Arshad *et al. EURASIP Journal on Wireless Communications and Networking* (2018) 2018:62
https://doi.org/10.1186/s13638-018-1064-y

EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

A survey of local/cooperative-based malicious information detection techniques in VANETs

Muhammad Arshad[1], Zahid Ullah[1], Naveed Ahmad[2], Muhammad Khalid[3], Haithiam Criuckshank[4] and Yue Cao[3*]

Abstract

Vehicular ad hoc networks (VANETs) are emerged technology where vehicles and roadside units (RSUs) communicate with each other. VANETs can be categorized as a subbranch of mobile ad hoc networks (MANETs). VANETs help to improve traffic efficiency and safety and provide infotainment facility as well. The dissemination of messages must be relayed through nodes in VANETs. However, it is possible that a node may propagate false information in a network due to its malicious behaviour or selfishness. False information in VANETs can change drivers' behaviour and create disastrous consequences in the network. Therefore, sometimes false safety messages may endanger human life. To avoid any lass, it is more important to detect and avoid false messages. This paper has explained some important algorithms that can detect false messages in VANETs. The categorization of false message detection schemes based on local and cooperative behaviour has been presented in this article. The limitations and consequences of existing schemes as well as future work has been discussed.

Keywords: VANETs, MANETs, Misbehaviour, False message detection, Security

1 Review

This article analyses Single/local and Cooperative based malicious information detection techniques in VANETs. Single/local based detection schemes are further comprised of plausibility, consistency and single node behavior. However, these techniques performances are not upto the mark, because of single node reliance. The cooperative based detection techniques are more efficient than Single/local based detection schemes. The prerequisites for these scheme need more nodes, unlike Single/local based detection schemes. These techniques are classified based on consistency and behavior with neighbors. Trust-based detection techniques are analysed on previous communication history. However, these scheme needs a honest and sufficient number of nodes for reliable result.

*Correspondence: yue.cao@northumbria.ac.uk
[3]Department of Computer & Information Sciences, Northumbria University, NE1 8ST, Newcastle upon Tyne, UK
Full list of author information is available at the end of the article

2 Introduction

Vehicular ad hoc networks (VANETs) have got much importance for road side safety, security and traffic efficiency in recent years. VANETs have emerged as subclass of mobile ad hoc networks (MANETs). VANETs are having various differences in properties from MANETs; therefore, protocols of MANETs cannot directly be applied to VANETs [1]. In recent announcements from car manufacturers, they have equipped their vehicles with wireless access vehicular environment (WAVE) devices. WAVE protocols are based on IEEE 802.11p standard and provide basic radio standard for dedicated short-range communication (DSRC) in VANETs [2–5]. The DSRC protocol is used for vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication [6]. Every vehicle consists of an on-board unit (OBU), which broadcasts messages about its position, speed and other events. OBU has the capability to verify incoming messages from valid entities. Roadside units (RSUs) are fix units which monitor vehicle activities and collect important information about nearest vehicles [5, 7, 8]. Vehicular communication consist of two types of messages. Periodic messages show

presence of vehicle in network and emergency messages, which are propagated in the occurrence of some damaging event(s) [3]. Various applications of VANETs exist on road safety, passenger comfort and traffic efficiency [9, 10].

In the future, VANETs will decrease road accidents by providing real-time information about traffic and road status to drivers [9]. The public key infrastructure (PKI) has been developed for VANETs' security. The PKI concentrates on data integrity and authentication schemes. It provides traditional solutions for VANETs' communication [11]. The certificate authorities (CAs) are responsible for maintaining credentials of vehicles in network [7, 12]. However, in V2V communication node, misbehaviour may propagate false messages, where a single malicious node may disturb the whole network [13]. False messages in VANETs can create many issues like higher time required to reach destination, more fuel consumption, higher pollution and traffic accidents [6, 14]. The emergency messages are relayed in multi-hop fashion in the network. Bandwidth may become limited due to broadcasting of false messages. There must be some mechanisms to detect and avoid these false messages [3]. A malicious vehicle can broadcast false position information in the network that has adverse consequences in safety applications [15–20]. VANETs' routing, safety application, traffic management and data aggregation rely on correct vehicle position information [21, 22].

This article has investigated current research efforts on false data detection schemes, like false messages and false position information detection schemes. This article has also described all existing false message detection schemes. The major contributions of this article are as follows:

- Local-based false information detection schemes have been categorized into plausibility, consistency and behaviour-based detection schemes.
- Cooperative-based data detection schemes are normally used for bogus information detection. The cooperative-based schemes are divided into behaviour, consistency and trust-based detection schemes. Trust-based detection techniques are further categorized into direct trust, indirect trust and hybrid trust-based detection schemes.
- This article has described different detection protocols and their issues. These issues must be eradicated to make VANETs' application more reliable and safe.
- This paper has bring an analysis of the insight information about these protocols.

The rest of the paper is organized as follows:

Section 3 is an introduction to the VANETs. Section 4 delivers a description on secure communication in the VANETs. Section 5 describes misbehaviour in the VANETs. Section 6 categorizes cooperative-based detection schemes for malicious information detection. Section 6 provides a detailed image of cooperative detection schemes. Section 7 presents malicious information detection techniques, and finally, conclusion and future work has been drawn in Section 8.

3 Vehicular ad hoc networks

VANETs are a subclass of MANETs that enable vehicles to communicate with each other and RSUs. In VANETs, vehicles act as a router node as well as a terminal node. The communication takes place in VANETs using V2V and V2I.

The architecture of VANETs consists of different software and hardware components. In VANETs, vehicle are equipped with an OBU. The RSU is deployed on roadside to monitor network nodes' behaviour information [15] and provide Internet facility access to pasenger on wheels. The CAs distribute security-related information through RSU like public key, private key and privacy-related information in VANETs (Fig. 1).

In VANETs, communication information consist of two types of messages, which are beacon and safety messages. Beacon messages are periodic information which shows presence of vehicle in network. It contains position of vehicle, identity of sender, speed and time. Safety messages are broadcasted in the case of safety event occurrence showing location of event [23]. VANET applications consist of vehicle cooperation for traffic management, notify drivers about danger on road and provide other comfort messages for passengers. VANET applications improve passenger safety, avoid collission, detection of movable and fixed obstacles and broadcast weather information [24]. Road safety applications consist of emergency electronic brake light (EEBL), slow/stop vehicle advisor (SVA), cooperative collision warning (CCW), road hazard notification (RHN) and post-crash notifications (PCN) [25, 26]. The driver assistance applications warn driver in specific situations like overtaking vehicles and traffic congestion. This application category contains toll booth collection [27], parking notification and congested road notification(CRN) [24, 28]. The third kind of application facilitates drivers and passengers while travelling. It provides mobile Internet services, discussions between vehicles [24] and entertainment [29]. MANETs and VANETs have some similar properties like self-management and low bandwidth. Frequently disconnected network, vehicle density and pattern of traffic flow are well-known challenges in VANETs. These issues directly effect security protocols and safety on wheels.

High mobility of vehicles is one of the important features, where the vehicle moves with different speed and direction. Signals fading is taken place in communication

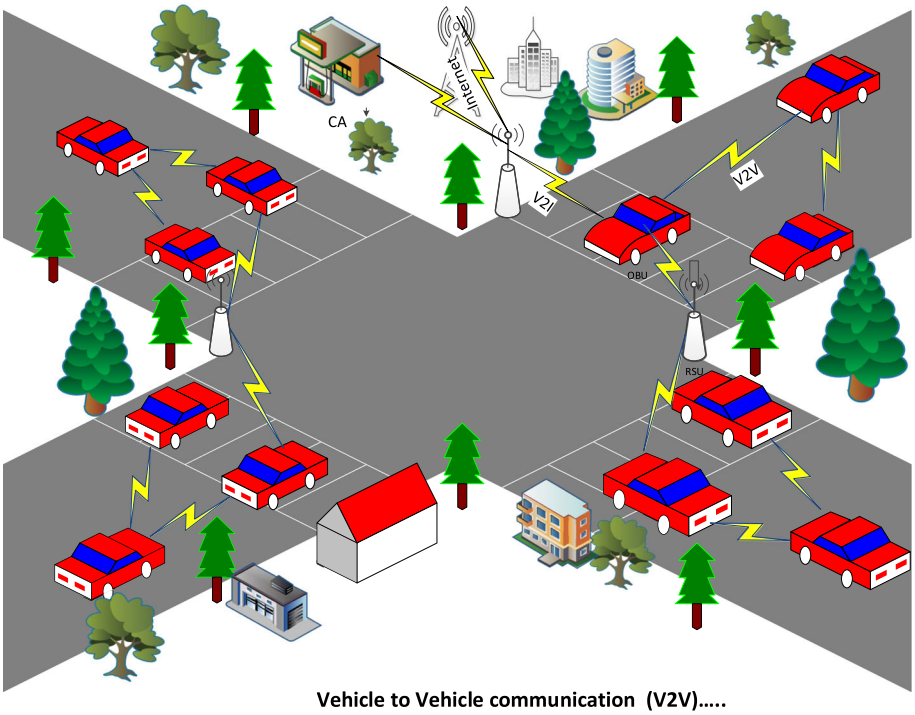

Fig. 1 VANET architecture

range because there are so many high-rise building, houses, vehicles and obstacles specially in cities. It may weaken signal strength as well. High traffic density creates jam in network which may cause frequent disconnections in the network. In high mobility VANETs, routing is a very difficult task because vehicle moves with various speeds [30–32]. High mobility makes a frequent topology change in result over a short time connection that is established between nodes in VANETs. Therefore, strong medium access control (MAC) protocols are a prerequisite for effective data dissemination strategies to enhance throughput and reduce communication overhead [33–35]. A dynamic topology network is vulnerable to different security attacks.

