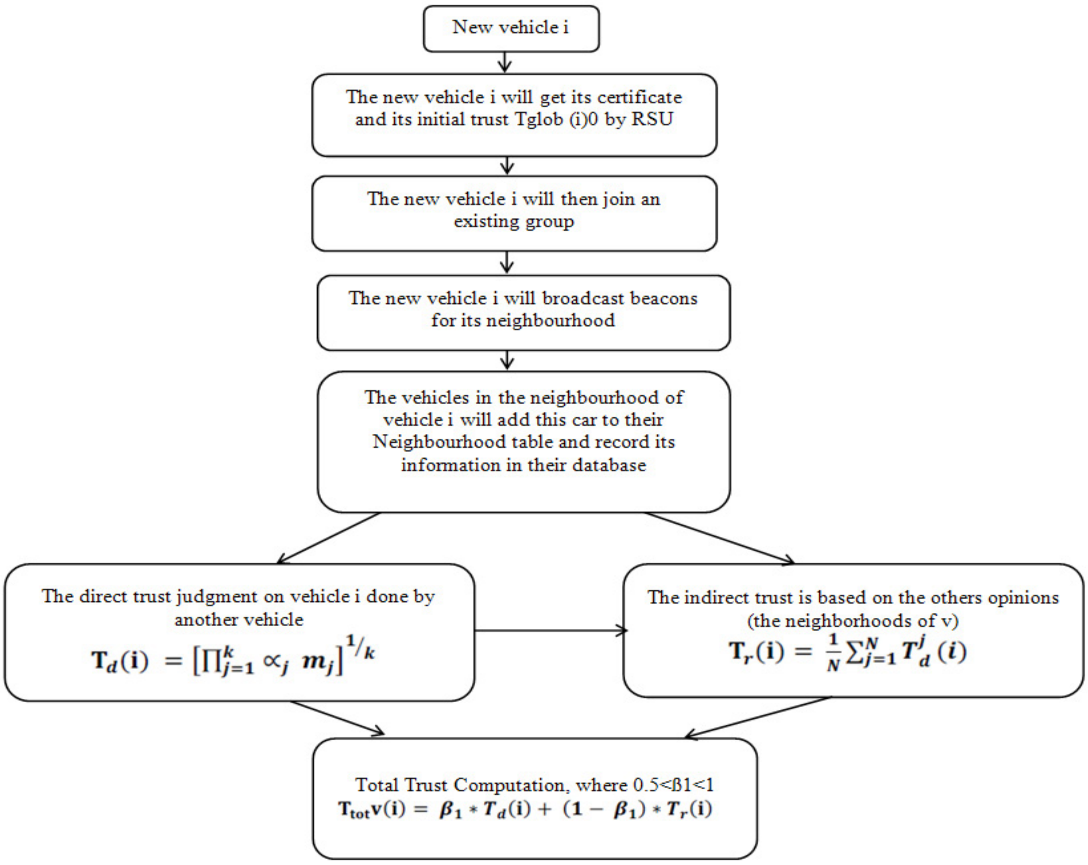
New vehicle i
The new vehicle i will get its certificate and its initial trust Tglob (i)0 by RSU
The new vehicle i will then join an existing group
The new vehicle i will broadcast beacons for its neighbourhood
The vehicles in the neighbourhood of vehicle i will add this car to their Neighbourhood table and record its information in their database
The direct trust judgment on vehicle i done by another vehicle
$\mathbf{T}_{d}(\mathbf{i}) = [\prod_{j=1}^{k} \propto_j m_j]^{1/k}$
The indirect trust is based on the others opinions (the neighborhoods of v)
$\mathbf{T}_r(\mathbf{i}) = \frac{1}{N}\sum_{j=1}^{N} T_d^j(i)$
Total Trust Computation, where 0.5<ß1<1
$\mathbf{T_{tot}v(i)} = \beta_1 * T_d(\mathbf{i}) + (1 - \beta_1) * T_r(\mathbf{i})$

Figure 14: GL.

