Jurnal Teknologi

Full paper

Data Verification and Misbehavior Detection in Vehicular Ad-hoc Networks

Fuad A. Ghaleb[a*], Anazida Zainal[a], Murad A. Rassam[b]

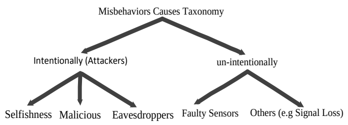
[a]*Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia*
[b]*Faculty of Engineering and Information Technology, Taiz University, Yemen*

*Corresponding author: fuadeng@gmail.com

Article history

Received :10 December 2014
Received in revised form :
1 February 2015
Accepted :12 February 2015

Graphical abstract



Abstract

Vehicle Ad hoc Network (VANET) is an emerging and promising technology for the Intelligent Transportation System (ITS). VANET can help to increase safety and traffic efficiency in flexible and feasible way. However, disseminating incorrect information in VANET has wide range of implications effecting drivers' behaviors and causing serious, and may be catastrophic, results. Misbehaving attackers can create traffic illusion to disturb VANET operations as well as the potential deployment of safety and traffic efficiency applications. In this paper, a holistic view of the existing misbehavior detection approaches for countermeasures against spreading malicious data in VANET is studied. In addition, the importance and the challenges faced when verifying the correctness of VANET messages are discussed. Finally, the drawbacks of existing detection and verification approaches are analyzed.

Keywords: ITS; VANET; misbehavior detection; malicious data verification

■1.0 INTRODUCTION

With the increasing demands of the private vehicles wide world, traffic accidents and congestions are increased lifted disastrous figures of fatalities, loss of properties and affecting the economic growth. Intelligent Transportation System (ITS) is a passive system used for monitoring the roads visually using cameras and displays the warning on screens hanging on the roads. It needs many infrastructures to be installed along the roads. Thus, the traditional ITS is considered very expensive (installing, maintaining, computation and processing cost) causing lack of availability. For that, Vehicle Ad Hoc Network (VANET) is proposed to enhance ITS efficiency, scalability, and availability.

In VANET, vehicles can exchange information about their status, roads hazards, or traffic situations to warn others. Vehicles can communicate with each other via a WiFi-like interface installed in each vehicle. This communications will enhance vehicles' awareness of its environment and thus reduce the road accidents and optimize the traffic flows [1]. Vehicles communicate via a Dedicated Short Range Communication Protocol (DSRC), in which different types of communications can be obtained such as vehicle-to-vehicle (V2V), vehicle to infrastructure (V2I) or both between vehicle-to-infrastructure/vehicle (V2X) [2]. With this emerging technology, wide range of applications for safety, traffic efficiency and passenger comfort has been suggested. An extensive summary of VANET applications can be found in [3-6].

Safety and traffic efficiency applications received a significant interest from researchers and industries. V2V communication type has advantages over V2I such as low operation cost, and flexibility. V2V type motivates misbehaving nodes to inject false information to the network. Even if the majority are honest in VANET, a few misbehaving nodes that send false information can disturb the whole network operations.

Security plays a vital role in VANET deployment. Without employing strong security, VANET applications could be used against the community by criminals [6]. Developing proper security mechanisms that prevent attackers from abusing VANETs applications is challenging task [7]. Most of the critical threats are coming from the internal nodes. Internal attackers can be active that threaten the whole VANET operations or passive that threaten user privacy. An active insider can send false information which might cause serious accidents that may lead to threaten people lives and lose their properties and affect the practical deployment of VANETs. Securing VANET has been extensively studied by many researchers and it has achieved significant growth: the related works can be found in those surveys [7-10]. The Public Key Infrastructures (PKI) has been introduced as the security solution for VANET in [2]. Actually, current research mainly focuses on the integrity and authentication mechanisms which are partial solutions for VANET.

The main different between VANET and other ad hoc networks that VANET nodes (vehicles) are the source and the target of the information i.e. if vehicle has an observation about the road, it send messages based on that observation asking other nodes to believe its own observation and change their behaviors. From this point of view, attackers in VANET can send false information aiming to gain some advantage or causing problems for road users and may be serious for people lives and properties. One of the serious attacks in the application level is called illusion attack [11], in which the attacker sends false mobility information about his to motivate the corresponding system to send wrong traffic warning. Therefore, VANET information must be verified and validated before relayed to the operations. There is no way to defend against these types of attacks rather than detecting them. Data validation is necessary to ensure that the received information is reliable. Data is reliable when it is reflect the ground truth [12]. How network nodes in VANET can autonomously evaluate the plausibility of the information in the context of the road status such as accidents, or vehicles status such as breaking, or mobility data and etcetera? This question is a hot research challenge in VANET and it is discussed in this paper. We surveyed and analyzed the methods that are proposed for verifying VANET data with considering security, and privacy issues in the discussion.