4 Secure communication in VANET

Wireless network communication makes VANETs faster, but evil doer may inject bogus information for accident and misleading purposes. Therefore, safety of information has uttermost priority. It is more important that information must not be modified or deleted by attacker [36]. Secure communication have many important metrics. In non-secure communication, outsider attackers try to enter with a fake identity in the network. The authentication is an important task to tackle because the attackers always try to authenticate with fake key/ID in the network. The sender-broadcasted messages must be authenticated to prevent outsider attackers from denial of service (DoS) attacks [37], where a large number of messages are authenticated through group signatures with low overhead and a timely manner [38]. In this category, there are several attacks but key/certificate replication, position faking and Sybil (malicious node create fake IDs and transmit false messages) are considered as critical attacks in VANETs [24]. The delay in authentication should be as minimum as possible [39, 40]. Confidentiality is also a security requirement in VANETs, and it ensures the fact that data will only be read by an authorized entity. In VANETs, data are exchanged among nodes and attacker can get information about locations and privacy related to driver. It is a difficult task in VANETs to detect an attack on confidentiality. Traffic analysis and information gathering are well-known attacks on confidentiality [24]. Securing data from unauthorized alteration during communication in VANETs is very important. Integrity techniques protect data from alteration, deletion and addition. These integrity detection schemes are for V2V and V2I communication in VANETs. In VANETs, an attack is happened when sensor or other OBU and RSU are manipulated by a malicious node [41]. Replay and fabrication/alteration are well-known attacks in VANETs as far as integrity is concerned [24]. Fabrication attack happens when a node creates bogus information in order to get certain privileges [42].

Availability of information is an important factor in VANETs. It enables a system to work all the time and provides information to vehicles. The goal behind DoS attack is to bring the network down and unavailable [43]. Jamming is to disrupt the communication channel [44, 45]. Spamming are messages that have no usefulness for users [46, 47], and DoS are well-known attacks on availability in VANETs. In [48], insider and outsider DoS attackers are mitigated through hash message authentication code (HMAC) and threshold value in VANETs. The drawback of this scheme is that a malicious node can attack with the help of fake messages. In network security, non-repudiation means to ensure that the communication entities are original and cannot be denied after communication happened. Non-repudiation is normally achieved by public key-based techniques [49]. Manipulated data related to safety and privacy is always verified for non-repudiation. In privacy, the attacker analyses vehicle and driver information throughout the journey. The single identity of vehicle create issues for privacy [7, 50]. The user can easily trace or compromise their personal details [51]. Therefore, it is more important to protect the vehicle owner's privacy. However, for privacy to provide anonymous authentication with low computational cost is a challenging task [52]. Therefore, in VANETs, a set of names are assigned to vehicles called pseudonyms. The actual identity is only known to CA that provides pseudonyms. The other nodes and RSUs only know pseudonyms. Pseudonyms are generated in such a way that actual identity cannot be predicted from pseudonyms. The pseudonyms are changed from time to time specially in mix zone, where nodes are not able to observe [53]. If there is only one vehicle in mix zone, then change in pseudonyms belongs to same node. In [54], a trade-off between security and privacy in VANETs is proposed because trust information is not useful due to frequent change in pseudonyms from time to time.

The management of large number of vehicles require an appropriate security infrastructure. The PKI is a combination of hardware, software and procedural components. A PKI provides many services, and the most important is a trusted third-party validation between the counterparts in VANETs. PKI ensures its role as a CA. It delivers sign and keeps digital certificates up to date that represent digital IDs of nodes. The new vehicular public key infrastructure (VPKI) uses digital certificate as a rapid authentication in vehicular environment [24]. There are other security requirements as well that is handled by VPKI (see Fig. 2).

The above security issues are handled by traditional VPKI. However, there are insider attackers that are equipped with valid credentials (public key/private key). These attackers propagate fake messages in VANETs. These attacks cannot be detected through VPKI. To detect fake messages, VANETs will need newly developed enhanced security techniques.

5 Malicious information detection in VANETs

VANETs uses different applications for road safety and traffic management. Safety and non-safety information is disseminated in vehicular network. Therefore, assessment of node behaviour is required for reliable communication. The misbehaviour in VANETs is referred as a kind of abnormal behaviour of node, and it is different from the average behaviour of nodes in network [1]. Why misbehaviour happens in VANETs? There are many reasons. According to [6], the causes of misbehavior are divided in two types, intentionally (attacker) or unintentionally (faulty). The intentional misbehaviour type is further divided into selfishness and malicious intent. The unintentional misbehaviour happens due to signal loss or fault in sensors [5]. The selfishness misbehaviour occurs because the node does not want to utilize its own resources for other nodes in the case of node centric misbehaviour. While in data centric misbehaviour, selfish node broadcasts bogus event information (like false congestion information) to change the normal behaviour of other nodes for own benefit. The malicious misbehaviour (attacker) takes place to disturb normal operation and produce confusion in the network. The misbehaviour is sometimes due to signal loss because nodes leave or enter in the network very frequently. The limited communication range of node is also the reason for misbehaviour. The faulty sensor information also plays a role towards misbehaviour in VANETs [32].

The main objective is to detect those misbehaving nodes that broadcast fake data in VANETs. Revoking misbehaving nodes is a process which may prevent fake packets from further participation in network. Detection schemes are divided in two types, node centric detection and data centric detection. The focus of this article is on fake information detection techniques.

5.1 Node centric detection

In the node centric detection scheme, a security model monitors security credentials of a node, like digital signature with the help of PKI [55]. The node centric mechanism is precisely concern with a participating agent (node) in the network. They verify node behaviour by analysing packet and message pattern. Node centric detection is divided in two categories, behaviour-based detection and trust-based detection.

5.1.1 Behaviour-based detection

In the behavioural scheme, looking for a node with an observable behaviour and extracting a metric that recognizes how healthy nodes behave, for example, behaviour schemes, may monitor neighbour node transmitting

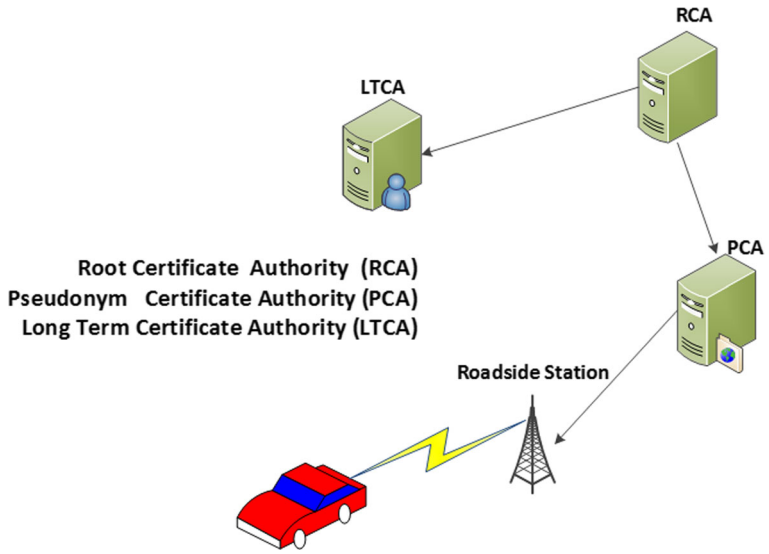

Fig. 2 Simple VPKI structure

packets whether rates are exceeding from normal rates or not [55]. In this mechanism, consider how many messages in correct pattern (message format) has been delivered? The main focus of these mechanisms are node-related information [56].

The abnormal behaviour of a node is to monitor packet drop or duplication in VANETs. A verifier node is responsible for monitoring misbehaviour. The verifier node is elected on the basis of their trust value. A verifier may discredit a node that drop or duplicate packets. After crossing the threshold value for misbehaviour, a verifier node reports to cluster head (CH) and update whitelist(good nodes) and blacklist(bad nodes). The CH also reports to CA and revoke them from whitelist. The CA updates the whitelist and blacklist and broadcast it in network [57].

5.1.2 Trust-based detection

Trust-based detection depends on past and present reputation of node. A node whose reputation is good in the past is more likely to behave well in the future [55]. The main advantage of trust-based is that it has one step forward to revocation.

Trust-based system consists reputation system that maintains a past communication history of nodes. Trust management also have a voting scheme, where honest vehicles vote for communication in VANETs [56].

5.2 Data centric detection

Data centric detection focuses on application data from various neighbours. Data centric misbehaviour detection schemes analyse transmitted data for possible misbehaviour. The data is compared with other nodes in network to verify truism of safety messages. In VANETs, vehicles propagate different kinds of safety messages for road safety and collision avoidance. The false safety messages are considered misbehaviour in VANETs [1]. In data centric detection scheme, the node searches for possible evidence to verify application data locally or with the help of neighbour vehicles. The detection of false safety alerts consist of local-based detection and cooperative-based detection mechanisms.

