Soleymani *et al. EURASIP Journal on Wireless Communications and Networking* (2015) 2015:146
DOI 10.1186/s13638-015-0353-y

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

REVIEW Open Access

Trust management in vehicular ad hoc network: a systematic review

Seyed Ahmad Soleymani[1*], Abdul Hanan Abdullah[1], Wan Haslina Hassan[3], Mohammad Hossein Anisi[2], Shidrokh Goudarzi[3], Mir Ali Rezazadeh Baee[1] and Satria Mandala[1]

Abstract

The basis of vehicular *ad hoc* networks (VANETs) is the exchange of data between entities, and making a decision on received data/event is usually based on information provided by other entities. Many researchers utilize the concept of trust to assess the trustworthiness of the received data. Nevertheless, the lack of a review to sum up the best available research on specific questions on trust management in vehicular *ad hoc* networks is sensible. This paper presents a systematic literature review to provide comprehensive and unbiased information about various current trust conceptions, proposals, problems, and solutions in VANETs to increase quality of data in transportation. For the purpose of the writing of this paper, a total of 111 articles related to the trust model in VANETs published between 2005 and 2014 were extracted from the most relevant scientific sources (IEEE Computer Society, ACM Digital Library, Springer Link, Science Direct, and Wiley Online Library). Finally, ten articles were eventually analyzed due to several reasons such as relevancy and comprehensiveness of discussion presented in the articles. Using the systematic method of review, this paper succeeds to reveal the main challenges and requirements for trust in VANETs and future research within this scope.

Keywords: Systematic literature review; Trust management; VANET; Trust metric

1 Review

1.1 Introduction

Vehicular *ad hoc* networks (VANETs) are a class of *ad hoc* networks that consist of vehicles and roadside units (RSUs). VANETs were originally created to enhance safety on the road using cooperative collision warning via vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In V2V communication, vehicles send and receive messages to and from one another. These messages can alert signals about road congestion, accidents ahead, or information about traffic on a given route. V2I communication takes place between nodes and roadside infrastructure and involves finding the nearest cheapest gas station, internet services, online toll payment, etc.

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

In order to overcome these threats and increase security, several concepts have been proposed by researchers. Wei and Chen [3] stated that authentication is one method for ensuring the integrity of transmitted messages. In [4], the reputation of a vehicle is introduced to evaluate the reliability of received data. Dotzer et al. also stated that a common method to deal with the safety threats in VANETs is to establish trust relationships and detect selfish and malicious entities [5].

Security is one of the main issues in VANETs, and trust is a key element of security [6]. Hence, since VANETs are based upon data exchange among vehicles, trustworthiness of data is of great importance. In addition, data communication between trusted vehicles directly affects

*Correspondence: asseyed4@live.utm.my
[1] Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor Malaysia
Full list of author information is available at the end of the article

security. Moreover, the quality of safety/non-safety applications in VANETs largely depends upon the trustworthiness of data [7], and trust plays a vital role in the security and quality of a vehicular network. Thereby, comprehensive studies on trust and reviewing existing trust models are necessary. However, the lack of a review on trust in VANETs to sum up the best available research on specific questions is sensible, which must be done by synthesizing the results of existing studies.

This study conducts a systematic literature review (SLR) of current research that aim at managing trust on vehicular ad hoc networks. The present study investigates the existing trust models published between 2005 and 2014 and extracts the advantages and weaknesses of the proposed trust models. The process of trust measurement in each model along with the relevant flowchart is also described. In addition, this study exploits trust metrics and properties of the trust model. As a result, based on the existing problems and gaps in the proposed models, a new framework to develop an intelligence trust model in VANETs is proposed.

The rest of the paper is organized in the following way: Section 1.2 discusses the research methodology in this review. Sections 1.3 and 1.4 present the definition of trust and trust management in VANETs, respectively. In addition, in Section 1.4, we present some of the existing trust models. Section 1.5 presents the trust metric. Section 1.6 describes the comparison of proposed trust models and also presents our framework. Section 2 concludes the review.

1.2 Research methodology

Two main methods of review articles are commonly found in the scientific literature: systematic and narrative review of the literature. A narrative review describes and discusses the state of the science of a specific topic from a theoretical and contextual point of view [8]. A systematic literature review provides a means of identifying, evaluating, and interpreting the literature relevant to a particular research question or topic area [9].

To provide comprehensive and unbiased information on trust in VANETs, this study presents a systematic literature review. There are five steps in conducting a systematic review [10] which we are presenting briefly next: (a) identification of resources, (b) selection of studies, (c) study quality assessment, (d) Data extraction and monitoring progress, and (e) data synthesis. Furthermore, according to [9], the research question is 2 the most important pre-review activity in SLR. In this study, the research questions related to trust management in VANETs are as follows:

- What are the methods used in the proposed trust models?
- What are the trust metrics used to measure trust in the existing trust model?
- What are the properties of the trust model?

1.2.1 Identification of resource

The first step towards resource identification is recognizing the relevant keywords. For this purpose, we have conducted a broad search on Google Scholar using 'Trust in VANET' as keyword. The initial result shows that 'reputation' is a common issue related with 'Trust in VANET'. Therefore, we refined the search for articles using 'Reputation and Trust in VANET'.

Based on both levels of keywords in the search, we have found 98 articles. These articles are stored in LIST 1. The detailed activity for searching articles is presented in Figure 1.

- First level of keywords
  - (Trust Management) and (VANET)
  - (Trust Model) and (VANET)
- Second level of keywords
  - (Reputation) and (VANET)

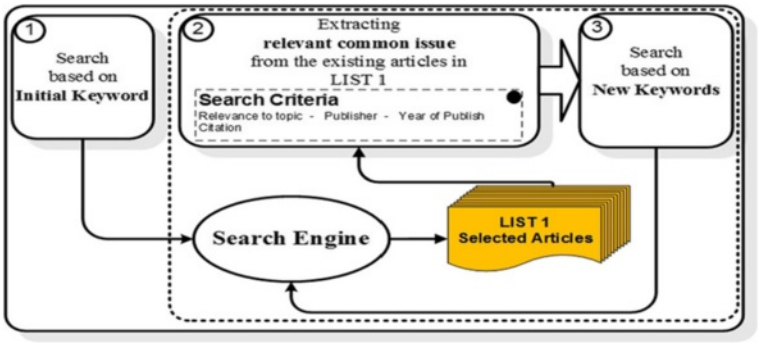

Figure 1 First step to extract articles based on keywords.

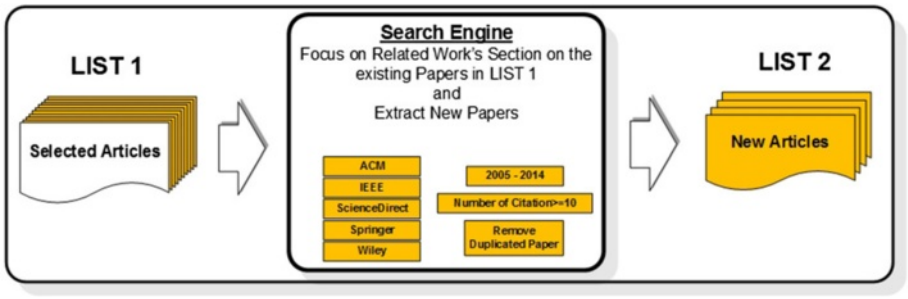

Figure 2 Second step to extract articles based on the related work section.

In the second step, to reduce the likelihood of bias and to find relevant new articles, we focused on the related work section of existing articles in LIST 1. Based on this step, we have found 13 new articles related to trust and reputation in VANETs which are stored in LIST 2. The process of this step is illustrated in Figure 2.

1.2.2 Selection of studies

Different methods of selection are proposed in the existing systematic review [11,12]. In this paper, we consider several criteria as exclusion criteria for screening. Based on these criteria, studies that were not clearly related to the research questions will be excluded. These criteria are related to publisher, year of publication, number of citation, and so on. In the following, we describe them in detail. Figure 3 also shows the detailed activity for selection of studies.

- The first rule indicates that five databases - IEEE, ACM, Springer, Science Direct, and Wiley - are acceptable to find relevant studies in the field. However, this study is not limited to these databases, and few numbers of articles are selected from other databases. The main condition to select articles from other databases is the high number of citations.
- The second rule is related to the year of publication of articles. For this purpose, the search is limited to studies published between 2005 and 2014.
- The third rule is related to articles that were accepted in a conference. For this purpose, we consider a special condition to exclude or include articles that were accepted in conferences. Based on this condition, we exclude articles that have less number of citations than the threshold (i.e., threshold $= 10$).
- In the process of searching for articles, we have found that some papers have been duplicated. Therefore, according to the fourth rule, we exclude the duplicate articles.

1.2.3 Data extraction

In the data extraction and synthesis step, the key details from the selected papers will be obtained. This work divides data extraction into two groups:

(1) Methods, where the different methodological approaches of trust in VANET are synthesized
(2) Demographics of the published works, e.g., the year of publication

1.2.4 Data analysis

The data analysis extracts the terms and definitions used in the FINAL LIST of selected papers. Therefore, we focus on the existing trust models in the FINAL LIST and extract the concepts that have been used in each model. We summarize them and briefly describe each of them in Table 1. In addition, we show the results of extract execution in the following figures and tables.

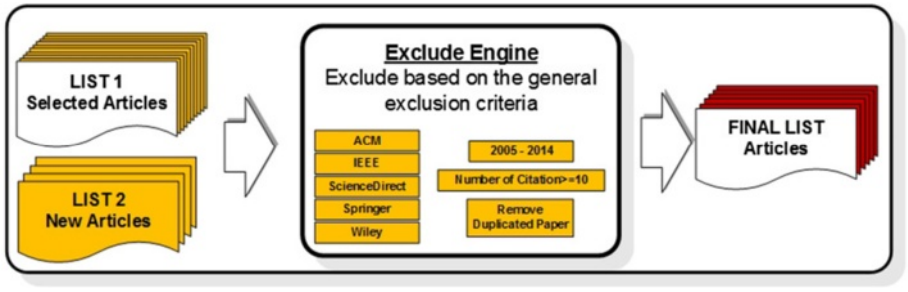

Figure 3 Selection of final studies.

Table 1 Important concepts in this review

Concept	Description
Type of trust model	Type of trust model in terms of the main object
Trust metric	Factors that are used to measure trust value in each model
Trust model properties	Properties that trust models have to satisfy them

Table 2 shows the results of all steps as determined in a summary of the studies selected in each stage of the selection procedure for each source. LIST 1 shows the results which were obtained by running the search string on the selected sources. The LIST 2 shows articles which were selected based on the related work section. The last row shows the number of final papers selected after the study selection procedure.

Figure 4 illustrates the details of LIST 1 and LIST 2 that present the number of publications in different databases over a specific time period, between 2005 and 2014.