The paper is organized as follow: Section 2 illustrates types of malicious data in VANET. Section 3 describes the significance of data verification in VANET. Section 3 describes the possible misbehavior data in VANET. In section 4, we describe the challenges facing possible misbehavior in the VANET. In section 5, analyzing the current approaches for data verifications is presented and discussed. Section 6 concludes the paper.

2.0 MISBEHAVIOR IN VANET

Malicious data is the type of data that is not represents the ground truth. Misbehaving nodes may send false information intentionally or due to unintentional faults in their operations. Misbehavior is a term used in the ad hoc networks for any deviation from the expected behavior. In VANET, deviating from normal operation can take many forms such as sending false information, conceal some information, tamper with messages content such as identity, alert type, event location, node position, and time, creating fake messages, or forcing another node to send false message are considered misbehaviors in data and need to be detected each time a message received. According to Gosh *et al.,* in [13], a node is called misbehaving node when it can send messages claiming an event that either has not occurred, or wrong information confirming a real event, or both, causing applications to failure.

Generally in VANET, misbehaviors can exist at any layer of the network. For example, in physical layer outsider attackers can lunch DoS by jamming attack, tamper with hardware, or deceive sensors to send false information. In data link layer vehicles can send bogus information by altering beaconing rate or lunching channel capturing attack. At network level, a malicious node can spoof the identity of another node to receive specific information. Another serious threats presence of black hole attack on the network where an attacker claim its existing in best location to forward the information. Wormhole attack where multiple nodes could be black hole nodes agreed to transfer the event happened in place to make another event in the second place such as accident. In the application layer malicious vehicle can generate false messages such as pretending to be in multiple locations e.g. Sybil attack. Sybil attack could be a source for every possible attack in VANET. It can deceive some verification mechanisms that based on the voting and can implement black and worm whole attack. Also it can send bogus information to cause node fall into fake computational and communication overhead.

Misbehavior can be intentionally for malicious or selfish reasons or it can be unintentionally due malfunction of the hardware equipment or other signal related problem such as signal loss. Figure 1 shows misbehavior causes taxonomy.

There are two types of messages that are used for enabling VANET safety and traffic efficiency applications. These messages can be classified based on their generation: periodic or event driven. Vehicles use periodic messages so called beacons for announcing their existence in the network. Beacons are broadcasted continuously contains position, time and mobility information such as speed accelerating of the vehicles. Vehicles use this information to take farther decision about their physical or network behaviors. For example in safety application vehicle, vehicle can detect abnormal situations on the roads such as accidents or congestions even before they appear. The second type of messages is the event driven messages which are resulted from the interaction among three objects vehicles, roads, and drivers.

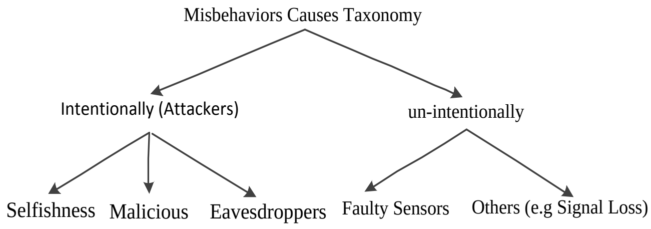


Figure 1 Misbehavior detection causes

3.0 IMPORTANCE OF MISBEHAVIOR DETECTION IN VANET

For many considerations such as implementation cost and availability, VANET applications rely on V2V communications. In the absence of the infrastructure, there will be malicious data. Even with high security mechanisms, a vehicle can issue false information unintentionally (e.g. faulty nodes) or intentionally by simply manipulating vehicle sensors [14]. Detecting malicious content is very important for VANET applications. Moreover, most VANET applications will use geographical routing protocols where the position will be used to achieve better routing and enhance network performance [15]. In addition, safety and traffic efficiency needs reliable and trusted data. Verify the plausibility of VANET data is necessary for reliability of the decision taking to avoid use this information. Moreover, detecting misbehaving node that send false information is important to be stopped or isolated from disturb network operations such in [16]. Recently, many misbehavior detection mechanisms have been proposed in order to enhance VANET security and safety. For accountability and liability, detecting the misbehaving nodes allow authorities to penalize the actual sender of the false information and discourage the intentionally misbehaving.