5.2.1 Local-based detection

The local-based detection techniques check each piece of information independently. In local-based detection, each received data from same sender will be consistent with a previous data. These techniques do not rely on other node response for data detection. These techniques are further divided into the following subcategories. These are plausibility checking, consistency checking and behaviour checking (Fig. 3).

Plausibility checking. In plausibility checking data, from each node is verified through some predefined rules, for example, one location is not occupied by two nodes at the same time. The allowed speed of vehicles should not exceed that has been established by road authorities. The movement of vehicle is verified by two beacon messages which form distance travelled by the node. It is compared with speed in beacon messages. The plausibility checking model can be used for an expected misbehaviour and filtering false safety messages. Plausibility model can produce a valid result in case majority vehicles are not honest nodes because plausibility checking does not rely on other neighbour information [56].

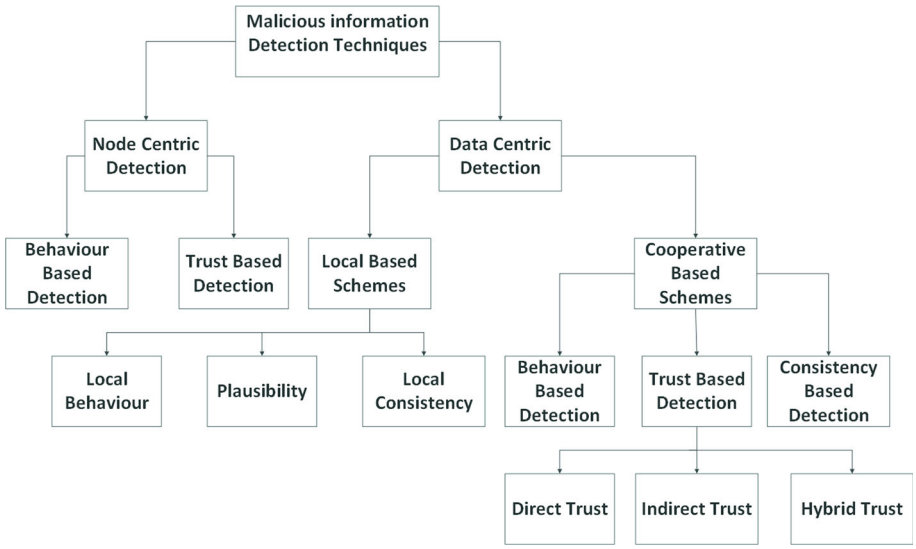

Fig. 3 Malicious information detection schemes in VANETs

- **Database checking model:** To protect VANETs from false information, plausibility validation in network is proposed and consist of database rules and checking model. These rules depend on message type. A valid message will be succeeded in all verifications. In order to detect fake vehicle messages, the rule is vehicle location. It will be in range and plausible and time stamp will be checked, and also, velocity should be plausible [58].
- **Multiple parameters:** For position verification, plausibility is checked for multiple parameters. The parameters are called maximum density threshold (MDT), acceptance range threshold (ART) and mobility grade threshold (MGT). Messages outside the range will be discarded. Multiple messages sent from single location indicates false position. For a Sybil attack detection, map-based verification and claim position are used. Map-based assign plausibility value to beacon messages and compare it with positions in road map [59].
- **Classifier framework:** A security framework which categorizes misbehaviour in VANETs. A different attack creates various misbehaviours. J-48, Naive Bayes, IBK, Rrndom forest and Ada Boost1 are used as classifiers. These classifiers efficiently classify different misbehaviour attacks. Features related to verification of position, acceptance range, speed and received signal strength (RSS) are used to classify position and identity spoofing attack. The classification framework is used for different misbehaviour detections. Multiple classifier creates overhead and increases computation cost in detection scheme for single node in VANETs [60].
- **RSU-based detection:** A centralized detection approach is proposed for a malicious node that is propagating false position information in VANETs. This method develops a series of verifications, which includes acceptance range verification, maximum allowable speed check, maximum density of nodes, speed consistency verification and time interval substantiation. These verifications are the responsibility of RSUs to find the legitimacy of node position. This detection scheme minimizes overhead on other mobile vehicles in the network. For safety alerts, position verification is important, and vehicle will wait for RSU response which creates more latency [15].
- **ELIDV**: In efficient and light-weight intrusion detection scheme for vehicular network (ELIDV) design to detect false information. The aim of the detection scheme is to protect network from three kinds of attacks like false safety messages, integrity and denial of service (DoS) attacks. The ELIDV detects false information detection based on a set of rules. The drawback of this scheme is when the number of node increases then the detection performance decreases [61].

Local-based consistency checking. In consistency checking, each data must be consistent to previous data, for example, node at location A in first report and second time report represents location C. The speed to reach from location A to C must be consistent in the second report [55]. In these schemes, false information is detected locally rather than other vehicles in VANETs. The detection is based on consistency of messages

from same sender while inconsistency is represented as misbehaviour.

- **Data centric (DC):** This algorithm detects false messages and node's misbehaviour by observing their action after sending messages. In the data centric misbehaviour detection scheme (MDS), each node locally decide whether information is correct or not. Consistency-based scheme fails when nodes are at equal distance from each other. This algorithm also fails when a node turns around. It detects false location information. When the vehicle is moving on a flyover, then the actual distance is different from the calculated distance. When the vehicles are moving in a group and one turns to the right and the others turn to the left, then the vehicles behind them consider it as a correct alert. When the nodes are moving in an opposite direction and send false alert, it is not a selfish reason but a malicious intent. The second drawback is if a node cannot receive a beacon after an alert message, so it is assumed as a misbehaviour, but sometimes, honest cannot send beacons due to bad signal. Position verification needs a more efficient mechanism rather than sender and receiver timings [7].
- **Heartbeat-based detection (HBBD):** A short-term misbehaviour detection scheme for node that propagates false position and speed information through heartbeat/beacon messages. The observing node analyse incoming heartbeat/beacons messages for honest and malicious information detection. From present and past information, an expected and observed position is calculated. If information does not match, the suspicious index of vehicle is increased. When suspicious index crosses threshold value, then the vehicle is declared as a malicious vehicle. The main feature of this misbehaviour detection technique is low overhead and there is no need of additional sensors but use of beacon messages. This scheme looks for inconsistency in consecutive beacons. This is effective, has low overhead, and gets misbehaviour detection from few beacon messages, but beacon messages might loss in a process which effects credibility [62].

Behaviour-based detection. In malicious information detection schemes, driver behaviour has a key role. These schemes monitor behaviour of event reporter. These schemes rely on behaviour information from single node. A scheme required little time for detection because it does not need behaviour information of other vehicles in reporter vicinity. It consist of techniques that are elaborated below (Fig. 3).

- **Trajectory-based detection (TBD):** This is a misbehaviour detection scheme for false post-crash notification. This detection technique depends upon the behaviour of driver after sending alert. The position of vehicle is sensed each time slot form the time alert received till passed to crash position. The expected trajectory of event crash modulated mobility is calculated. The actual car trajectory is also calculated. If the differences between two trajectories are above the certain threshold, then it will be considered as false alert, the reason a car does not follow the crash trajectory; otherwise, alert will be considered as true. The main drawbacks of MDS is that it assumes vehicle position. The other issue is low threshold which creates more false positive rate [63].
- **Root cause-based detection (RCBD):** This is another MDS for PCN. After receiving a PCN message observer monitor the behaviour of driver for comparing with expected behaviour of driver, it finds different root causes based on observation between two nodes. The node will follow the free mobility model in case of no alert. The node follows the crash-modulated mobility model in case of alert messages. The scheme assumes node will always send the right location information. This assumption is invalid because a node can send false location information too and may produce false results [64].

6 Classification of cooperative-based detection

The cooperative data detection schemes observe node verification for false information with the help of neighbour nodes. In cooperative data detection techniques, when the node receives safety-related messages, then it is checked for data relation with multiple vehicles in the network. The neighbour node's conformation about the safety event will ensure the receiver to accept message and notify the driver. The main benefit of cooperative detection is to identify efficiently misbehaviour node with more confidence. The cooperative-based detection schemes have sufficient knowledge for bogus message detection while detecting fake messages. It has produced low false positive and false negative rates of a node. The cooperative-based data detection schemes consist of behaviour-based detection, trusted-based detection and consistency-based detection, as shown in (Fig. 3).