1.3 Trust

In computer science, as well as in the social sciences, trust has many meanings [13,14]. Although definitions and classifications of trust have been borrowed from the social science literature, there is no clear consensus on the definition of trust in computer networks [15]. Nevertheless, the researchers in the field of security in *ad hoc* networks [16,17] utilized the concept of trust to improve security. Yu et al. [18] and Yang and Sun [19] stated that mechanisms of trust are the strategy to improve security of MANET. In addition, Abdel-Hamid et al. in [20] reported that trust is a key element of security in vehicular *ad hoc* networks. Liu et al. have mentioned that trust is the belief that an entity has about other entities [15]. Due to the importance of this concept in the security of *ad hoc* networks and to enhance safety, we have collected some of the existing definitions of trust in VANETs in Table 3.

1.4 Trust management

Due to the lack of centralized services in self-organized systems, vehicular *ad hoc* networks cannot be secured by the existing security solutions [21]. Therefore, researchers have proposed different techniques to enhance security. Gomez and Martinez [22] refer to trust and reputation management in distributed networks as a novel and original way to address and tackle some of those not yet solved threats. Li et al. [23] introduced also the trust establishment scheme in VANETs to help normal nodes make the right choice and constrain the harmful behavior of bad ones. Moreover, authors in [24] mentioned that trustworthy communication in vehicular *ad hoc* networks is essential to provide a reliable traffic safety to improve the efficiency of applications. Table 4 presents some definitions of trust management proposed by researchers.

Table 2 Summary of studies selected at each stage of the selection procedure

	IEEE	ACM	Springer	Science Direct	Wiley	Other	Total
LIST 1	51	5	11	6	3	22	98
LIST 2	6	2	0	0	0	5	13
FINAL LIST	5	0	2	1	1	1	10

As mentioned above, trust management has become a main method to ensure the security of vehicular *ad hoc* networks, and trusted relation between vehicles is the outcome of the trust establishment in VANET environment [25]. Especially in critical applications like hazard warning, a receiving node needs to ensure authenticity and trust ability of received messages before any reaction. In recent years, various models of trust have been proposed in VANETs. For instance, Hong et al. [26] described a novel trust model based on situation, namely 'SAT'. The goal of SAT is to build a new trust model using architecture and cryptographic tools that provide predictive trust information and quick and flexible key management, thus improving driving experience. In [7], a real-time message content validation (RMCV) scheme is proposed, which is based on the information-oriented trust model. It empowered each individual vehicle with the capability of evaluating the trustworthiness of the possibly large amount of messages received in VANETs, without relying on any infrastructure support such as roadside units or central servers. Huang et al. [27] stated that almost all the existing reputation systems compute trust value based on the past interaction with target nodes. They argue that due to the dynamic and open environment, this assumption is not valid in VANETs. In fact, if a vehicle is communicating with another vehicle, it is not guaranteed whether it will interact with the same vehicle in the future. Therefore, the existing algorithms which are based on the long-term relationship are not suitable for VANETs. To solve this problem, they proposed a social network approach for trust management in VANETs.

In general, based on the main object in model (data or entity), the trust models in VANETs can be categorized into three major groups as follows [28]: (i) entity-centric, (ii) data-centric, and (iii) combined.

- *Entity-centric*: The entity is the main object in this group, and the trust model focuses on the trustworthiness of vehicles. To achieve this, the trust model needs sufficient information about the neighbors and sender of the message. But the high mobility of vehicles leads to failure to collect enough information about the neighbors/sender. In addition, the correctness of data is another problem in this

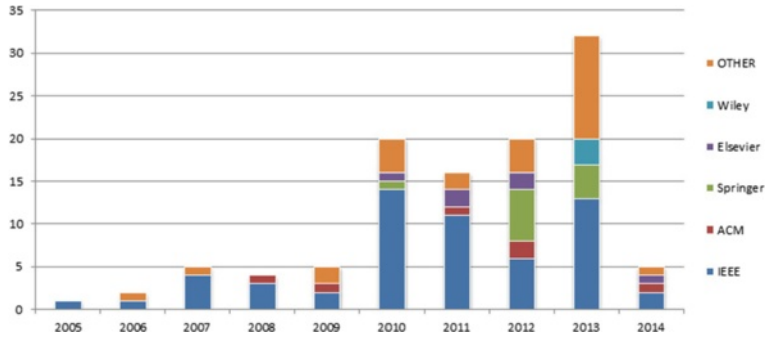

Figure 4 Number of publications over a specific time period.

group. When an entity received data from a trustworthy sender, according to the presence of attackers as well as limitation of sensors, data correctness still remains obscure.

- *Data-centric*: The data/event message is the main object in this group, and the trust model focuses on the trustworthiness of data. In this group, the trust model needs to assess the level of trust for each received event message. Therefore, the large number of data as well as duplicated data in heavy traffic density leads to increased latency and lost data. In contrast, in the sparse traffic density, this model would not perform well [28].
- *Combined*: Both entity and data are the main objects in this group. The trust model uses vehicle trust to evaluate the trustworthiness of data [29].

Based on the method of selection that proposed in this study, ten article are selected to review in more details. We extracted the type of model based on the classification mentioned above. In addition, we focused on trust measurement and decision making applied in the selected trust models in the FINAL LIST. Table 5 presents these models along with the type, publisher, year of publication, and number of citations. We also extracted the workflow of proposed trust models. We exploited the trust metrics, properties, and decision making methods that applied in the proposed trust models.

1.4.1 Entity-based trust management

In the entity-oriented trust model, trustworthiness of information is estimated based on the trustworthiness of the message sender [7]. Minhas et al. [30] and Gomez and Martinez [22] proposed two models of trust based on entity.

To deal with selfish vehicles that try to maximize a car owner's utility by sending out false information, Minhas et al. developed a framework that models the trustworthiness of the agents of other vehicles

Table 3 Definition of trust in VANETs

Study	Definition
[15]	The belief that an entity has about other entities, from past experiences, on knowledge about the entity's nature, and/or on recommendations from trusted entities.
[44]	Trust mechanisms not only help in node behavior detection, but also improve network performance because honest nodes can avoid working with untrustworthy nodes.
[36]	Trust is a relation among entities that is established based on the observations of historical interactions.
[20]	Trust is the key element in creating a trusted vehicular environment which promotes security in vehicular networks.
[45]	A trust value is introduced in order to support the rating of intersecting nodes as benign or malicious.
[46]	Trust can be described as the expectation and belief about future behavior, based on experiences and evidences collected in the past, either direct or indirect.
[47]	Trust describes the level to which an entity accepts the dependence on another one.

Table 4 Trust management in other studies

Study	Description
[33]	Trust management is to determine whether the traffic event reported by a warning message is really occurring and to prevent false traffic warning messages from being spread on VANET.
[22]	Trust and reputation management has been proposed in the last years as an accurate alternative to deal with some security threats in highly distributed and dynamic scenarios.
[23]	Trust management has become a main method to ensure the security of VANETs.
[46]	Trust management is to provide functional and reliable traffic safety and efficiency applications.
[7]	Trust management directly impacts the quality of the applications.
[48]	Trust management is important to secure the application's integrity and reliability.

Table 5 Existing trust models in the FINAL LIST

Class	Study	Year	Publisher	Citation
Entity-based trust model	[30]	2011	IEEE Journal	12
	[22]	2012	Elsevier	20
Data-based trust model	[31]	2008	IEEE Conference	178
	[7]	2013	Springer	0
	[32]	2013	Wiley	0
	[33]	2010	IEEE Conference	12
	[34]	2009	Hindawi	33
	[35]	2011	IEEE Conference	10
Combined trust model	[36]	2013	IEEE Journal	3
	[37]	2012	Springer	0

[30]. This model considers a multifaceted trust modeling approach that incorporates role, experience, priority, and majority-based trust. As shown in Figure 5, when an agent/vehicle receives a few reports (s) that are relevant to an event from different agents/vehicles (k), depending on the task, a number of agents (n) are chosen and an ordered list of agents to ask is constructed. The existing agents/vehicles in the ordered list based on both role-based and experience-based trust values will be prioritized. Then, the agent attempts to send a request to existing agents in the list and receives responses from them. According to the time closeness, location closeness, experience-based trust, and role-based trust, the aggregated effects of its report (E_{R_j}) for each agent in the ordered list will be calculated. To consider the effect of all the different reports, the majority opinion (M_{R_j}) which is the report with maximum effect among all reports will be obtained. Based on the aggregated effect, the majority opinion, and the maximum error rate (ε), the agent will decide on how to react on the report. If there is a majority consensus on the response, then this response is taken as the advice and is followed. Otherwise, the agent follows the advice of an agent with the highest role and highest experience trust value.

In order to quickly and accurately distinguish malicious or selfish nodes that are spreading false or bogus messages throughout the network, an infrastructure-based trust and reputation model, namely TRIP, is proposed in [22]. This model computes reputation score based on the recommendation given by other vehicles and RSUs. The decision making in this model is based on fuzzy logic and probability.

As shown in Figure 6, the reputation score of each vehicle (v_i) computes a trust score for other vehicles (v_j) from which it receives a message. To this end, TRIP considers the recommendation given by the RSU ($\mathrm{Rec}_{\mathrm{RSU}_j}$), recommendation given by other vehicles (Rec_{k_j}), and reputation score at previous time (Rep_{ij}^{t-1}). The reputation score will determine which trust level the vehicle is placed: TRUST, NOT TRUST, or +/- TRUST. Moreover, this model considers each message as having a certain severity level: high, medium, and low. Messages with high severity can be only accepted when they were issued by vehicles placed in the 'TRUST' trust level, whereas medium and low severity messages can be accepted from nodes which were given either the 'TRUST' or '+/- TRUST' level. The probability of accepting a message sent by a vehicle which was placed in the trust level '+/- TRUST' will be calculated using $\mathbb{P}_{+/-T}$.

1.4.2 Data-based trust management

The data-based trust model attempts to verify whether the reported information is reliable or not. Based on the trust value, the model decides how to react on the reported event. A few models of trust based on data have been proposed such as the data-centric, RMCV, intrusion-aware trust model, reputation-based trust model, event-based reputation system (ERS), and roadside-unit aided data-centric trust establishment (RATE).

Raya et al. [31] proposed a framework for data-centric trust establishment where trust in each individual piece of data is computed. They proposed the collection of multiple reports related to the same event and of their weights and their combination into a robust decision scheme. Thus, the reports along with their weights are passed to a decision logic module. Figure 7 shows the process applied in this trust model.