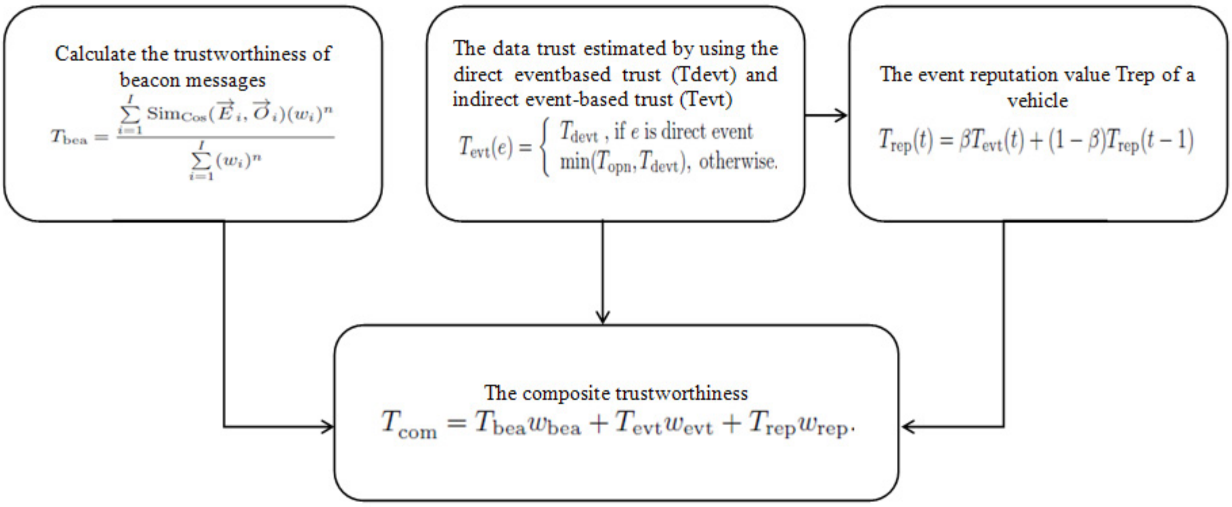
Calculate the trustworthiness of beacon messages
$T_{\text{bea}} = \frac{\sum_{i=1}^{I} \text{Sim}_{\text{Cos}}(\vec{E}_i, \vec{O}_i)(w_i)^n}{\sum_{i=1}^{I} (w_i)^n}$
The data trust estimated by using the direct eventbased trust (Tdevt) and indirect event-based trust (Tevt)
$T_{\text{evt}}(e) = \begin{cases} T_{\text{devt}}, \text{ if } e \text{ is direct event} \\ \min(T_{\text{opn}}, T_{\text{devt}}), \text{ otherwise.} \end{cases}$
The event reputation value Trep of a vehicle
$T_{\text{rep}}(t) = \beta T_{\text{evt}}(t) + (1-\beta) T_{\text{rep}}(t-1)$
The composite trustworthiness
$T_{\text{com}} = T_{\text{bea}} w_{\text{bea}} + T_{\text{evt}} w_{\text{evt}} + T_{\text{rep}} w_{\text{rep}}.$

Figure 15: BTM.

Hamssa et al. [23], proposed a hybrid trust model based on a public key infrastructure and allocation to determine the most reliable vehicle defined as the group leader (GL). The model manages the communication between the members and references all the exchange information in the cluster. This model estimates the value of trust in direct / indirect way to build an evaluation of a total trust.The vehicle that has which the highest of the trust value used as though Group Leader. The RSU given for every new vehicle authenticate. Consequently, the new vehicle contains value of confidence called trust initial. The vehicle broadcasts a message containing a direct trust list for its neighbor, whom will use it to calculate indirect trust. Then, the trust value of the vehicle is sent to the GL, which in turn will send its trust value to the RSU. Figure 14 describes a GL.

In [24], the authors proposed a Beacon-Based Trust Management (BTM) system, which prohibits the internal attackers from sending false messages and privacy enhancement. The system estimate a hybrid trust by cross-checking the plausibility of event messages and beacon messages, which computes entity trust by using beacon messages and evaluate data trust by the determination of event messages and beacon messages.

In this model, secure beacon based trust protocol is used to estimate direct and indirect trust. In order to calculate the direct trust observed by a vehicle itself or neighboring vehicles, that evaluates the first-hand information by position and movement verification. Indirect trust is obtained via the recommendations from other vehicle. Entity trust uses cosine similarity for to estimate values by position, velocity, and direction. The reputation value is calculated based on the indirect event trust value where the previous reputation value is considered. Data trust is based on direct event based trust and on indirect event based trust. Figure 15 describes a BTM.

Evalution of Trust Models

In this section, we will describe the properties to take into account for the trust models mentioned above, which imposes big challenges and constraints to take into consideration.

Dynamic

The vehicle ad hoc networks have the properties fast moving and the variable densities on the road. The rapid movement of vehicles disrupts communications, causing frequent interruptions. This makes it difficult or impossible to obtain this information such as identification and position of the vehicle because it will not stay in a few seconds. The density varies depending on the number of vehicle sometimes very high or very low depending on road situations. The high density increases by the number of vehicles on the highway preserves the available connectivity. On the other hand, the low density is measured by the numbers of the vehicles diminishing on the highway causing breaks disconnections. Low density leads to a long waiting period risk for routing. Therefore, we use these definitions to compare trust models.