6.1 Behaviour-based detection

In behaviour-based detection for false event information, a receiver is compared with average driver behaviour, with event reporter behaviour at location of the event. The similarity of average behaviour of vehicles with reporter behaviour confirms an event. In case of behaviour difference below the threshold will provide a solid proof for false information. These kinds of detection

technique performance rely on maximum number of honest vehicles in the vicinity of malicious node. The behaviour base detection scheme is normally used for verification of false congestion alerts and PCN application. It has some detection techniques that are as follows:

- *IDS*/RC^2RL**:** An MDS in where misbehaviours like false position information or intrusion detection scheme (do not follow known pattern) are tested. In this case, more density of vehicles the CRL are compressed through the use of a bloom filter RC^2RL (revocation using compressed certificate revocation lists). An MDS is to detect false information by comparing the behaviour of each node with the average behaviour of other nodes in its vicinity to build data models on the fly. Moreover, if a true event appears on the low density, MDS will be considered wrong. It is bad for safety messages [65].
- **Acknowledgement-based detection (ABD):** This scheme consists of false information detection and mechanism for non-cooperative node detection to isolate malicious node from the network. A data packet is used for false information detection. Vehicle "A" sends information about dense traffic while another node "B" is moving with an appropriate speed. The node "B" report that "A" is sending false information. Another case in same geographic area that a node sends information about traffic jam while another node reports high speed is also considered as fraud. Non-cooperative node is identified through time stamp acknowledgement packet. In false congestion, information of a node is also detected through responses of other nodes in network. A non-cooperative node is detected through acknowledgements. The false information detection technique performance is degraded with a decrease of nodes on the road. The second drawback is that acknowledgement process creates a higher overhead and produce more delay for node and that may be time-critical messages. For selfish and non-cooperative nodes, two lists are used, that is, the individual reputation list (IRL) and the general reputation list (GRL). The main limitation of IRL is that a malicious node can insert wrong information about neighbours without communication with them [9].

6.2 Consistency-based detection

Consistency-based detection uses consistency data from multiple vehicles to determine false information. A vehicle which uses previous average speed of neighbour vehicles must be consistent with the new speed from beacon messages.

A maximum difference of inconsistency of average speed will provide evidence of false information [56]. Consistency mechanisms are used when there is a conflict of information from more than one vehicle. For example, in the VANET environment, one group of nodes disseminate false road congestion information while the other group propagate no congestion information. Cooperative consistency need maximum number of honest nodes; otherwise, this scheme would be non-effective for malicious information detection.

- **Detection based on database (DBD) :** The first model proposed for detecting and correcting malicious data in VANETs. It was a general framework that is used to validate safety information based on local sensor data to detect Sybil node attackers. Each node checks validity of data through a model. When inconsistencies are found, then data is considered as malicious. Adversarial model is used based on parsimony argument for best explanations to correct malicious data. There is no validation or performance testing for this approach. To maintain a global database in VANETs is almost impossible. This scheme does not provide location privacy. This scheme will fail when the number of malicious nodes are more than honest nodes in VANETs [66].
- **Detection based six source of information (DBSSI):** A security model enable VANETs to distinguish false alerts from legitimate alerts. The detection model is based on six sources of information. The drive is sent an alert after agreement of six sources. The filtering model is dependent on two components. One is threshold curve (TC), and the other is certainty of event curve (CoE). The TC depends on distance between event and driver. The CoE means the confidence of received message from neighbour node. If the CoE intersects threshold curves, then the driver will be notified. The performance of scheme depends on two parameters which are TC and CoE. The threshold is important to the driver while certainty of event is related to event confidence. However, this scheme creates more computation and delay due to six sources for false PCN or congestion event detection. In some scenarios, a threshold may not be crossed due to VANETs' characteristics only to analyse or to endorse the EEBL applications, and no further applications has been tested or evaluated [67].
- **Secondary information based detection (SIBD):** A secondary information is generated in the result of primary information. The secondary information is used for detection of primary information. This scheme depends on how many vehicles generate secondary information. This means correlated

information in response to primary information is known as degree of belief. In the absence of primary alert, it is also a probability that malicious node send secondary information. However, in case of true primary alerts, neighbour node sends large number of secondary alerts that provide a belief on primary alert. When the degree of belief is 1, it indicates a true event. The degree of belief which is 0 shows a false event; however, the performance of this scheme degraded due to high speed. The minimum density of nodes also effect truism of the scheme [68].

- RD^4 **:** The proposed scheme is RD^4 which is used for cooperative deceptive data detection. RD^4 filters false accident in VANETs. Detection of true accident is handled by accident sources. The car which is actually involved in accident is equipped with tamper-proof component to resist against propagation of fake identities. When accident report is received by vehicle, the decision is based on the signal strength of his own observation and signal strength of the same event of others. In design when accident happens, the road is black and vehicles slow down. Integrating both signal strength of events for accumulative signal strength, if the accumulated signal strength exceeds the pre-set bound to confirm the event, a velocity deceleration used as a signal strength and accumulative signal strength is observed by the vehicle. An increase in speed indicates low signal strength which does not produce good accuracy for false event detection schemes in VANETs [69].
- **VANETs association rule mining (VARM) :** It is an introductory scheme for detection of malicious data disseminated by malicious or faulty node in VANETs. The scheme builds a mining association role based on routine messages in VANETs. These messages provide a relation among vehicles. In high density, a mining association between vehicles on a single vehicle creates more computation overhead. It needs more storage capacity for a single node [70].
- **Cheater Detection Scheme (CDS):** The Cheater Detection Scheme (CDS) for a node is a mechanism that broadcasts fake congestion events. This approach is based on local velocity and distance with the help of a radar to verify the congestion event. It uses a kinematic wave to detect congestion period and distance. It is a very effective technique against fake IDs and sent false congestion event because kinematic wave packets contain signatures and certificates. In kinematics, a wave packet is used for detection of non-existing congestion event in VANETs. This is an effective technique for single misbehaviour vehicle (cheater), but when the cheater increases, then the detection process will take more time because the distance between the leading cheater and the last cheater increases as well [71].
- **Fox hole region (FHR):** A scheme to detect false PCN in VANETs. MDS is based on FHR event which happens at a certain location. An FHR is a four-coordinate region with dimensions depending on speed of the node. The high speed means larger FHR, and the low speed have smaller FHR. The FHR consists of safe and unsafe zones. Two consecutive beacon messages are used for average speed of vehicles; after that, a FHR is found for each vehicle. We find that in threshold D, if the parameter of belief is between D^+ and D^-, there might be a misbehaviour. The information may be correct if it is greater than D^+ and smaller than D^-. The FHR help to find a safety value for the node on his current location and speed. This detection approach is valid for static event like PCN. The weight-age information is obtained from consecutive beacons. In some cases, it is not useful when an event is near because the vehicle may cross event location [23].
- **Misbehaviour Discovering Method (MisDis):** A misbehaviour detection method is known as Misbehaviour Discovering method (MisDis), having accountability of vehicle behaviour by record of evidence to conform it from inside and outside vehicles. MisDis has also identified misbehaviour through inside device (state of automata monitoring) and supervision. A MisDis also keeps a record (security log) for behaviour characteristic of target vehicles. If anything is observed, then a system will inform the RSUs or other security in charge for further assistance. MisDis assumes strong authentication and identification but cannot provide privacy and practical implementation for performance evaluation [72].
- **Cooperative Detection and Correction ($C-DAC$):** In Cooperative Detection and Correction ($C-DAC$), each vehicle calculates his own value of flow (speed, density, flow, location information) and send information to other vehicles. The rest of the vehicles also calculate the value of Speed, density, flow and location information. It provides us a good model for traffic. Each vehicle transmits its flow to another vehicle. If received flow does not match with a VANET model flow, then data will not be accepted. This scheme has effectiveness against node that shares wrong location information. When a node will send false information from multiple identities, then honest nodes that are behind of malicious node ignore this information because of their own speed. When multiple attackers send false information, then the $C-DAC$ scheme cannot detect information as wrong information. The scheme does not provide better

result in low density [3]. The scheme performance is enhanced with IDS (intrusion detection system). The IDS uses statistical schemes to identify malicious nodes which broadcast false information [73].

- **Subjective logic-based detection (SLBD):** A position verification method by enhancing two position verification methods and fusing its data in framework that is known as subjective logic. The parameters have acceptance range threshold (ART) and pro-active neighbour exchange (PNE). Both mechanisms are integrated in the framework. Subjective logic expresses truth value as opinion which consists of belief, disbelief, uncertainty and base rate. Using two methods for position verification ART and exchanging of table is minimum. Therefore, more parameter can be used for better results and low false positive rate in VANETs [22].

6.3 Trust-based detection

Trust and reputation are two important tools of security that facilitate nodes in decision making of network [74]. Generally, trust is the expectation and level of confidence of one vehicle about the other vehicle's action in VANETs [75, 76]. In VANETs, a high dynamic environment and an adapted trust establishment are needed. VANETs are ephemeral kind of network where the connection life is very short and vehicles meet for few seconds. Decision about trust of other nodes must be conducted individually rather than other nodes. Therefore, trust information is collected from other nodes for very limited time [77]. Trusted-based detection techniques assign value to nodes based on their past historical data communication [78]. Trust-based detection system is categorised in three trust systems as shown in Fig. 3.

6.3.1 Direct trust

The established trust is based on mutual sharing of information between nodes in VANETs. This kind of trust does not rely on other node's trust information. The direct trust is feasible in VANET environment, but sometimes, it cannot provide sufficient trust information for false information detection.