They mentioned that vehicles can become faulty or compromised by attackers and hence need to be revoked. In addition, the location and time of report generation change fast and are important in assigning trustworthiness values to events. To this end, they defined a security status function ($s(v_k)$) to determine legitimate and revoked vehicles and dynamic trust metric functions that indicate different node attributes that dynamically change. For each attribute, a different metric is defined (μ_l). In addition, in this model, vehicles are classified according to a system-specific set of node types. The type of each vehicle will be determined by ($\tau(v_k)$). Moreover, for all vehicle types, there exists a trustworthiness ranking where the trustworthiness ranking of each vehicle is different with respect to a task. Therefore, based on the type of vehicle and the type of event, the event-specific trustworthiness function (f) does differentiate among any two or more nodes of the same type. Then, the trustworthiness of a report ($F(e_k^j)$) will be computed based on security status, dynamic trust metric, and event-specific trustworthiness. Because it can be hard to decide whether the reported event took place based on a single message, they proposed

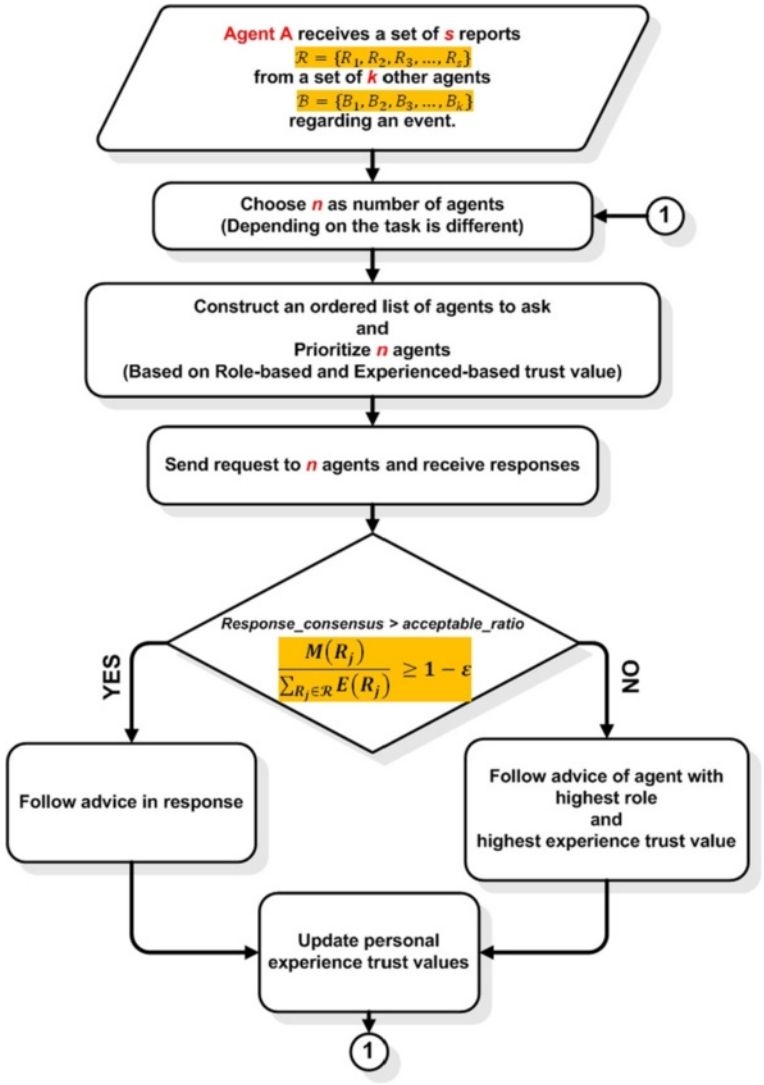

Figure 5 Multifaceted approach to modeling agent trust.

the collection of multiple reports related to the same event and of their weights. At the end, the reports along with their weights are passed to a decision logic module.

Gurung et al. [7] proposed an information-oriented trust model that empowers each individual vehicle with the capability of evaluating the trustworthiness of the possibly large amount of messages received in VANETs, without relying on any infrastructure support such as roadside units or central servers. The proposed trust model 'RMCV' considers several factors that have impact on the trustworthiness of messages including message content similarity, content conflict, and message routing path similarity. The RMCV scheme consists of two main components: (i) message classification and (ii) information-oriented trust model.

Message classification is to identify the messages describing the same event from the potentially large amount of received messages and to cluster these messages using clustering algorithms. In this model, a two-level clustering algorithm is proposed. The first level clustering groups messages describing the same event regardless of the message content. The aim of the second level clustering is to identify conflicting information regarding the same event. The information-oriented trust model is to determine which group of messages is telling the truth. As shown in Figure 8, three important factors affect message trustworthiness, which are content similarity, content conflict, and routing path similarity. Based on these factors, the trust score of each message will be computed at the individual vehicle level.

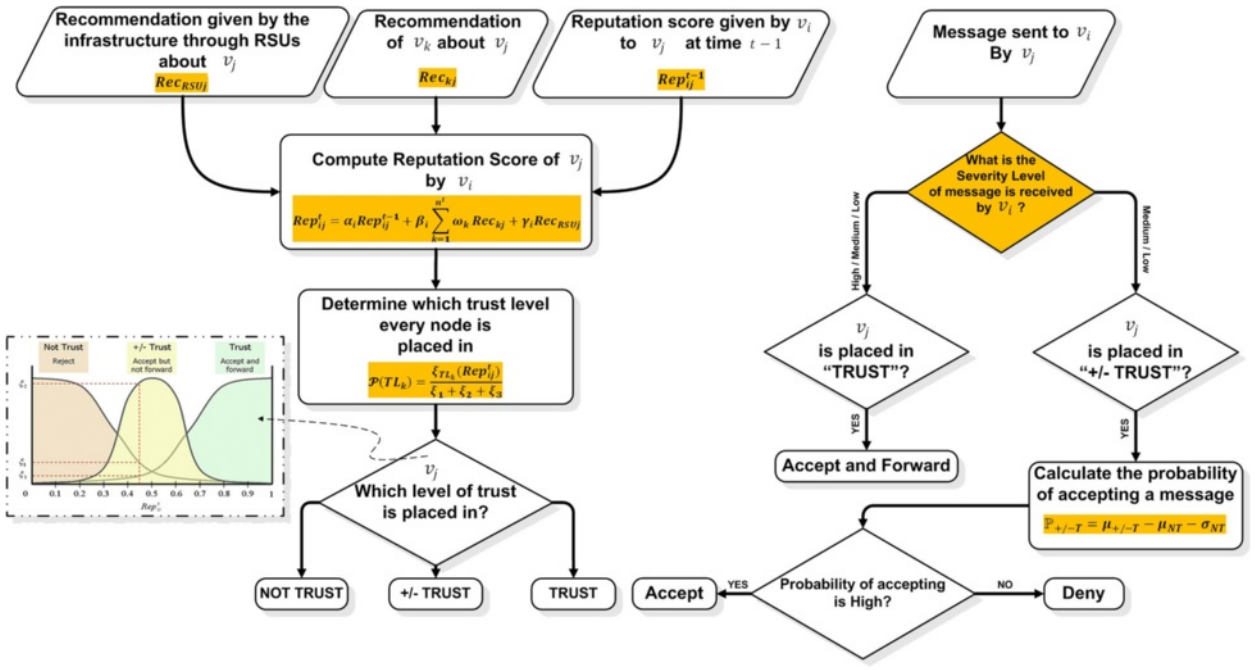

Figure 6 TRIP.

Given a group of messages associated with the same event, similar messages are generally considered to be supportive to one another. It is an important factor to judge the trustworthiness of a message. To model these two effects, two parameters are used: (i) maximum distance (maxD_c) of the content between two messages in the same cluster and (ii) the number of messages (N_c) in the cluster.

The path similarity serves as a penalty value to the support value of a cluster of messages. The more similar the routing paths of messages in the same cluster, the less support to each other will be considered. If similar messages share more common nodes during their routing paths, the risk of messages being tampered increases. Based on the model, three parameters affect routing path similarity: the number of messages (N_c) in the cluster,

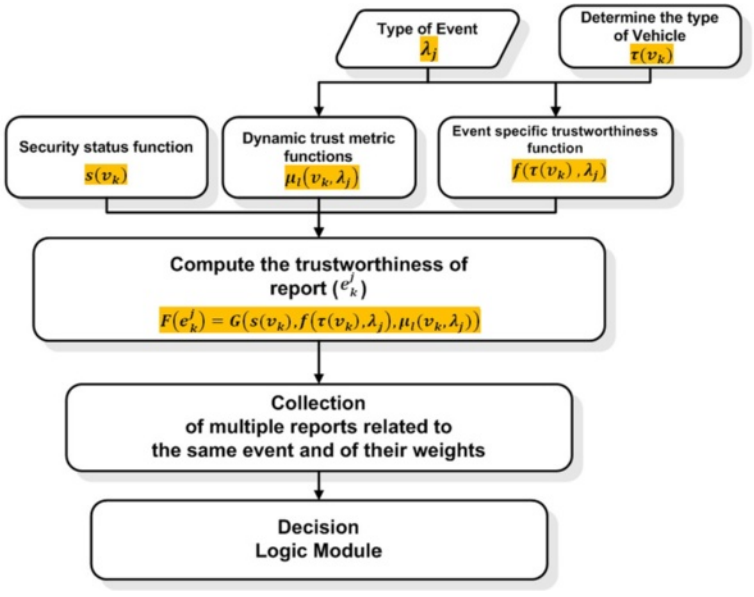

Figure 7 On data-centric trust establishment.

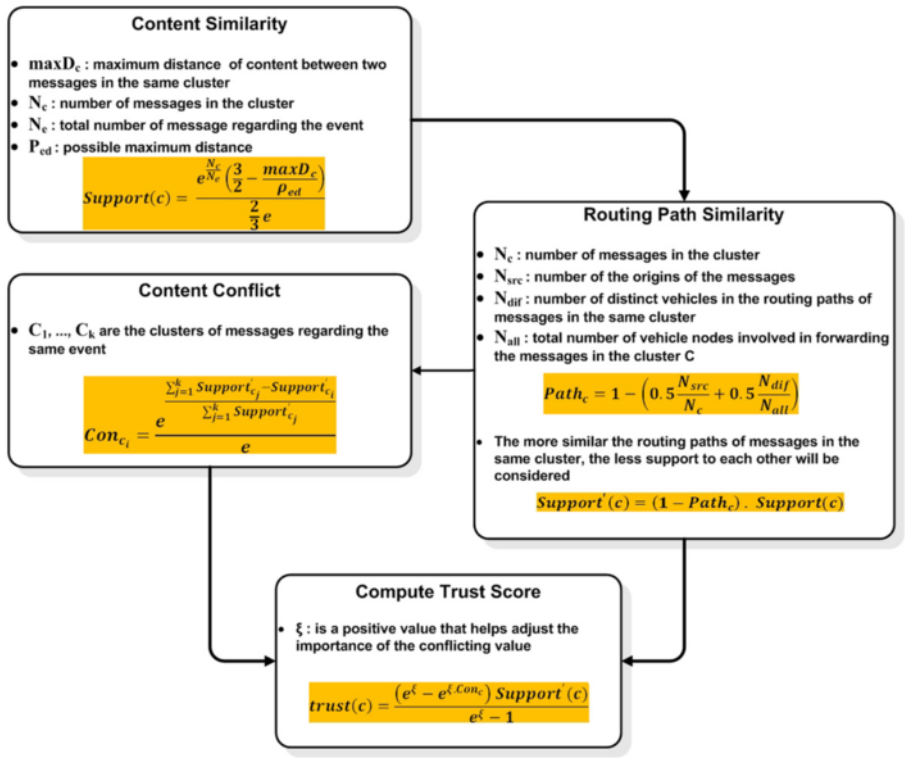

Figure 8 RMCV.

the number of the origins of the messages (N_{src}), and the number of distinct vehicles (N_{dif}) in the routing paths of messages in the same cluster.