Decentralization

The vehicle can at any time join or leave the network at random, which is a major drawback for the centralization of trust management. The establishment of trust must be achieved without the existence of a centralized infrastructure. It is a requirement for a decentralization environment.

Security

Security is several required such as authentication and encryption / decryption method. The authentication is established through the reliability of messages when sending the message. In addition, the authentication is an important step in building trust and revealing the true identity of peers. The cryptography technique is a very important parameter to guarantee secure communication. The results estimate security incapacity in trust models.

Privacy

The information of location and identification of the vehicle considered as the most critical information. This information privacy allows decided the trust of a vehicle via its identity, once its identity authenticated, position and its own honest behavior is verified, we can trust the information received by this vehicle.

Real-time processing

In VANETS, delay is strictly intolerant. The power of trust management is in providing security based on real time communications. If a required message could not be received in time, that could pose certain problems facing the accurate establishment of the correct trust value for the sender, which requires a real time and high performance for processing units in the infrastructure [25-27].

Discussion

In the previous section, we describe in detail the existing trust models in VANET environment in Section II. The trust model defines three categories as such: (A) entity-centric, (B) data-centric and (C) combined. The applications in VANETs are based on the shared information between the entities. The different applications are exposed to some security attacks, even if the target is a specific service, for sure other related services will be affected as well. The VANETs applications are classified according to their: safety, security, and infotainment [28]. This classification of applications presents different impacts of each type of attack.

The trust is adopted for secure the network and ensure the integrity data against the different threats either dishonest entities, malicious messages, or both. In other words, the trust defenses against the inside attackers in those situations where cryptography completely fails. Based on this model, we observed the trust model concentration on the properties and the trust metrics. Consequently, the trust metrics define precisely for requirement to need the properties of the trust model. Therefore, this model is based on evaluating the properties of the trust model. According, the trust models design to evaluate the entity and reliable data in the VANET network. In addition, we will present the properties of criteria need for the trust management, to make a comparison between the models of trust with the properties in Table 1.

The different requirements must be enough of the properties elements in the trust models to avoid the large number of more targeted attacks. We above present the results of our evaluation concerningthis list of properties, namely dynamic, decentralization, security, privacy, real-time.

This result shows that trust models have the insufficient of effectiveness for the list of properties. Form this table, we note that

Properties	Dynamic	Decentralization	Security	Privacy	Real-time
VDDZ [8]	+	-	+	+	-
TRIP [10]	+	-	-	-	-
DTT [12]	+	+	+	-	+
MILTIFACTED[13]	+	+	-	-	+
WATCHDOG [14]	+	+	-	-	+
TACR [15]	+	+	-	-	+
Black-hole [16]	+	+	-	-	+
RMCV [17]	+	+	-	-	+
INTRUSION AWARE [18]	+	+	-	+	+
RATE [19]	+	+	+	-	-
INCIDENT REPORTS [20]	+	+	-	-	+
FUZZY [21]	+	-	+	-	+
Hashing [22]	+	+	+	-	+
GL [23]	+	+	-	-	-
BTM [24]	+	+	-	+	+

Table 1: Summarizes the comparison between the discussed.

none of the trust models apply all properties, in fact, the trust model has not focus the privacy ignore this properties by the researchers.

Conclusion

The trust model allows evaluating trustworthy entity or messages, which reduces the risk misbehavior vehicles during the communication. The evaluation of trust is so important to assure secured communications in VANET. The trust management has been proposed in the last years as an accurate alternative to deal with some security threats in highly distributed and dynamic scenarios. In this paper, we present survey the trust model for the networks VANET domain. Thus, we will describe in detail of the several trust model. Accordingly, the trust models distinguish three categories as follows: (A) entity-centric, (B) data-centric and (C) combined. We chose thislist of the properties to evaluate the effectiveness of the trust model. Then we will describe all the property in the list as follows: dynamic, decentralization, security, privacy, real-time. In this study we discussedthe comparison trust model with the list of the properties. Based on this result, we allow us interested to the trust management in the network VANET, more particularly in a context the trust of data.

In future work, we will propose a new approach to the trust model that can detect and mitigate entities and malicious behaviors in VANET networks.

Acknowledgment

This research was supported by the University of Paris-Seine, France, and the Algerian Ministry of Higher Education Fellowship awarded to Nourelimane Bousmaha.