- **Particle filter-based detection (PFBD):** In this scheme, particle filtering is performed to check the plausibility of data and assess trustworthiness of neighbour nodes. This scheme combines information from different data sources in one particle filter per neighbour, for example, position information is verified through cooperative awareness message (CAM) by sender nodes and neighbour nodes as well as with local sensors (digital road map, radar, Lidar, directional antennas). This scheme is based on the transition shift between two incoming messages. The main benefit of this scheme is that it locally assess trust of neighbour for location verification rather than other vehicles. The accuracy of scheme depends on local sensor data and local sensor data effected from high speed. The drawback of this scheme is more computation overhead and delay for a single vehicle [79].
- **Behaviour and position-based trust system (BPBTS) :** A method that detects malicious data in traffic signal at intersections. Node creates fake multiple identities (Sybil attack) and transmits information from these fake identities to manipulate traffic signal. The detection of malicious data with the help of combination models expected behaviour of driver and position verification technique. In false information for traffic signal, control is detected by control node. The control node assigns trust level to each node for detection of malicious data. The trust change (update) after each node's information is received. Sending data with a low or zero trust is considered as a malicious data. In detection scheme, assumption is not valid for node trust to stop on green signal because it will not stop on green signal in a selfishness situation [80].
- **Similarity-based trust management system (SBTMS):** A similarity-based trust management system (SBTMS) checks for bogus safety event detection in node using similarity index. It assigns trust to one-hop neighbour in the network. This scheme also enhances decision-making power using trust and utilizing echo protocol to check reaction of reporting vehicle. This scheme is feasible when there is more meeting time between vehicles for communication to build a trust system. The second limitation is when a safety event elevator (SEE) sends echo safety event alert to a safety event reporter (SER). If SER does not reply due to signal loss or out of range communication from SEE, it is also considered as malicious data [81].

6.3.2 Indirect trust

In indirect trust system, the node shares trust information of other nodes based on their past communication relationship. This kind of trust is transitive and effective in terms of sufficient information.

- **Proof of relevance (PoR) :** An event verification responsibility is to put on the reporter. When a vehicle sense safety event, it must be endorsed from vehicle in the detecting area and disseminate it in the network. The drawback is that malicious node could endorse message with fake digital signature in the detecting area. Low density of vehicles in reporter area is also considered as a failure of this scheme [82].

6.3.3 Hybrid trust

Hybrid trust is a combination of direct and indirect trust. The hybrid trust system is good for detection rather than individually using direct and indirect trust, but it consumes more time in detection. Therefore, VANETs need a short time trust management system.

- **Vehicle ad hoc network reputation system (VARS):** A vehicle ad hoc network reputation system (VARS) uses direct and indirect trust as well as appended opinions from sources to enable confident decisions on event packets. The main problem of this scheme is that it involves accumulation of reputation evaluation which takes more time [83].
- **Event reputation system (ERS):** The event reputation system (ERS) prevents inaccurate traffic messages in VANETs. A dynamic reputation system is used to determine the incoming traffic trustworthiness to the driver. In this scheme, the vehicle gets enough reputation from inside sensors and received messages. When enough reputation is received, then the traffic warning will be broadcasting to other vehicles in the network. The scheme is dependent on two parameters: event reputation value and event confidence list. Event reputation system consists of three interfaces and four functionalities. One is event table storage for received messages or event from on-board unit sensors. The event table consists of event identity, type of event, time stamp of event, event location, event transmission range, event reputation value and event confidence value list. The event table stores each event separately and set event reputation value. The ERS uses aggregative event observation mechanism and reputation adoption mechanism. The event confidence threshold and event reputation threshold assess event intensity and reliability at the same time. The limitation of ERS is that event reputation value is low in high speed because of the sensor capability (minimum detection). The event confidence is small in low density. The other factors like event duration and transmission range also have an effect on ERS [84].
- **Event reputation model (ERM):** An event-based reputation model is where an event observer node checks the expected behaviour of event reporters. If the behaviour matches, then the reputation of event as well as that of node's increases. Otherwise decreases in false information situation. A faulty or malicious node can inject wrong reputation value [85].
- **Cascading and oversimple (CAO):** A misbehaving node cannot send malicious information at all times due to selfishness reasons. Therefore, depending on circumstance in the network, having said that a node cannot point out all the time a good or bad. Another issue of trust management is based on the voting system. The voting threshold value is not reached due to a constantly changing topology. Another problem in trust management is cascading (where nodes influence other nodes in decision-making). The cascading is solved through a mechanism where more weight-age is given to a node that is closer to event location from nodes which are away from the event location but till there are loopholes. If the nodes are at same distance from event propagating different opinions about same event, then the proposed scheme does not work properly [86].
- **RMS:** The misbehaviour detection scheme is based on reputation management system (RMS). The RMS has three components: misbehaviour detection, event rebroadcast, and global eviction and filtration of false information. Each node maintains event information and a corresponding action for detecting misbehaving nodes. The detection scheme uses a risk value of bad node to calculate risk level. The event reporter's sense event creates alert and sends it to their neighbours. If an event observer within one hop of reporter can observe the behaviour of reporter, vehicles beyond one hop of reporter participate and can forward the alert but cannot detect behaviour of reporter [87].

7 Analysis

The purpose of this article is to provide an overview of current cooperative-based malicious information detection schemes in VANETs. The detection of malicious event information is very important for road safety and human lives. This article has categorized data centric misbehaviour detection schemes based on their tendency for malicious information.

Local-based detection schemes rely on available information from a single source. Although it is efficient in term time for detection due to not having any dependance on other nodes, there is another well-known parameter for fake data detection that means delay and is experienced in the network due to VANET characteristics. The delay has various parameters in Table 1. A scheme with low delay is considered to be fast and vice versa [88]. All mechanisms in Table 1 efficiently detect location of nodes. However, lack of sufficient information from single node cannot provide accurate result for malicious information detection [7, 62]. The schemes in [7, 62] are also vulnerable to weak signal strength in detection area.

However, local base detection can produce good result in low density like [7, 62]. In [63, 64], observing behaviour of node after transmission of safety message. The main drawback of these schemes is they assume valid position information at detection time. A malicious node can provide consistent and plausible data to reduce the

Table 1 Local-based detection schemes

MDS	Type	Drawback	Privacy	Delay	Overhead	(FP) Rate	Applications
Database rules [58]	Plausibility	This model allows passing fake sign messages from database rules.	No	High	High	Min	CRN
Multiple parameters [59]	Plausibility	False position in past checking might create false positive	No	High	Low	Max	Position data
Classifier framework [60]	Plausibility	Uses multiple classifier for detection	No	High	High	Min	Speed & Position
RSU-based detection [15]	Plausibility	Vehicles will be waiting for position validation from RSUs	No	High	Low	Min	Position data
ELIDV [61]	Plausibility	Performance decreases when malicious nodes increase in VANETs	No	High	Low	Min	EEBL, PCN, CRN
Data centric (DC) [7]	Consistency	Sometimes, this scheme cannot provide useful information for detection	Yes	Low	Low	No	EEBL, PCN, CRN
HBBD [62]	Consistency	Beacon messages lose due to weak signal.	Yes	Low	Low	Min	Position & speed
TBD [63]	Behaviour	Assumed true location information for trajectory.	No	Low	Low	Max	PCN
RCBD [64]	Behaviour	Assumed position information is correct	No	High	High	Min	PCN

effectiveness of local-based schemes as in Table 1. The accuracy of the schemes is measured in terms of overhead and false positive rate in worst scenarios. In worst scenarios, there are more malicious vehicles that propagate false messages. The exchange of extra data with vehicles is known as communication overhead. To incorrectly classify honest nodes as malicious is false positive. The schemes having low overhead and minimum false positive rates are normally considered better false data detection schemes [73] (see Tables 1 and 2)

The cooperative-based detection schemes have more effectiveness than local-based detection. The neighbour vehicles provide evidence for malicious behaviour. These schemes provide low false positive rate than local-based detection schemes. They accurately detect Sybil attacks. Cooperative detection scheme creates more overhead and computation rather than local detection schemes. The malicious information detection requires minimum latency as shown in Table 2. The [66, 70] maintain database for malicious information detection on single node. A high density network cannot maintain database on one node. The main drawback of these schemes are when malicious nodes increase than honest nodes which creates a false result [3]. In VANETs, low density of vehicles also decreases the performance of cooperative detection schemes [9, 65, 68] as shown in Table 2.

VANETs is an ephemeral kind of network where connection between nodes is very short time [86]. Therefore, VANETs are vulnerable to different security attacks [89]. To constitute trust system is a difficult task [90]. A misbehaviour node may not be malicious all the time but due to selfishness.