Authors mentioned that content conflict can negatively affect the trustworthiness of messages and a higher conflicting value will be obtained if there are more messages against the current cluster (C_i). Suppose that $C_i, \ldots, C_k$ is the clusters of messages regarding the same event and the conflicting value (Con_{c_i}) is for each cluster of messages.

Shaikh and Alzahrani [32] stated that the existing trust models that measure trust based on the history of interactions are not suitable due to the ephemeral nature of VANETs. To deal with this limitation, they proposed an intrusion-aware trust model that works in three phases. The first phase calculates the confidence value, and the second phase calculates the trust value. The last phase takes the decision on message.

According to Figure 9, the confidence value is based on location closeness (L_c), time closeness (T_c), location verification (L_v), and time verification (T_v). To calculate the trust value, the total number of sender nodes (n_{x_k}) and confidence value (C_i) of all the nodes that send a message is required. The decision process comprises of two steps: In the first step, the system will select the message that has a higher trust value. The second step will accept that message if the trust value of the selected message is greater than the minimum acceptable threshold; otherwise, the message will be discarded.

Ding et al. [33] proposed an event-based reputation model to filter bogus warning messages. In this model, vehicles have different roles, and based on this, a dynamic role-dependent reputation evaluation mechanism is presented to determine whether an incoming traffic message is significant and trustworthy to the driver. Reputation functions are designed for these different roles: event reporter, event observer and event participant. Each role has its own reputation evaluation mechanism to determine whether an incoming traffic message is trusted.

As shown in Figure 10, the reputation value of event in the event reporter (ER) will be calculated based on the detection frequency and standard frequency for this type of event. Based on the observing succeeding behavior of ER, the event observer (EO) will calculate the reputation value of event. By integrating data from EOs and EPs, the reputation value of event will be calculated in the event participant (EP). At the end, if the calculated value of the reputation is more than the predefined threshold, the vehicle will send the event message to all neighbors. Otherwise, the event message will be denied.

To prevent the spread of false traffic warning messages, Lo and Tsai [34] proposed an event-based reputation

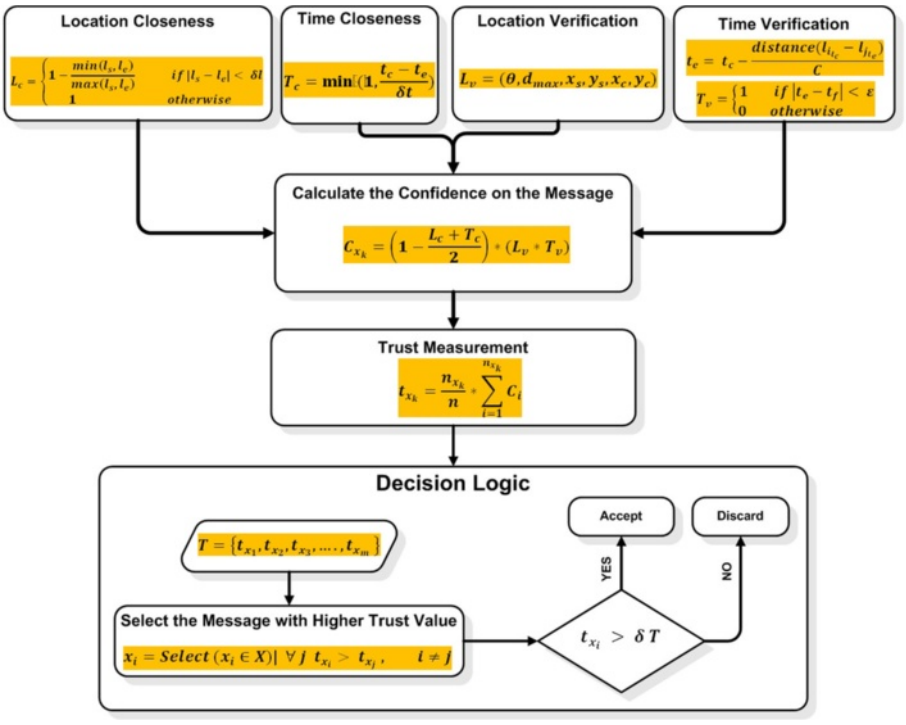

Figure 9 Intrusion-aware trust model.

system, namely, 'ERS'. This model is composed of three interfaces, four functionalities, and one repository for table storage. The decision making is based on the event reputation value and event confidence value. The event reputation value (ER) defines the intensity degree of a traffic event, and its initial value is always set to zero. The event confidence value (EC) indicates the reliability extent of a traffic event. Moreover, the event reputation threshold and event confidence threshold in an ERS are dependent on the sensor capability of a vehicle and

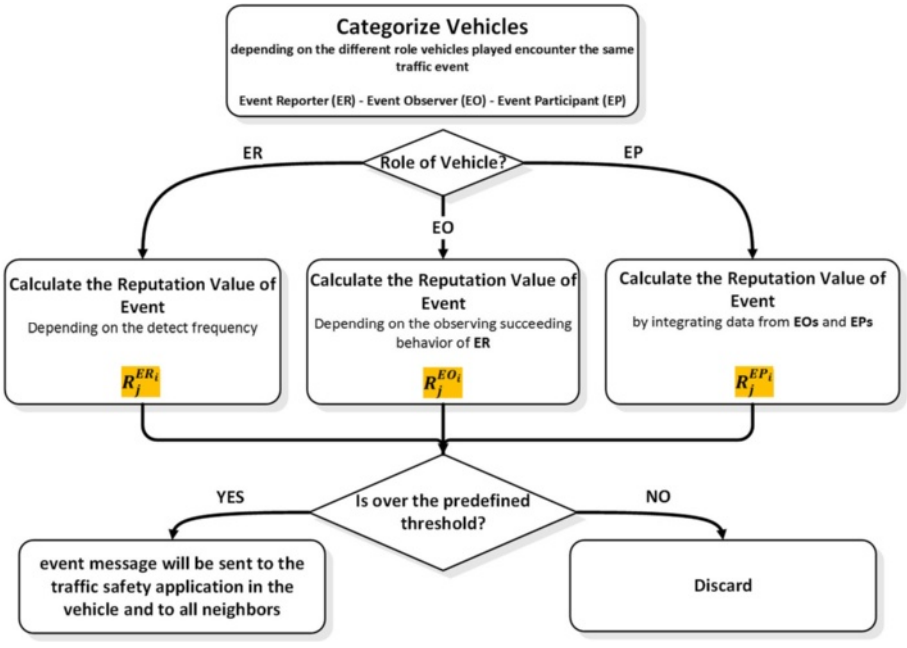

Figure 10 Reputation-based trust model.

the type characteristics of a traffic event. This model is illustrated in Figure 11.

Based on the type of detection, by sensor or by other vehicles, event reputation value collection and event confidence list collection both have different reactions. It means that when a vehicle detects an event with its onboard sensors, the value is increased by one. On the other hand, when a vehicle receives a traffic warning message from another vehicle, the ERS adds the event reputation value in the received message into the field of event reputation value at the same event record in the event table or creates a new event record in the event table.

When a given vehicle detects a traffic event by sensor, the given ERS will append its vehicle's identity into the relevant field in the event confidence list at the corresponding event entry. In contrast, when a vehicle receives a traffic warning message from another vehicle, the content of the event confidence list in the message will be appended in the event confidence list field at the corresponding event entry.

In addition, two important thresholds are introduced in this model, namely, event reputation threshold (ER_{thld}) and event confidence threshold (EC_{thld}). The configuration of the event reputation threshold and event confidence threshold is based on the event type and sensor capability. When ERS detects that the event reputation value and the event confidence value of a traffic event are over the corresponding threshold, it means that the traffic event really exists and is still there. Therefore, the ERS will send this event information through the user interface to notify the driver and at the same time broadcast a traffic warning message with the current event reputation value and the corresponding confidence list to nearby vehicles.

Lo and Tsai mentioned that some traffic safety applications actively send traffic revocation messages to inform other vehicles when an event is resolved. Therefore, in

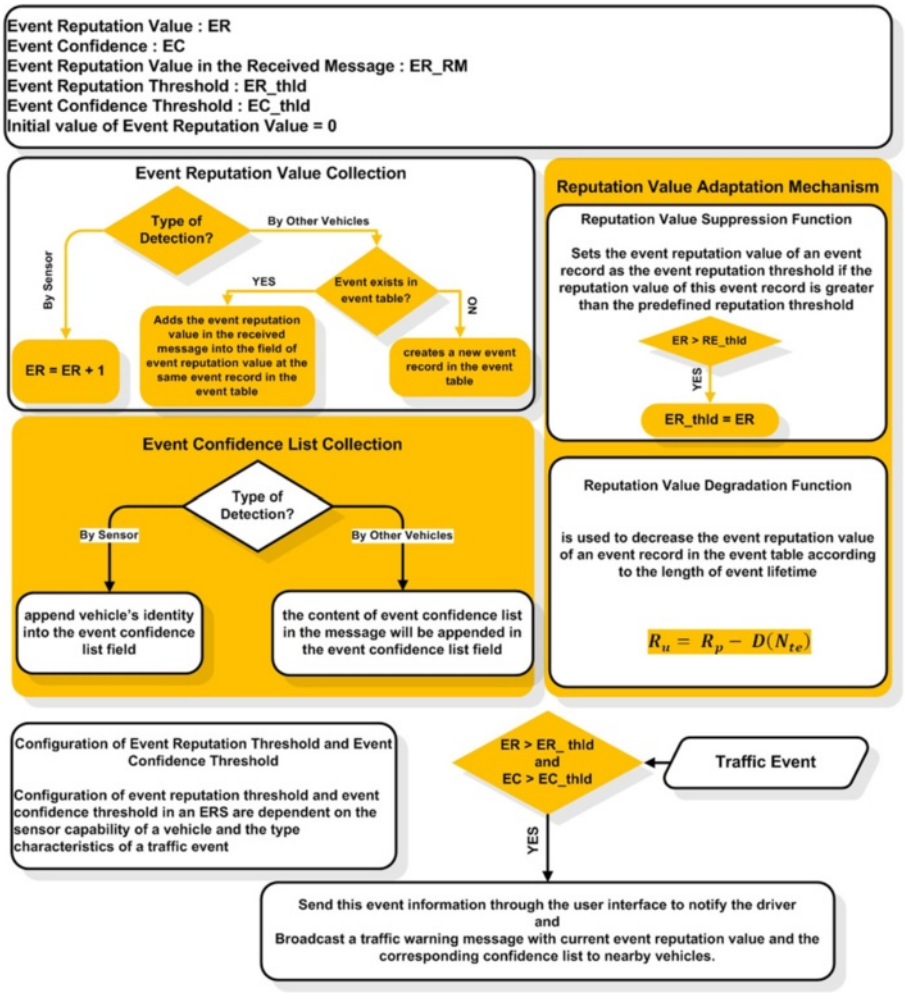

Figure 11 ERS.

order to eliminate the weakness of the event message revocation scheme, the reputation value adaptation mechanism is introduced in ERS. In this mechanism, two functions to control the corresponding event reputation value of a detected event during the event's life time are utilized so that the event status (resolved or not) is reflected by its reputation value. The first function is the reputation value suppression function which sets the event reputation value of an event record as the event reputation threshold if the reputation value of this event record is greater than the predefined reputation threshold. The reputation value suppression function helps ERS to control the maximum value of the reputation measurement. The second function is the reputation value degradation function which is used to decrease the event reputation value of an event record in the event table according to the length of event lifetime.