The information provided in this paper is the sole responsibility of the authors.

Competing Interests

The authors declare that they have no competing interests.

References

1. Dhamgaye A, Chavhan N (2013) Survey on security challenges in VANET. IJCSN 1: 2277-5420.
2. Al-Sultan S, Al-Doori MM, Al-Bayatti A, Zedan H (2014) A comprehensive survey on vehicular Ad Hoc network. Journal of Network and Computer Applications 37: 380-392.
3. Mejri MN, Ben-Othman J, Hamdi M (2014) Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications 1: 53-66.
4. Samara G, Al-Salihy WAH, Sures R (2010) Security Analysis of Vehicular Ad Hoc Networks (VANET). Second International Conference on Network Applications, Protocols and Services.
5. Engoulou RG, Bellaïche M, Pierre S, Quintero A (2014) VANET security surveys. Computer Communications 44: 1-13.
6. Wex P, Breuer J, Held A, Leinmuller T, Delgrossi L, et al. (2008) Trust Issues for Vehicular Ad Hoc Networks. IEEE.
7. Bißmeyer N, Mauthofer S, Kpatcha B, Kargl F (2012) Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters. IEEE.
8. Gazdar T, Benslimane A, Belghith A (2011) Secure Clustering Scheme Based Keys Management in VANETs. Vehicular Technology Conference IEEE.
9. Rachedi A, Benslimane A (2008) A Secure and Resistant Architecture against Attacks for Mobile Ad Hoc Networks. Security and Communication Networks.
10. Mármol FG, Pérez GM (2012) TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of Network and Computer Applications.
11. Zadeh LA (1965) Fuzzy sets. Information and control 8: 338-353.
12. Wang Z, Chigan C (2007) Countermeasure Uncooperative Behaviors with Dynamic Trust-Token in VANETs. IEEE.
13. Minhas UF, Zhang J, Tran T, Cohen R (2011) A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. IEEE 3: 407-420.
14. Hortelano J, Ruiz JC, Manzoni P (2010) Evaluating the usefulness of watchdogs for intrusion detection in vanets. In Communications Workshops (ICC), IEEE International Conferenc.
15. Al-Sultan S, Al-Doori MM, Al-Bayatti AH, Zaden H (2014) A comprehensive survey on vehicular Ad Hoc network. Journal of Network and Computer Applications 37: 380-392.

16. Yao X, Zhang X, Ning H, Li P (2016) Using trust model to ensure reliable data acquisition in VANETs. Ad Hoc Networks.

17. Gurung S, Lin D (2013) Information-oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks. International Conference on Network and System Security.

18. Shaikh RA, Alzahrani AS (2013) Intrusion-aware trust model for vehicular ad hoc networks. Secur Commun Netw.

19. Wu A, Ma J, Zhang S (2011) RATE: a RSU-aided scheme for data-centric trust establishment in VANETs. IEEE.

20. Liao C, Chang J, Lee I, Venkatasubramanian KK (2013) A Trust Model for Vehicular Network-Based Incident Reports. International Symposium on Wireless Vehicular Communications: WiVeC.

21. Tahani G, Benslimane A, Rachedi A, Belghith A (2013) A trust-based architecture for managingcertificates in vehicular ad hoc networks. Communications and Information Technology (ICCIT), International Conference on.

22. Agarwal P, Bhardwaj N (2016) Enhance the Security by using Hashing Technique and Trust Values in Vehicular Ad Hoc Networks. IJSART 2: 2395-1052.

23. Hasrouny H, Samhat AE, Bassil C, Laouiti A (2018) Trust Model for Group Leader Selection in VANET, International Journal of Digital Information and Wireless Communications (IJDIWC).

24. Chen YM, Wei YC (2013) A beacon-based trust management system for enhancing user centric location privacy in VANETs. J Commun Netw 15: 153-163.

25. Soleymani SA, Abdullah AH, Hassan WH, Anisi MH, Goudarzi S, et al. (2015) Trust management in vehicular ad hoc network: a systematic review. EURASIP Journal on Wireless Communications and Networking.

26. Cooper C, Frankliny D, Ros M, Safaei F, Abolhasany M, et al. (2016) A Comparative Survey of VANET Clustering Techniques. IEEE Communications Surveys & Tutorials.

27. Zhang J (2011) A survey on trust management for VANETs. IEEE International Conference on Advanced Information Networking and Applications.

28. Kerrache CA, Calafate CT, Cano JC, Lagraa N, Manzoni P, et al. (2016) Trust Management for Vehicular Networks: An Adversary-Oriented Overview. IEEE 4: 2169-3536.