The reasons depend on multiple circumstances in the network. A simple trust model is needed to be constructed for fast data evaluation in VANETs [91]. In [92], trust management system for malicious information detection needs high trust nodes and RSUs. The RSUs already has an overhead due to other responsibilities. Another issue is trust management on voting systems. The threshold value does not reach due to the constantly changing topology. In trust management system, faulty or malicious nodes can share false trust information. The single identity of vehicle create problems for privacy. The user can easily trace or compromise their personal details. That is a resaon that a set of names are assigned to a vehicle called pseudonyms. The actual identity is only known to CA who provides pseudonyms [7]. Therefore, pseudonyms are changing after certain time period depending on the mechanism. The trust-related data is removed due to privacy issues. For these reasons, VANETs may be needed as a trade-off between privacy and trust management system [93]. In indirect trust management system, a malicious

Table 2 Cooperative-based detection schemes

MDS	Type	Drawback	Privacy	Position	Delay	Overhead	(FP) Rate	Applications
IDS/RC^{2}RL [65]	Behaviour	Performance degradation in case of sparse network	No	Yes	High	Low	Min	Position data
(RCBD) [9]	Behaviour	Loss of acknowledgement due to bad signal	No	Yes	High	High	Min	CRN
(DBD) [66]	Consistency	No validation for performance evaluation	Yes	Yes	High	High	Not mentioned	Not mentioned
(DBSSI) [67]	Consistency	Minimum threshold might create more false positive rate	No	Yes	High	Low	Min	
(SIBD) [68]	Consistency	Malicious nodes can generate secondary information in low density network	No	No	Low	Low	Min	PCN
RD^4 [69]	Consistency	Degradation in accuracy due to high mobility	No	No	Low	Low	Min	PCN
(VARM) [70]	Consistency	Computation overhead for single node	No	Yes	Low	High	Not mentioned	Not mentioned
(DWD) [71]	Consistency	Detection will take more time in case of increase in malicious nodes	Yes	Yes	Low	Low	Max	CRN
(FHR) [23]	Consistency	Mechanism uses for static events	Yes	Yes	High	Low	Not mentioned	PCN
(C-DAC) [3]	Consistency	Multiple malicious nodes can degrade performance	No	Yes	High	High	Not mention	PCN,CRN
(Host IDS) [73]	Consistency	Honest neighbour nodes must be prerequisite for detection	No	Yes	High	Low	Min	PCN,CRN
(SLBD) [22]	Consistency	More parameters can be used for accurate result	No	Yes	Low	High	Min	Position data

node can provide bad reputation value for honest node. The majority of vehicle must be honest for false information detection. The trust value is assigned based on their past history of communication, but unpredictable behaviour of vehicle sometimes falsifies their past history.

The following prerequisites are required while designing an efficient trust model for MDS in VANETs [94] as shown in Table 3.

- **Decentralization**: VANETs are dynamic and distributed networks. Therefore, a decentralized trust management system is required for reliable data communication. The trust models use one to one or one to many interactions while trust-building in a decentralize manners [28]. Some strong authentications are prerequisite for nodes before establishing a decentralized trust management system in VANETs.
- **Data scarcity**: VANETs have dynamic and distributed type of network where interaction between same nodes in future is almost impossible. Due to short network life, the data received at first time is important for trust-building.
- **Network scalability**: Scalability is considered as an important factor for trust management. The density of nodes are more, and few of them interact and send information in the network. The observer need to quickly decide about the incoming information. The trust information may be updated a little bit according to the network size. For a good trust management, trade-off between scalability and trust mechanisms are required. In efficient trust management, priorities are given to nodes that are frequently interacting.
- **Metric**: In trust management, different types of metrics are used for dynamic trust establishment. The metrics for trust management system include post-crash notification (PCN), congestion and weather condition beacons [95, 96]. In [97], trust management system is based on behaviour analysis of neighbour nodes to assign trustworthiness value which is additionally disseminated in network. The priorities are given to event reporters that are relatively close to event location [86] or close in terms of time.
- **Confidence**: In order to remove uncertainty for event, trust management requires reliability and confidence in the VANETs. A trust management

Table 3 Trusted based detection schemes

MDS	Decentralization	Data scarcity	Scalability	Metrics	Confidence	Security	Privacy	Robust	(FP) Rate	Applications
(PFBD) [79]	+	+	+	-	+	+	+	-	Low	Position data
(BPBTS) [80]	+	+	-	+	+	+	-	+	Low	Traffic signal
(SBTMS) [81]	+	+	+	+	-	-	-	-	Not mentioned	Safety event
(VARS) [83]	+	+	+	+	+	-	-	-	Not mentioned	Not mentioned
(PoR) [82]	+	-	+	+	+	+	-	-	Not mentioned	Not mentioned
(ERS) [84]	+	+	+	-	+	+	-	-	Not mentioned	PCN,CRN
(ERM) [85]	+	+	+	+	+	-	-	-	Low	Not mentioned
(CAO) [86]	+	+	-	+	+	+	+	-	Low	PCN
(MBRMS) [87]	+	+	+	-	+	-	+	-	High	PCN, CRN

assigns high trust value to nodes that report same event [98–100].

- **Security**: Trust management system requires strong security credential to authenticate sender that reports safety information in VANETs [101]. Normally, PKI is used to verify reporter authenticity in VANETs [102].
- **Privacy**: In VANETs, decentralized trust management is dependent on strong authentication for vehicles while using single key create security concern to vehicle owners. Therefore, using multiple keys reduce privacy issues in network [103]. To protect location privacy in VANETs, many pseudonym changing techniques have been proposed to achieve pseudonym changing [104]. In Table 3, most of trust management schemes have not provided good privacy.
- **Robustness**: Trust management system itself faces challenges of Sybil attack, new comer attack, betrayal attack (trusted node suddenly started misbehaviour) and bad mouthing attack (some nodes provide low reputation intentionally). A robustness trust mechanism is needed to tackle these kinds of attackers as well.

  VANETs require a quickly responsive detection mechanism for malicious information detection. New trust management system is necessary that uses current parameters in different scenarios for VANETs. The focus is needed on alert messages rather than nodes. In VANETs, trust management system should have minimum information (data scarcity), strong authentication and privacy and must be decentralized and scalable.

8 Conclusions

In VANETs, vehicle communication takes place with each other and RSUs. VANETs have different kinds of applications for health, safety and traffic efficiency. A malicious node can broadcast bogus messages, which can change the behaviour of other nodes. Therefore, detection of malicious information is an important factor to be investigated. This article has categorised existing detection mechanisms in cooperative data detection, local-based detection and trust-based detection techniques. Cooperative-based detection schemes are efficient in the case of dense network and greater number of honest nodes. Trust-based detection schemes showed good performance when the frequency of interaction among nodes was high. Trust-based schemes depend on past interaction information among the nodes for better malicious information detection. However, trust management system and local-based detection for malicious information detection has its own challenges due to VANET characteristics. The existing detection mechanisms cannot provide good and up to the mark performance due to various challenges. Therefore, VANETs require such detection techniques that should provide data scarcity and have minimum delay time.

Local node information-based detection techniques depend on available information from a single node. They are efficient in terms of time because they do not rely on other nodes while detecting bogus messages. The lack of sufficient information from single node does not provide accurate result for malicious information detection. These schemes need more information from single node to enhance their performance.

The cooperative techniques create more delay and overhead while detecting malicious data as compared to local-based detection in VANETs. If a number of malicious nodes increases than honest in VANETs, then it creates false result for malicious data detection. Low density of vehicles in VANETs reduce effectiveness of these techniques as well.

Abbreviations

CAs: Certificate authorities; OBUs: On-board units; RSUs: Roadside units; RHN: Road hazard notification; VANET: Vehicular ad hoc network

Acknowledgements

We thank Mr. Waqar Khalid for his valuable inputs in the revised form of this paper.

Funding
This research work is funded by authors themselves.

Authors' contributions
All authors have contributed jointly to all parts throughout the preparation of this manuscript, and all authors has read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Author details
[1]Department of Computer Science, Institute of Management Sciences, Peshawar, Pakistan. [2]Department of Computer Science, University of Peshawar, Peshawar, Pakistan. [3]Department of Computer & Information Sciences, Northumbria University, NE1 8ST, Newcastle upon Tyne, UK. [4]Institute for Communication Systems, University of Surrey, GU2 7XH Surrey, UK.

Received: 12 August 2017 Accepted: 22 February 2018
Published online: 15 March 2018