Wu et al. [35] have also proposed an RSU-aided scheme that is completely data-centric, namely, 'RATE'. The trust establishment, which is executed in RSUs, applied the ant colony optimization algorithm. This model is based on the observation and feedback factors. Upon the detection of an event, vehicles generate observations and corresponding confidence. The observation factor reflects recently reporting frequency of the evidence, together with the confidence of the observer on this piece of evidence and the weight corresponding to reporter's identity. Based on all the confidence and weight, RATE calculates the observation factor. The feedback factor indicates the evidence's practically verified usefulness. The management of feedback consists of three stages: initialization, aging, and promotion. Figure 12 shows the process of RATE.

Upon the reception of observation reports in RSU, RATE puts them in the recently received observation list (L_{ro}). RSUs check the recent observation reports in (L_{ro}) and calculate the observation factor (η) for each piece of evidence (E_i^j). The observation factor will be calculated based on all the confidence $\left(C_i^j\right)$ and weight $\left(W_i^j\right)$.

In RATE, the confidence $\left(C_i^j\right)$ depends on the distance from the vehicle to the event k (D_k), maximum detection range of the vehicle ($D_{\max}$), the number of sensors that can detect the event (N_k), and total number of sensors equipped in the vehicle ($N_{\max}$). In addition, the weight of vehicle $\left(W_i^j\right)$ depends on the type of vehicle. In order to manage the membership of evidence, RATE also uses a quantity threshold (T). Therefore, based on these factors, the following processes will be performed:

- If ($\eta \geq T$) and (E_i^j is not member of L_e), add E_i^j into L_e and $\tau_{\mathrm{init}} = \tau_{\max}$.
- If($\eta \geq T$) and (E_i^j is already in L_e), do nothing.
- If ($\eta < T$) for evidence in L_e, remove them from L_e.

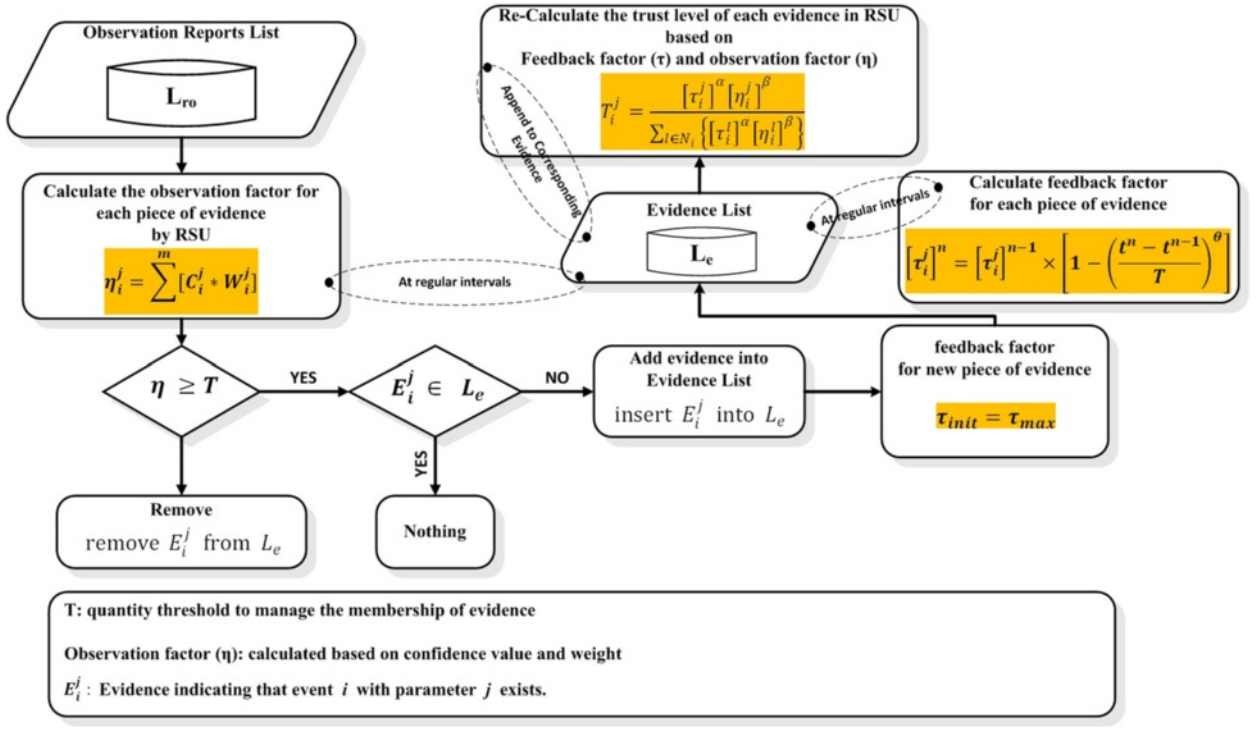

Figure 12 RATE.

In the last step, based on the two factors (τ, η), the trust level of evidence is re-calculated and appended to the evidence. Moreover, RATE will decrease the feedback factor (τ) and will calculate the observation factor (η) of each evidence in L_e at regular intervals.

1.4.3 Combined based trust management

According to [28,36] in the combined based trust model, data trust evaluation is performed using entity trust. The combined trust model aims to determine trustworthiness of the messages based on opinions provided by other vehicles. The basic idea is to suggest a vehicle to trust a message that has been evaluated to be trustworthy by many other trusted peer vehicles [7].

Chen and Wei [36] proposed a beacon-based trust management system namely 'BTM'. It aims to thwart internal attackers from sending false messages in privacy-enhanced VANETs. The proposed model is a hybrid trust management mechanism, which constructs entity trust from beacon messages and computes data trust from cross-checking the plausibility of event messages and beacon messages.

As shown in Figure 13, in order to compute entity trust from beacon messages, cosine similarity is used to compute similarity ($\mathrm{Sim}_{\cos}$) between the claimed position, velocity, and direction with the estimated values. In order to maintain the historical beacon-trust information of neighboring vehicles, a time-based weighting method is proposed to calculate the trustworthiness of beacon messages (T_{bea}).

In this model, data trust depends on the direct event-based trust (T_{devt}) and indirect event-based trust (T_{evt}). In order to compute the trustworthiness of a direct event-based message, a position- and movement-verification mechanism is proposed. By this mechanism, a receiving vehicle is able to evaluate the trustworthiness of the sender vehicle by analyzing both the received event messages and the beacon messages from a vehicle. To compute the similarity between historical beacon messages and received event messages, the Tanimoto coefficient is used.

On the other hand, in this model, when the message receiver establishes trust relationships through the recommendation of other vehicles, the trustworthiness between the sender and receiver should not be more than the trust value between the receiver and the forwarder (T_{opn}), as well as the trust value between the sender and the forwarder. Therefore, based on this assumption, the indirect event-based trust is computed by Equation (1):

$$T_{\mathrm{evt}} = \min(T_{\mathrm{opn}}, T_{\mathrm{devt}}) \tag{1}$$

When a vehicle computes the event trust value T_{evt}, it updates the previous reputation value in order to take the historical event trust value into consideration. Therefore, to compute the reputation value (T_{rep}), the indirect event trust value and the previous reputation value are considered.

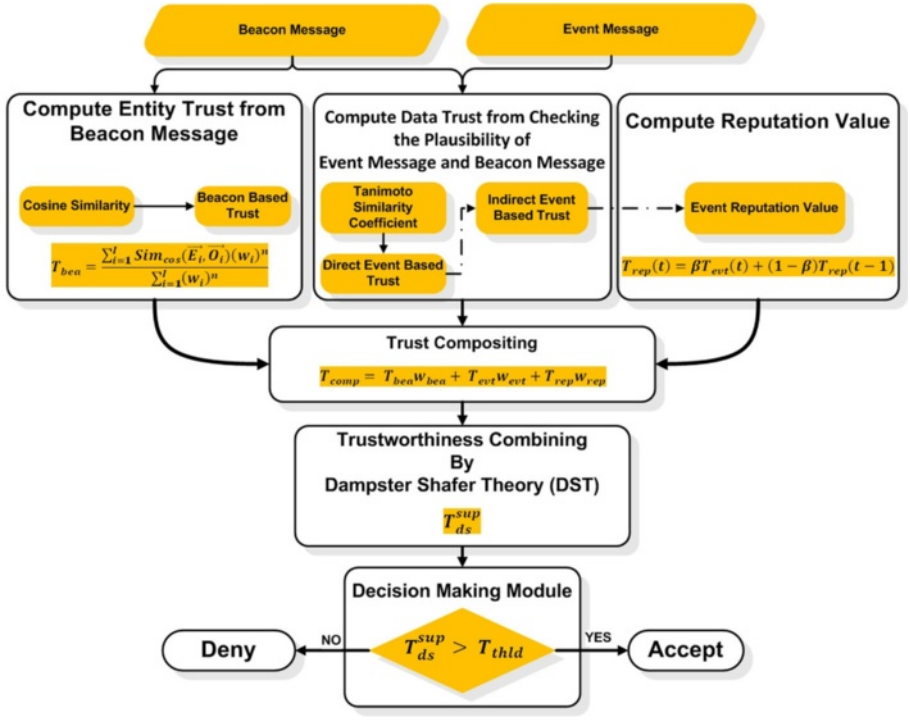

Figure 13 BTM.

In the next step, based on T_{bea}, T_{evt}, and T_{rep}, the composite trustworthiness (T_{com}) of the received event message will be calculated. In addition, due to the fact that vehicle receives a direct event message or an indirect event message opinion transmitted from multiple vehicles, it needs to combine the received opinions and then to determine the overall trustworthiness ($T_{\text{ds}}^{\text{sup}}$) of this event message. In this model, to accommodate the nature of uncertainty of VANETs, the Dempster-Shafer theory (DST) is used for opinion combination. At the end, it will make a decision according the threshold of trust degree T_{thld}.

Wei and Chen [37] also proposed a RSU and beacon-based trust management model, namely, 'RaBTM'. This model allows both OBUs and RSUs to construct entity trust by cross-checking the plausibility of event messages and beacon messages. The objective of the proposed model is to prorogate message opinions quickly while preventing internal attackers from sending or forwarding forged messages in privacy-enhanced VANETs.

According to Figure 14, based on direct and indirect event messages from other vehicles, RaBTM evaluates the combined trust value (T_{ds}) corresponding to the event. To this end, DST is utilized as the evidence combination method.

In addition, if a vehicle also receives the set of original event message from RSUs (R), RaBTM will evaluate the opinion confidence of RSUs (O_{rsu}). Then, the overall event trust value (T_{oval}) will be evaluated based on T_{ds} and O_{rsu}. In the last step, it will make a decision based on the threshold of trust degree (T_{thld}).

1.5 Trust metric

An overview on the proposed trust models shows that based on the objective of the trust model and intended solution, different parameters are applied to measure data/entity trust value. According to [38], these metrics inherit the properties of trust. Therefore, the proper and correct selection of metrics, to achieve the ultimate objectives, is very important when designing and developing a trust model.

Due to the importance of trust metrics, we re-examined the proposed trust models in terms of parameters utilized for measuring the trust value. Table 6 represents the results of this review.

In order to determine the importance degree of each metric, we summarize them in Table 7. Then, based on this table, we analyzed these metrics in terms of repetition rate in the proposed trust models by Microsoft Excel. The results of this assessment are illustrated in Figure 15. According to this diagram, distance, time and recommendation by other vehicles had the highest repetition rate with 60%, 50%, and 50%, respectively. The number of senders at 40% and the type of vehicle at 30% had the next-highest repetition rate. Other parameters had the same repetition rate of 20%. The definition of metrics are as follows:

- *Distance*: refers to location closeness, distance from vehicle to event, distance between the message receiver and the message transmitter, distance between sender and RSU, and distance between RSU and event
- *Time*: refers to time closeness, time delay between the event message time-stamp and the receiver's current time-stamp, and transmission delay
- *Rec. by vehicle*: refers to opinion of vehicle on data/entity
- *Number of sender*: refers to the number of origin entity that create messages and the number of transmitter entity
- *Type of vehicle*: refers to different roles of vehicles on VANETs

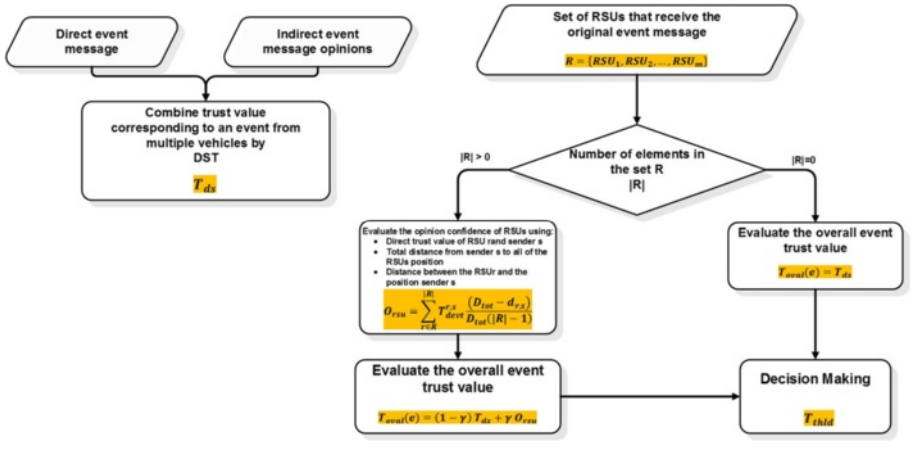

Figure 14 RaBTM.

Table 6 Trust metric

Study	Metric
Multifaceted approach	Time closeness (T_c)
	Location closeness (L_c)
	Role-based trust value (T_r) :
	•*Authority* • *Expert* • *Seniority* • *Ordinary*
	Experience-based trust value (T_e): depends on the number of interaction
TRIP	Direct previous experiences with the target node (Rep_{ij})
	Recommendations from other surrounding vehicles (Rec_{kj})
	Recommendation from central authority through roadside units ($\text{Rec}_{\text{RSU}j}$)
Data-centric	Dynamic trustworthiness factors, e.g., location and time ($\boldsymbol{\mu}_l$)
	Event-specific trust ($\boldsymbol{\lambda}_j$)
	Security status ($s(v_k)$)
	Type of vehicle ((v_k))
RMCV	*Content similarity* (supprt(c))
	- Maximum distance of content between two messages in the same cluster
	- Possible maximum distance - number of messages
	Content conflict (Con_c)
	Route similarity (Path_c)
	- Number of messages in the cluster
	- Number of source providers
	- Number of distinct vehicles in the routing paths of messages in the same cluster
Intrusion-aware trust model	*Confidence value* (C_i)
	- Location closeness (L_c)
	- Time closeness (T_c)
	- Location verification (L_v)
	- Time verification (T_v)
	Total number of sender nodes (n_{x_k})
Reputation-based trust model	Real event frequency (E_f)
	Standard frequency of event (E_s)
	Degree behavior deviation (D_k)
	Number of all vehicles sent the message to other vehicles (m, n, k, l)
ERS	*Event reputation value*: indicates the intensity degree of an event
	Event confidence value: indicate the reliability extent of an event and the value is the number of vehicles that received the message
RATE	*Observation factor* ($\boldsymbol{\tau}$)
	- Distance from vehicle to event
	- Maximum detection range of the vehicle
	- Number of sensors that can detect the event
	- Total number of sensors equipped in the vehicle
	feedback factor ($\boldsymbol{\eta}$)
BTM	*Beacon-based Trust* (T_{bea})
	- Similarity between beacon and estimate value (Sim_{cos})
	Vehicle's position
	Velocity
	Drive direction
	Direct event-based trust (T_{devt})

Table 6 Trust metric *(Continued)*

	- Similarity between historical beacon and received event message (Sim_{tan})
	Vehicle's position
	Velocity
	Drive direction
	- Distance between the message receiver and the message transmitter (Δd)
	- Time delay between the event message time-stamp and the receiver's current time-stamp (Δt)
	- Maximum transmission distance (D_{max})
	- Maximum transmission delay (T_{max})
	Indirect event-based trust (T_{evt})
	Recommendation of other vehicles (T_{opn})
	Reputation and trust compositing (T_{rep})
RaBTM	Opinion confidence of RSU (O_{rsu})
	Direct trust value ($T^{r,s}_{devt}$)
	- Transmission distance
	- Transmission delay
	Distance between sender and RSU (D_{tot})
	Distance between RSU and event ($d_{r,s}$)

- *Experience*: refers to the experience of a vehicle on the event/other vehicles
- *Rec. by RSU*: refers to opinion of RSU on data/entity
- *Velocity*: refers to speed of a vehicle
- *Vehicle position*: refers to the position of a vehicle
- *Vehicle direction*: refers to the direction of a vehicle
- *Type of event*: refers to different events in terms of safety or non-safety and severity

1.6 Evaluation and comparison of trust models

Development of an appropriate trust model requires a set of characteristics and parameters that should be taken into account when designing. These parameters are based on the challenges in a VANET environment. In [22], several parameters as requirements of a trust model have been identified. They mentioned that a suitable trust model should be accurate, scalable, simple and fast, resilient to security and privacy threats, and independent of mobility patterns. Zhang [28] also proposed a set of properties including decentralization, scalability, sparsity, privacy, security, confidentiality, dynamics, and robustness, which are requirements that effective trust management should take into account. In [32], other features as requirements of the trust model have been identified. They introduced anonymity, scalability, decentralization, and dynamics as requirements of the trust model. They also stated that the trust model should be able to detect fake locations and false time-stamps.

In this study, to perform qualitative comparison, we have selected the following parameters as the trust model's requirements (Table 8): (i) complexity, (ii) dynamics, (iii) scalability, (iv) decentralization, (v) security level, and (vi) privacy.

- *Complexity*: High mobility is the main feature in a VANET environment. Therefore, a simple and fast trust model is required. In this study, to evaluate the complexity of the trust model, time complexity is considered as the main factor. Time complexity refers to the amount of time taken by the trust model in both the main process (trust measurement) and pre-process (operations before trust measurement). Based on these factors, we found TRIP and the reputation-based trust model as simple and low-complexity models. In contrast, due to the operations in pre-processing, RMCV and RATE have high complexity.
- *Dynamics*: Rapid change network topology and different traffic densities are other features in a VANET environment. The frequent topology change can cause link breakage, and changes in traffic density from sparse to heavy and vice versa leads to a negative impact on information dissemination. Therefore, a dynamic trust model is needed to deal with these situations. To this end, independent of mobility pattern, low dependence on infrastructure and dynamic trust metric are requirements to develop a dynamic trust model. We have compared the existing trust models based on these definitions. The results of comparisons show that most, but not all, proposed data-based trust models are completely dynamic and entity-based models are somewhat dynamic. In other

Table 7 Summary of trust metrics in the proposed trust model

	Metrics										
Study	**Time**	**Distance**	**Rec. by vehicle**	**Rec. by RSU**	**Experience**	**Number of sender**	**Velocity**	**Vehicle position**	**Vehicle direction**	**Type of vehicle**	**Type of event**
A multifaceted approach	✓	✓		✓	✓					✓	
TRIP			✓	✓	✓						
On data-centric	✓	✓								✓	✓
RMCV						✓					
Intrusion-aware trust model	✓	✓				✓					
Reputation-based trust model			✓			✓				✓	
ERS			✓			✓					✓
RATE		✓									
BTM	✓	✓	✓				✓	✓	✓		
RaBTM	✓	✓	✓	✓			✓	✓	✓		

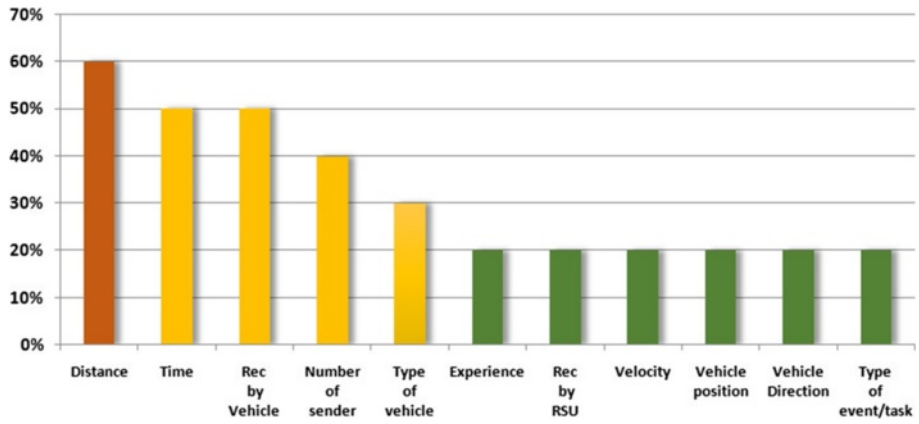

Figure 15 Comparison trust metrics based on repetition rate.

words, infrastructure-less trust models are more dynamic than infrastructure-based ones.