References

1. U Khan, S Agrawal, S Silakari, in *Information Systems Design and Intelligent Applications*. A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks. (Springer, 2015), pp. 11–19
2. S Al-Sultan, MM Al-Doori, AH Al-Bayatti, H Zedan, A comprehensive survey on vehicular ad hoc network. J. Netw. Comput. Appl. **37**, 380–392 (2014)
3. K Zaidi, M Milojevic, V Rakocevic, M Rajarajan, in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. Data-centric rogue node detection in vanets. (IEEE, 2014), pp. 398–405
4. F Qu, F-Y Wang, L Yang, Intelligent transportation spaces: vehicles, traffic, communications, and beyond. **48**(11) (2010)
5. N Ilyas, M Akbar, R Ullah, M Khalid, A Arif, A Hafeez, U Qasim, ZA Khan, N Javaid, Sedg: scalable and efficient data gathering routing protocol for underwater WSNS. Procedia Comput. Sci. **52**, 584–591 (2015)
6. F Ghaleb, A Zainal, M Rassam, Data verification and misbehavior detection in vehicular ad-hoc networks. J. Teknologi. **73**(2), 37–44 (2015)
7. S Ruj, MA Cavenaghi, Z Huang, A Nayak, I Stojmenovic, in *Vehicular Technology Conference (VTC Fall), 2011 IEEE*. On data-centric misbehavior detection in vanets. (IEEE, 2011), pp. 1–5
8. X Shen, X Cheng, L Yang, R Zhang, B Jiao, Data dissemination in vanets: a scheduling approach. IEEE Trans. Intell. Transp. Syst. **15**(5), 2213–2223 (2014)
9. J Molina-Gil, P Caballero-Gil, C Caballero-Gil, Countermeasures to prevent misbehaviour in VANETs. J. UCS. **18**(6), 857–873 (2012)
10. M Khalid, Z Ullah, N Ahmad, H Khan, HS Cruickshank, OU Khan, in *Recent Trends in Telecommunications Research (RTTR), Workshop On*. A comparative simulation based analysis of location based routing protocols in underwater wireless sensor networks (IEEE, 2017), pp. 1–5
11. 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, 2012), pp. 73–82
12. M Khalid, Z Ullah, N Ahmad, A Adnan, W Khalid, A Ashfaq, Comparison of localization free routing protocols in underwater wireless sensor networks. Int. J. Adv. Comput. Sci. Appl. **8**(3), 408–414 (2017)
13. T Qiu, D Luo, F Xia, N Deonauth, W Si, A Tolba, A greedy model with small world for improving the robustness of heterogeneous internet of things. Comput. Netw. **101**, 127–143 (2016)
14. X Cheng, C Chen, W Zhang, Y Yang, 5g-enabled cooperative intelligent vehicular (5genciv) framework: when benz meets marconi. IEEE Intell. Syst. **32**(3), 53–59 (2017)
15. J Grover, MS Gaur, V Laxmi, RK Tiwari, in *Proceedings of the Fifth International Conference on Security of Information and Networks*. Detection of incorrect position information using speed and time span verification in vanet. (ACM, 2012), pp. 53–59
16. T Leinmuller, RK Schmidt, E Schoch, A Held, G Schafer, in *GLOBECOM Workshops, 2008 IEEE*. Modeling roadside attacker behavior in VANETs (IEEE, 2008), pp. 1–10
17. J Grover, MS Gaur, V Laxmi, in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*. Position forging attacks in vehicular ad hoc networks: implementation, impact and detection. (IEEE, 2011), pp. 701–706
18. G Yan, S Olariu, MC Weigle, Providing VANET security through active position detection. Comput. Commun. **31**(12), 2883–2897 (2008)
19. T Leinmuller, E Schoch, F Kargl, Position verification approaches for vehicular ad hoc networks. IEEE Wireless Commun. **13**(5) (2006)
20. K Penna, V Yalavarthi, H Fu, Y Zhu, in *Neural Networks (IJCNN), 2014 International Joint Conference On*. Evaluation of active position detection in vehicular ad hoc networks (IEEE, 2014), pp. 2234–2239
21. M Raya, J-P Hubaux, Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
22. RW Van der Heijden, F Kargl, OM Abu-Sharkh, A Al-Momani, in *IEEE Vehicular Technology Conference*. Enhanced position verification for vanets using subjective logic. (Universität Ulm, 2016)
23. SK Harit, G Singh, N Tyagi, in *Computer and Communication Technology (ICCCT), 2012 Third International Conference On*. Fox-hole model for data-centric misbehaviour detection in vanets. (IEEE, 2012), pp. 271–277
24. MN Mejri, J Ben-Othman, M Hamdi, Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. **1**(2), 53–66 (2014)
25. R Zhang, X Cheng, Q Yao, C-X Wang, Y Yang, B Jiao, Interference graph-based resource-sharing schemes for vehicular networks. IEEE Trans. Veh. Technol. **62**(8), 4028–4039 (2013)
26. X Cheng, Q Yao, M Wen, C-X Wang, L-Y Song, B-L Jiao, Wideband channel modeling and intercarrier interference cancellation for vehicle-to-vehicle communication systems. IEEE J. Selected Areas Commun. **31**(9), 434–448 (2013)
27. B Mishra, P Nayak, S Behera, D Jena, in *Proceedings of the 2011 International Conference on Communication, Computing & Security*. Security in vehicular adhoc networks: a survey. (ACM, 2011), pp. 590–595
28. BK Chaurasia, S Verma, GS Tomar, in *Communication Systems and Network Technologies (CSNT), 2013 International Conference On*. Trust computation in vanets. (IEEE, 2013), pp. 468–471
29. X Cheng, L Yang, X Shen, D2d for intelligent transportation systems: a feasibility study. IEEE Trans. Intell. Transp. Syst. **16**(4), 1784–1793 (2015)
30. M Altayeb, I Mahgoub, A survey of vehicular ad hoc networks routing protocols. Int. J. Innov. Appl. Stud. **3**(3), 829–846 (2013)
31. Z Huang, On reputation and data-centric misbehavior detection mechanisms for VANET. PhD thesis (2011)
32. M Khalid, Z Ullah, N Ahmad, M Arshad, B Jan, Y Cao, A Adnan, A survey of routing issues and associated protocols in underwater wireless sensor networks. J. Sensors, 7539751 (2017)
33. R Zhang, X Cheng, L Yang, X Shen, B Jiao, A novel centralized tdma-based scheduling protocol for vehicular networks. IEEE Trans. Intell. Transp. Syst. **16**(1), 411–416 (2015)
34. X Cheng, C-X Wang, DI Laurenson, S Salous, AV Vasilakos, An adaptive geometry-based stochastic model for non-isotropic mimo mobile-to-mobile channels. IEEE Trans. Wireless Commun. **8**(9) (2009)
35. F Zeng, R Zhang, X Cheng, L Yang, Channel prediction based scheduling for data dissemination in vanets. IEEE Commun. Lett, 1409–1412 (2017)
36. L Zhang, Q Wu, A Solanas, J Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications. IEEE Trans. Veh. Technol. **59**(4), 1606–1617 (2010)
37. T Leinmuller, E Schoch, C Maihofer, in *Wireless on Demand Network Systems and Services, 2007. WONS'07. Fourth Annual Conference On*. Security requirements and solution concepts in vehicular ad hoc networks. (IEEE, 2007), pp. 84–91
38. A Wasef, X Shen, in *Communications (ICC), 2010 IEEE International Conference On*. Efficient group signature scheme supporting batch verification for securing vehicular networks. (IEEE, 2010), pp. 1–5
39. X Cheng, C-X Wang, B Ai, H Aggoune, Envelope level crossing rate and average fade duration of nonisotropic vehicle-to-vehicle ricean fading channels. IEEE Trans. Intell. Transp. Syst. **15**(1), 62–72 (2014)
40. X Cheng, C-X Wang, DI Laurenson, S Salous, AV Vasilakos, New deterministic and stochastic simulation models for non-isotropic scattering mobile-to-mobile rayleigh fading channels. Wireless Commun. Mobile Comput. **11**(7), 829–842 (2011)