- *Scalability*: Scalability, as a crucial feature in VANETs, is the ability of a system to handle the addition of vehicles or entities without suffering a noticeable loss in performance or increase in administrative complexity [39]. Based on this definition, the trust model should have the same performance in the face of different network sizes and traffic densities. Due to the existence of duplicated data/event sent by vehicles, especially in the high traffic density, most of the proposed data-based trust models, but not all, are somewhat scalable. In addition, due to the lack of necessary infrastructure in all VANETŠs environment, the trust models that are highly dependent on RSU cannot be completely scalable.
- *Decentralization*: Due to the extensive VANET environment as well as distributed communication in vehicular *ad hoc* networks, decentralization is another requirement in the trust model.
- *Security level*: In vehicular *ad hoc* networks, the accuracy of a message requires authentication of the sender. In other words, authentication as one of the security requirements [40] ensures that the message sent by the sender is valid. Moreover, cryptography as a technique for secure communication is another requirement of security. In order to identify the level of security of the proposed trust models, we review them in terms of authentication and encryption/decryption method. The results indicate the weakness of the trust models in this regard.
- *Privacy*: The personally identifiable information and location data are indeed among the most sensitive data. Because the basis of VANETs is the exchange of data between entities, data privacy is an important issue. Therefore, location and data privacy as a property in the trust model is required.

Based on the trust model requirements mentioned above, we extracted the properties of the trust models that

Table 8 Qualitative comparison

	Metrics					
Study	**Complexity**	**Decentralization**	**Dynamics**	**Scalability**	**Privacy**	**Security level**
A multifaceted approach	Somewhat simple	Y	Y	SW	SW	SW
TRIP	Simple	Y	SW	SW	N	N
On data-centric	Somewhat simple	Y	Y	SW	N	SW
RMCV	Complex	Y	Y	SW	N	N
Intrusion-aware trust model	Somewhat simple	Y	Y	Y	SW	N
Reputation-based trust model	Simple	Y	Y	SW	N	SW
ERS	Somewhat simple	Y	Y	Y	N	N
RATE	Complex	Y	SW	SW	N	Y
BTM	Somewhat simple	Y	Y	Y	Y	Y
RaBTM	Simple	Y	SW	Y	N	N

Note: Y, yes; N, no; SW, somewhat.

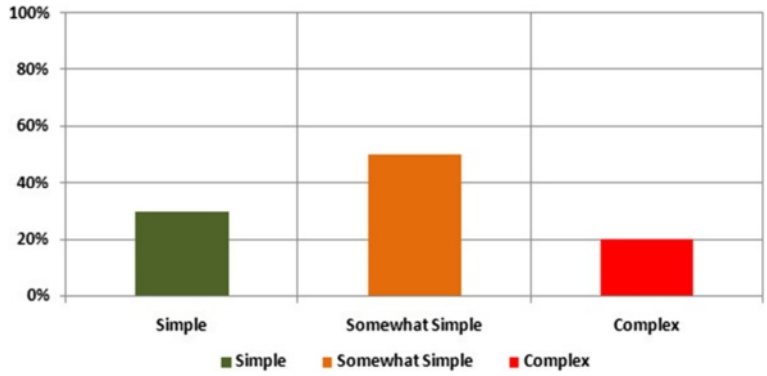

Figure 16 Analysis of proposed trust models based on complexity.

were surveyed in the previous section. Table 8 represents the results of the review. According to these results, we can conclude that none of the trust models have achieved all the desired requirements.

For a better understanding of the performance of the proposed trust models, two diagrams also are provided based on the complexity and other requirements in Figure 16 and Figure 17, respectively.

According to the bar graph in Figure 16, 30% of the proposed trust models in this study have low complexity and 20% of them have high complexity. In addition, 50% of the models are somewhat simple. The bar graph in Figure 17 shows which 70% of trust models have not satisfied privacy as a requirement. In addition, 50% of the models are lacking a proper security level.

1.6.1 Fuzzy trust model

According to the previous sections, to design and develop a new trust model in vehicular *ad hoc* networks, two important issues should be considered: (i) properties of the trust model and (ii) trust metrics. In [38], Wolfson et al. stated that trust metrics inherit the properties of trust. Therefore, to determine the appropriate trust metrics, properties of the trust model must be considered. Furthermore, trust metrics should be able to satisfy the trust model's properties. This interaction is shown in Figure 18.

Based on the trust model development process as well as trust model strategies that were discussed previously, we build our own strategy by taking advantage of the positive aspects of existing solutions. In the proposed framework, a fuzzy logic-based method is used based on the following reasons. First, trust has a fuzzy nature and it is indefinite or imprecise [41]. Second, trust is a graded phenomenon that is difficult to estimate experimentally. Third, the decision on trust is not straightforward because of its uncertainty. Fuzzy logic provides a natural framework to deal with its uncertainty and the tolerance of imprecise data inputs. Since the trust value is between the absolute trust and absolute mistrust, fuzzy techniques can be effectively used for trust decisions. Tajeddine et al. [42] stated that fuzzy logic is based on natural language and it is conceptually easy to understand. Furthermore, the calculation and measurement of trust in unsupervised *ad hoc* environments involve complex aspects such as credibility rating for opinions delivered by a vehicle, the

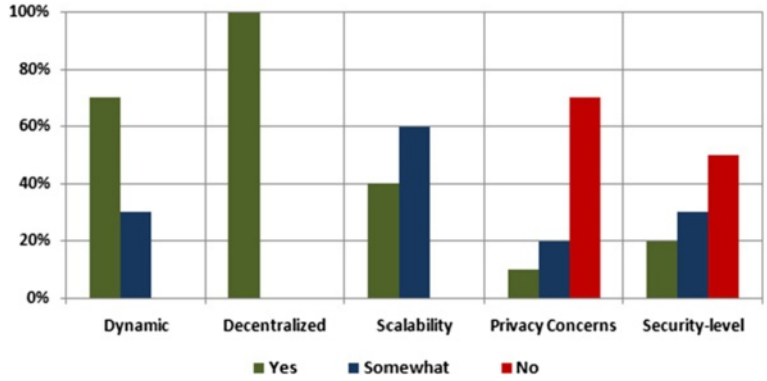

Figure 17 Performance of proposed trust models based on requirements.

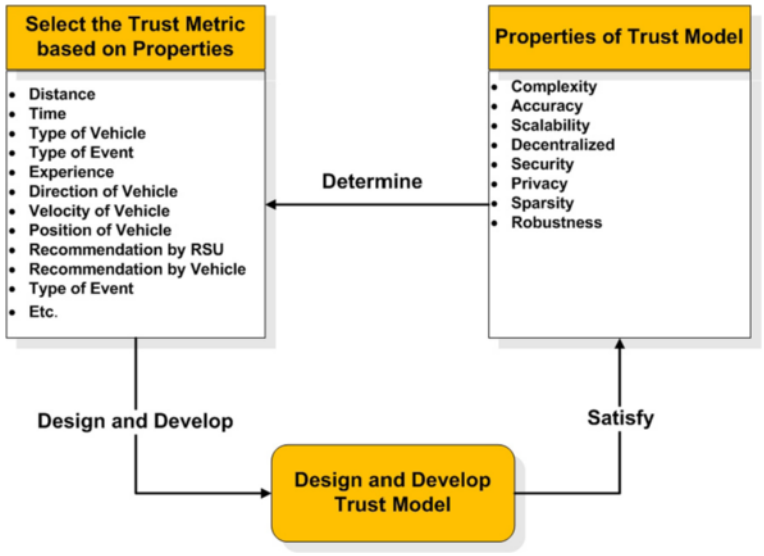

Figure 18 Process to develop a trust model.

honesty of recommendations provided by a vehicle, or the assessment of past experiences with the vehicle one wishes to interact with. The deployment of suitable algorithms and models imitating fuzzy logic can help to solve these problems [15].

In terms of data gathering, there are two existing solutions to get application system input [43]. One is to receive incoming messages by wireless antenna from RSUs and other vehicles. The other one is detecting data reported by sensors. In the proposed framework, to evaluate trustworthiness of messages/data, four main modules are considered: probability of event occurrence module, misbehavior detection module, trust measurement module, and decision making module. As shown in Figure 19, when a vehicle receives a traffic event by the information gathering module, based on some factors such as position of the sender/receiver, time of sending/receipt of data, time of event occurrence, distance to event, and velocity of the sender/receiver, the plausibility of data is checked. To this end, we proposed a misbehavior detection system (MDS) module based on fuzzy logic. In this module, a set of rules is used to represent the inference engine (knowledge base). Also, we proposed a module based on fuzzy logic to compute the probability of event occurring called PEO. Given that the probability of an event largely depends on environmental conditions, this module computes the probability of an event based on the vehicular environment conditions such as weather, lighting, type of the event location (urban area, rural area, highway, and so on) and traffic density. This module decides whether the reported event is probably true or not and what is the probability of the occurrence of the event. Then, the trust value of the event is measured by the trust measurement (TM) module. In this module, to measure the trust value, several parameters are considered such as similarity among received data, type of entity, experience, direction of vehicle movement, plausibility level, and probability of occurrence of the event. At the end, the results of previous steps are used in the decision making module to decide whether the reported event is trustworthy or not. This module is a multi-criteria fuzzy decision making and works based on the type of event (safety and non-safety) and level of plausibility of event. Furthermore, the proposed model addresses the properties of the trust model discussed in the previous section. In brief, the proposed framework considers various aspects to assess the trustworthiness of the reported event such as plausibility and probability. As compared to the existing trust models in literature, the proposed model not only increases the accuracy of trust evaluation but also enhances the performance of the model in different traffic densities. However, traditional drawbacks in fuzzy logic methods exist in the proposed fuzzy logic approach. In addition, having a variety of locations and events in a vehicular environment, the definition of a flexible and robust rule is still an open research issue for fuzzy models in VANETs. The proposed framework is shown in Figure 19.

2 Conclusions

The trust model enables vehicles to distinguish trustworthy vehicles or messages from untrustworthy ones. It leads to reducing the risk of vehicles being misguided by other malicious vehicles. Due to the importance of data and its quality in VANETs as well as the impact of trustworthiness on the quality of applications, this study has

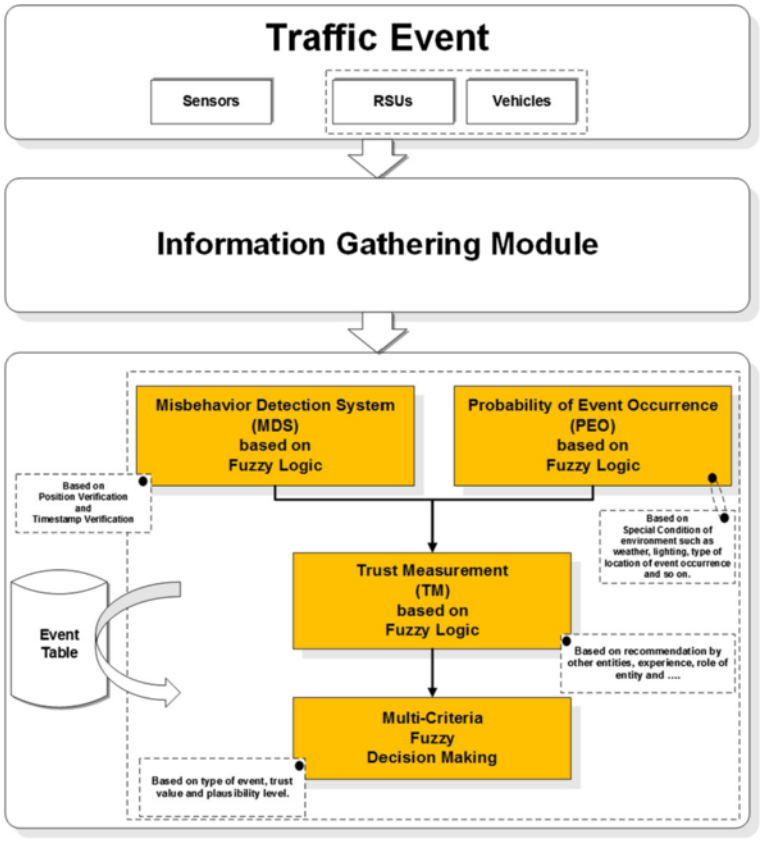

Figure 19 Our proposal.

conducted a systematic review of current research that aim at managing trust in vehicular *ad hoc* networks.

In this review, we have analyzed various studies focusing on trust models. Based on this analyze, we have extracted the methods and metrics that are required for designing and managing a trust model. We have concluded that none of the proposed trust models have achieved all the desired properties. Therefore, we developed a framework including probability module, plausibility module, trust measurement module, and decision making module. These modules are based on fuzzy logic. In terms of contributions to the theory, this paper gathers published works on trust models and allows researchers to find possible avenues for future studies in this area.

Looking into the future, development of a lightweight intelligence trust model for VANETs that satisfies all the desired properties of a trust model is sensible.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor Malaysia. [2]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia. [3]Communication System and Network (iKohza) Research Group, Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Jalan Semarak, 54100 Kuala Lumpur, Malaysia.

Received: 25 November 2014 Accepted: 7 April 2015
Published online: 23 May 2015

References

1. J Yin, T ElBatt, G Yeung, B Ryu, S Habermas, H Krishnan, T Talty, in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*. Performance evaluation of safety applications over DSRC vehicular ad hoc networks (ACM, Philadelphia, PA, USA, 2004), pp. 1–9
2. G Yan, S Olariu, MC Weigle, Providing VANET security through active position detection. Comput. Commun. **31**(12), 2883–2897 (2008)
3. Y-C Wei, Y-M Chen, in *Information Security Applications,13th International Workshop, WISA 2012*. Efficient self-organized trust management in location privacy enhanced VANETs (Springer, Jeju Island, Korea, 2012), pp. 328–344
4. Q Li, A Malip, KM Martin, S-L Ng, J Zhang, A reputation-based announcement scheme for VANETs. IEEE Trans. Vehicular Technol. **61**(9), 4095–4108 (2012)
5. F Dotzer, L Fischer, P Magiera, in *Sixth IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*. VARS: a vehicle ad-hoc network reputation system (IEEE, Taormina, Giardini Naxos, 2005), pp. 454–456
6. M Raya, J-P Hubaux, Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
7. S Gurung, D Lin, A Squicciarini, E Bertino, in *Network and System Security*. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks (Springer, 2013), pp. 94–108

8. ET Rother, Systematic literature review x narrative review. Acta Paulista de Enfermagem. **20**(2), vii–viii (2007)
9. B Kitchenham, S Charters, Guidelines for performing systematic literature reviews in software engineering (2007). http://www.dur.ac.uk/ebse/resources/Systematic-reviews-5-8.pdf
10. B Kitchenham, Procedures for performing systematic reviews. Keele, UK, Keele Univ. **33**, 2004 (2004)
11. A Bakshi, A Talaei-Khoei, P Ray, Adaptive policy framework: a systematic review. J. Netw. Comput. Appl. **36**(4), 1261–1271 (2013)
12. J Chai, JN Liu, EW Ngai, Application of decision-making techniques in supplier selection: a systematic review of literature. Expert Syst. Appl. **40**(10), 3872–3885 (2013)
13. D Gambetta, Can we trust trust. Trust: making and breaking cooperative relations. Department of Sociology, University of Oxford, chapter 13, 213–237 (2000)
14. M Gerlach, in *Eighth International Symposium on Autonomous Decentralized Systems, ISADS'07*. Trust for vehicular applications (IEEE, Washington, DC, USA, 2007), pp. 295–304
15. J Luo, X Liu, M Fan, A trust model based on fuzzy recommendation for mobile ad-hoc networks. Comput. Netw. **53**(14), 2396–2407 (2009)
16. S Mandala, AH Abdullah, AS Ismail, H Haron, M Ngadi, Y Coulibaly, *et al*, in *3rd International Conference On Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME)*. A review of blackhole attack in mobile adhoc network (IEEE, TB Bandung, Indonesia, 2013), pp. 339–344
17. S Mandala, K Jenni, MA Ngadi, M Kamat, Y Coulibaly, in *Second International Symposium, SSCC 2014*. Quantifying the severity of blackhole attack in wireless mobile adhoc networks (Springer, Delhi, India, 2014), pp. 57–67
18. Y Sun, W Yu, Z Han, KR Liu, in *IEEE Global Telecommunications Conference,GLOBECOM'05*. Trust modeling and evaluation in ad hoc networks, vol. 3 (IEEE, St. Louis, Missouri, 2005), p. 6
19. YL Sun, Y Yang, in *IEEE International Conference On Communications, ICC'07*. Trust establishment in distributed networks: analysis and modeling (IEEE, Glasgow, Scotland, UK, 2007), pp. 1266–1273
20. M Monir, A Abdel-Hamid, MA El Aziz, in *First International Conference, SecNet 2013*. A categorized trust-based message reporting scheme for vanets (Springer Cairo, Egypt, 2013), pp. 65–83
21. J Wang, Y Liu, X Liu, J Zhang, in *IEEE Intelligent Vehicles Symposium*. A trust propagation scheme in VANETs (IEEE, Xi'an, China, 2009), pp. 1067–1071
22. F Gómez Mármol, G Martínez Pérez, TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. J. Netw. Comput. Appl. **35**(3), 934–941 (2012)
23. X Li, J Liu, X Li, W Sun, in *5th International Conference On Intelligent Networking and Collaborative Systems (INCoS)*. RGTE: a reputation-based global trust establishment in VANETs (IEEE, Xi'an, China, 2013), pp. 210–214
24. N Bißmeyer, J Njeukam, J Petit, KM Bayarou, in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*. Central misbehavior evaluation for VANETs based on mobility data plausibility (ACM UK, 2012), pp. 73–82
25. P Wex, J Breuer, A Held, T Leinmuller, L Delgrossi, in *IEEE Vehicular Technology Conference*. Trust issues for vehicular ad hoc networks (IEEE, Calgary, AB, Canada, 2008), pp. 2800–2804
26. X Hong, D Huang, M Gerla, Z Cao, in *Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture*. SAT: situation-aware trust architecture for vehicular networks (ACM Seattle, WA, USA, 2008), pp. 31–36
27. Z Huang, S Ruj, MA Cavenaghi, M Stojmenovic, A Nayak, A social network approach to trust management in VANETs. Peer-to-Peer Netw. Appl. **7**(3), 229–242 (2014)
28. J Zhang, Trust management for VANETs: challenges, desired properties and future directions. Int. J. Distributed Syst. Technol. (IJDST). **3**(1), 48–62 (2012)
29. J Grover, MS Gaur, V Laxmi, in *Wireless Networks and Security*. Trust establishment techniques in VANET (Springer, 2013), pp. 273–301
30. UF Minhas, J Zhang, T Tran, R Cohen, A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. IEEE Trans. Syst. Man Cybern. C Appl. Rev. **41**(3), 407–420 (2011)
31. M Raya, P Papadimitratos, VD Gligor, J-P Hubaux, in *The 27th Conference on Computer Communications, INFOCOM 2008*. On data-centric trust establishment in ephemeral ad hoc networks (IEEE, Phoenix, AZ, USA, 2008)
32. RA Shaikh, AS Alzahrani, Intrusion-aware trust model for vehicular ad hoc networks. Secur. Commun. Netw. (2013)
33. Q Ding, X Li, M Jiang, X Zhou, in *International Conference On Wireless Communications and Signal Processing (WCSP)*. Reputation-based trust model in vehicular ad hoc networks (IEEE, Suzhou, China, 2010), pp. 1–6
34. N-W Lo, H-C Tsai, A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP J. Wireless Commun. Netw. **2009**, 9 (2009)
35. A Wu, J Ma, S Zhang, in *7th International Conference On Communications, Networking and Mobile Computing (WiCOM)*. RATE: a RSU-aided scheme for data-centric trust establishment in VANETs (IEEE, Wuhan, China, 2011), pp. 1–6
36. Y-M Chen, Y-C Wei, A beacon-based trust management system for enhancing user centric location privacy in VANETs. J Commun. Netw. **15**(2), 153–163 (2013)
37. Y-C Wei, Y-M Chen, in *Human Centric Technology and Service in Smart Space, HumanCom 2012*. Reliability and efficiency improvement for trust management model in VANETs (Springer, 2012), pp. 105–112
38. S Ma, O Wolfson, J Lin, in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science*. A survey on trust management for intelligent transportation system (ACM Chicago, IL, USA, 2011), pp. 18–23
39. T Kosch, CJ Adler, S Eichler, C Schroth, M Strassberger, The scalability problem of vehicular ad hoc networks and how to solve it. IEEE Wireless Commun. **13**(5), 22–28 (2006)
40. S Goudarzi, AH Abdullah, S Mandala, SA Soleymani, MAR Baee, MH Anisi, MS Aliyu, in *the 2nd Symposium on Wireless Sensors and Cellular Networks WSCN'13)*. A systematic review of security in vehicular ad hoc network (Jeddah, Saudi Arabia, 2013), pp. 1–10
41. EJ Chang, FK Hussain, TS Dillon, in *Proceedings of the 2005 Workshop on Secure Web Services*. Fuzzy nature of trust and dynamic trust modeling in service oriented environments (ACM, Alexandria, VA, USA, 2005), pp. 75–83
42. A Tajeddine, A Kayssi, A Chehab, H Artail, Fuzzy reputation-based trust model. Appl. Soft Comput. **11**(1), 345–355 (2011)
43. N-W Lo, H-C Tsai, in *IEEE Globecom Workshops*. Illusion attack on VANET applications - a message plausibility problem (IEEE, Washington, DC, USA, 2007), pp. 1–8
44. L Buttyán, J-P Hubaux, Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Netw. Appl. **8**(5), 579–592 (2003)
45. N Bißmeyer, C Stresing, KM Bayarou, in *Second IEEE Vehicular Networking Conference(VNC)*. Intrusion detection in VANETs through verification of vehicle movement data (IEEE, Jersey City, New Jersey, USA, 2010), pp. 166–173
46. N Bißmeyer, S Mauthofer, B Kpatcha, F Kargl, *Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters* (IEEE, Seoul, Korea, 2012), pp. 78–85
47. A Avizienis, J-C Laprie, B Randell, C Landwehr, Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Secure Comput. **1**(1), 11–33 (2004)
48. O Abumansoor, A Boukerche, in *IEEE Global Telecommunications Conference (GLOBECOM)*. Towards a secure trust model for vehicular ad hoc networks services (IEEE, Houston, Texas, USA, 2011), pp. 1–5