41. Y Qian, N Moayeri, in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*. Design of secure and application-oriented vanets. (IEEE, 2008), pp. 2794–2799
42. A-E Mihaita, C Dobre, F Pop, CX Mavromoustakis, G Mastorakis, in *Advances in Mobile Cloud Computing and Big Data in the 5G Era*. Secure opportunistic vehicle-to-vehicle communication. (Springer, 2017), pp. 229–268
43. RG Engoulou, M Bellaïche, S Pierre, A Quintero, Vanet security surveys. Comput. Commun. **44**, 1–13 (2014)
44. X Lin, X Sun, P-H Ho, X Shen, GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. **56**(6), 3442–3456 (2007)
45. M Tilal, R Minhas, Effects of Jamming on IEEE 802.11 p Systems (2010)
46. J Sun, Y Fang, in *Military Communications Conference, 2008. MILCOM 2008. IEEE*. A defense technique against misbehavior in vanets based on threshold authentication. (IEEE, 2008), pp. 1–7
47. S Zeadally, R Hunt, Y-S Chen, A Irwin, A Hassan, Vehicular ad hoc networks (vanets): status, results, and challenges. Telecommun. Syst. **50**(4), 217–241 (2012)
48. B Pooja, MM Pai, RM Pai, N Ajam, J Mouzna, in *Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference On*. Mitigation of insider and outsider dos attack against signature based authentication in vanets. (IEEE, 2014), pp. 152–157
49. S Jiang, X Zhu, L Wang, An efficient anonymous batch authentication scheme based on HMAC for VANETs. IEEE Trans. Intell. Transp. Syst. **17**(8), 2193–2204 (2016)
50. K Zaidi, M Rajarajan, Vehicular internet: security & privacy challenges and opportunities. Future Internet. **7**(3), 257–275 (2015)
51. N Ahmad, H Cruickshank, Z Sun, M Asif, in *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference On*. Pseudonymised communication in delay tolerant networks. (IEEE, 2011), pp. 1–6
52. M Azees, P Vijayakumar, LJ Deboarh, Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst., 2467–2476 (2017)
53. J Freudiger, M Raya, M Félegyházi, P Papadimitratos, J-P Hubaux, in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*. Mix-zones for location privacy in vehicular networks, (2007)
54. F Qu, Z Wu, F-Y Wang, W Cho, A security and privacy review of VANETs. IEEE Trans. Intell. Transp. Syst. **16**(6), 2985–2996 (2015)
55. R van der Heijden, S Dietzel, F Kargl, *Misbehavior detection in vehicular ad-hoc networks*. (Proceedings of the 1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2013), 2013)
56. RW van der Heijden, S Dietzel, T Leinmüller, F Kargl, Survey on misbehavior detection in cooperative intelligent transportation systems (2016). arXiv preprint arXiv:1610.06810
57. A Daeinabi, AG Rahbar, Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks. Multimedia Tools Appl. **66**(2), 325–338 (2013)
58. N-W Lo, H-C Tsai, in *Globecom Workshops, 2007 IEEE*. Illusion attack on vanet applications—a message plausibility problem. (IEEE, 2007), pp. 1–8
59. T Leinmüller, E Schoch, F Kargl, C Maihöfer, Decentralized position verification in geographic ad hoc routing. Secur. Commun. Netw. **3**(4), 289–302 (2010)
60. J Grover, NK Prajapati, V Laxmi, MS Gaur, in *International Conference on Advances in Computing and Communications*. Machine learning approach for multiple misbehavior detection in VANET. (Springer, 2011), pp. 644–653
61. H Sedjelmaci, SM Senouci, MA Abu-Rgheff, An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. IEEE Internet Things J. **1**(6), 570–577 (2014)
62. RP Barnwal, SK Ghosh, in *Connected Vehicles and Expo (ICCVE), 2012 International Conference On*. Heartbeat message based misbehavior detection scheme for vehicular ad-hoc networks (IEEE, 2012), pp. 29–34
63. M Ghosh, A Varghese, AA Kherani, A Gupta, in *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*. Distributed misbehavior detection in VANETs (IEEE, 2009), pp. 1–6
64. M Ghosh, A Varghese, A Gupta, AA Kherani, SN Muthaiah, Detecting misbehaviors in vanet with integrated root-cause analysis. Ad Hoc Netw. **8**(7), 778–790 (2010)
65. M Raya, P Papadimitratos, I Aad, D Jungels, J-P Hubaux, Eviction of misbehaving and faulty nodes in vehicular networks. IEEE J. Selected Areas Commun. **25**(8) (2007)
66. P Golle, D Greene, J Staddon, in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*. Detecting and correcting malicious data in VANETs. (ACM, 2004), pp. 29–37
67. TH-J Kim, A Studer, R Dubey, X Zhang, A Perrig, F Bai, B Bellur, A Iyer, in *Proceedings of the Seventh ACM International Workshop on VehiculAr InterNETworking*. VANET alert endorsement using multi-source filters (ACM, 2010), pp. 51–60
68. A Vulimiri, A Gupta, P Roy, SN Muthaiah, AA Kherani, in *International Conference on Research in Networking*. Application of secondary information for misbehavior detection in VANETs. (Springer, 2010), pp. 385–396
69. K Sha, S Wang, W Shi, rd^4: Role-differentiated cooperative deceptive data detection and filtering in vanets. IEEE Trans. Veh. Technol. **59**(3), 1183–1190 (2010)
70. J Rezgui, S Cherkaoui, in *Local Computer Networks (LCN), 2011 IEEE 36th Conference On*. Detecting faulty and malicious vehicles using rule-based communications data mining (IEEE, 2011), pp. 827–834
71. D Huang, SA Williams, S Shere, in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference On*. Cheater detection in vehicular networks. (IEEE, 2012), pp. 193–200
72. T Yang, W Xin, L Yu, Y Yang, J Hu, Z Chen, in *Asia-Pacific Web Conference*. Misdis: an efficent misbehavior discovering method based on accountability and state machine in vanet. (Springer, 2013), pp. 583–594
73. K Zaidi, MB Milojevic, V Rakocevic, A Nallanathan, M Rajarajan, Host-based intrusion detection for vanets: a statistical approach to rogue node detection. IEEE Trans. Veh. Technol. **65**(8), 6703–6714 (2016)
74. K Govindan, P Mohapatra, Trust computations and trust dynamics in mobile adhoc networks: a survey. IEEE Commun. Surv. Tutorials. **14**(2), 279–298 (2012)
75. A Tajeddine, A Kayssi, A Chehab, in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference On*. A privacy-preserving trust model for VANETs. (IEEE, 2010), pp. 832–837
76. NJ Patel, RH Jhaveri, Trust based approaches for secure routing in VANET: a survey. Procedia Comput. Sci. **45**, 592–601 (2015)
77. P Wex, J Breuer, A Held, T Leinmuller, L Delgrossi, in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*. Trust issues for vehicular ad hoc networks (IEEE, 2008), pp. 2800–2804
78. A Rivero-García, I Santos-González, P Caballero-Gil, C Caballero-Gil, in *Parallel, Distributed, and Network-Based Processing (PDP), 2016 24th Euromicro International Conference On*. Vanet event verification based on user trust. (IEEE, 2016), pp. 313–316
79. N Bismeyer, S Mauthofer, KM Bayarou, F Kargl, in *Vehicular Networking Conference (VNC), 2012 IEEE*. Assessment of node trustworthiness in vanets using data plausibility checks with particle filters. (IEEE, 2012), pp. 78–85
80. B Płaczek, M Bernas, in *International Conference on Computer Networks*. Detection of malicious data in vehicular ad hoc networks for traffic signal control applications. (Springer, 2016), pp. 72–82
81. H Al Falasi, N Mohamed, H El-Syed, in *Hybrid Intelligent Systems*. Similarity-based trust management system: data validation scheme. (Springer, 2016), pp. 141–153
82. Z Cao, J Kong, U Lee, M Gerla, Z Chen, in *INFOCOM Workshops 2008, IEEE*. Proof-of-relevance: filtering false data via authentic consensus in vehicle ad-hoc networks. (IEEE, 2008), pp. 1–6
83. F Dotzer, L Fischer, P Magiera, in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on A*. Vars: A vehicle ad-hoc network reputation system. (IEEE, 2005), pp. 454–456
84. N-W Lo, H-C Tsai, A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP J. Wirel. Commun. Netw. **2009**(1), 125348 (2009)
85. Q Ding, X Li, M Jiang, X Zhou, in *Wireless Communications and Signal Processing (WCSP), 2010 International Conference On*. Reputation-based trust model in vehicular ad hoc networks. (IEEE, 2010), pp. 1–6
86. Z Huang, S Ruj, M Cavenaghi, A Nayak, in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium On*. Limitations of trust management schemes in VANET and countermeasures. (IEEE, 2011), pp. 1228–1232

87. C-H Kim, I-H Bae, in *Embedded and Multimedia Computing Technology and Service*. A misbehavior-based reputation management system for vanets. (Springer, 2012), pp. 441–450
88. ZA Abdulkader, A Abdullah, MT Abdullah, ZA Zukarnain, Vehicular ad hoc networks and security issues: survey. Modern Appl. Sci. **11**(5), 30 (2017)
89. D Zhang, FR Yu, Z Wei, A Boukerche, in *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*. Software-defined vehicular ad hoc networks with trust management. (ACM, 2016), pp. 41–49
90. AS Alkalbani, AM Tap, T Mantoro, in *Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference On*. Energy consumption evaluation in trust and reputation models for wireless sensor networks. (IEEE, 2013), pp. 1–6
91. X Yao, X Zhang, H Ning, P Li, Using trust model to ensure reliable data acquisition in VANETs. Ad Hoc Netw. **55**, 107–118 (2017)
92. A Kumar, JR Singh, D Singh, RK Dewang, in *Computational Intelligence and Networks (CINE), 2016 2nd International Conference On*. A historical feedback based misbehavior detection (HFMD) algorithm in VANET. (IEEE, 2016), pp. 15–22
93. A Wasef, R Lu, X Lin, X Shen, Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]. IEEE Wireless Commun. **17**(5) (2010)
94. B Premasudha, VR Ram, J Miller, R Suma, A review of security threats, solutions and trust management in VANETs. Int. J. Next-Generation Comput. **7**(1), 38–57 (2016)
95. TRV Krishna, RP Barnwal, SK Ghosh, in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference On*. MDS-based trust estimation of event reporting node in vanet. (IEEE, 2013), pp. 315–320
96. W Li, H Song, Art: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans. Intell. Transport. Syst. **17**(4), 960–969 (2016)
97. RK Schmidt, T Leinmüller, E Schoch, A Held, G Schäfer, in *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008)*. Vehicle behavior analysis to enhance security in vanets (IEEE, 2008)
98. A Wu, J Ma, S Zhang, in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference On*. Rate: a RSU-aided scheme for data-centric trust establishment in vanets. (IEEE, 2011), pp. 1–6
99. J Zhang, in *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference On*. A survey on trust management for VANETs. (IEEE, 2011), pp. 105–112
100. S Ahmed, K Tepe, in *Wireless Communications and Networking Conference (WCNC), 2016 IEEE*. Misbehaviour detection in vehicular networks using logistic trust. (IEEE, 2016), pp. 1–6
101. H Zhu, X Lin, R Lu, P-H Ho, X Shen, in *Communications, 2008. ICC'08. IEEE International Conference On*. Aema: an aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks. (IEEE, 2008), pp. 1436–1440
102. L-Y Yeh, Y-C Lin, A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks. IEEE Trans. Intell. Transport. Syst. **15**(4), 1607–1621 (2014)
103. R Lu, X Lin, X Liang, X Shen, A dynamic privacy-preserving key management scheme for location-based services in VANETs. IEEE Trans. Intell. Transport. Syst. **13**(1), 127–139 (2012)
104. A Boualouache, S-M Senouci, S Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks. IEEE Commun. Surv. Tutor (2017)