4.0 CHALLENGES

Although VANET is considered a form of MANET, VANET behavior is fundamentally different, even from any existing ad hoc network. This diverse introduces many unique characteristics such as rapid topology change because of high mobility of the vehicles and causing frequent dis-connectivity and network segmentation. The connectivity time span among nodes may be very short. Thus, it is difficult to maintain secure and reliable communications [17]. Network density has high variance in small amount of time which leads to scalability or availability problems. As mentioned earlier, VANET is the source and the target of the information make it very sensitive to messages contain. For that, false messages could be fatal on the applications. For example, drivers might adjust their behaviors based on the data received from uncertain environment which could be fetal for people life and properties. Some applications such that related to safety need strict deadline [18].

Another challenge for implementing VANET applications is user motivations. Research has shown that 60% of accidents could be avoided if drivers were warned half a second before the impact of a collision [19]. However, presence of malicious data in the network can lead to degrade traffic efficiency or/and catastrophic accidents. In the following subsections, we briefly describe some of the challenges of data verification in VANET.

4.1 Entity Verification

VANE needs imposing strong authentication mechanisms in which attackers (e.g. Sybil) cannot impersonate other vehicles entities. However, in ephemeral network, such VANET, the communication between vehicles is very short and the topology is rapidly changes. For that, scalability, and real time requirements are important for secure communication in VANET. Verifying data of individual vehicle is very important to assess the behavior of their owner. Therefore, linking multiple messages from single vehicle is required for data verification. In the other hand, messages link-ability is a privacy concern. Vehicles are personal property and people are very concern about the privacy of their information. Drivers will not accept having their movement tracked by peers. Authentication protects vehicles from being impersonated by the Sybil attackers. However, it facilitates privacy violating by allowing attacker linking the messages of individual vehicle and track their journey or extract their privacy information such as driver name, or vehicle number.

4.2 Position Verification

Most VANET application, if not all, depends on reliable position information [20]. In some cases, vehicle position is used as vehicle identity to provide anonymity and protect its privacy [21]. Then, in such anonymity scenario, Sybil attackers can claim its existence in multiple location, thus the false information can be injected in the network. For example, a greedy driver uses multiple locations to report congestion in a specific region of the road causing other vehicle change their routes. In addition, vehicle position can be used to help routing protocol [22]. Moreover, positioning systems such as geographical positioning systems (GPS) is not accurate enough and it suffers availability problem e.g. in the tunnels, or bad weather [23]. Besides, GPS signal can be forged causing vehicles send its existence in false positions [9]. According to Yang *et al.*, in [24], verifying vehicles position is the most important issue for safety. Leinmuller *et al.* at in [22] described the effect of falsify position information on the performance geographical routing in VANET. Generally, frogged or cheated position can lead to many kind of attacks such as illustrated in Figure 2. Sybil attack [25], black hole attack [26], worm hole attack [27] are considered among serious threats for VANET safety and traffic efficiency applications.

4.3 Time Verification

In contrast to the traditional fixed network, VANET may has not access regularly to central control. Time is an important element in VANET for succession of all type of applications message verifications. VANETs assume the availability of common sources of time, such as base-stations or GPS. With the absence of clock synchronization, nodes need comparing the time of the upcoming messages with its local time. Safety applications is time critical wrong time estimation may lead to serious problem e.g. accidents. Vehicles may ignore some important safety messages while they might be very critical due to un-successful time verification. In addition, some verification techniques needs accurate timing among noes such that proposed in [14] for position verification.

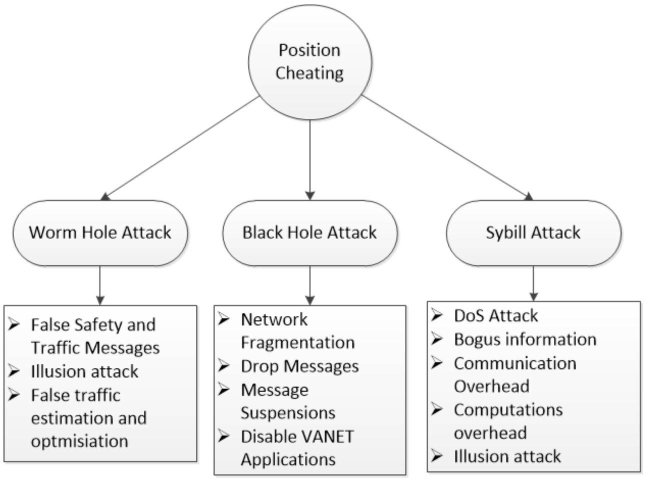


Figure 2 Threats of position cheating

4.4 Mobility Verification

Rather than information security perspective, human factor in VANET imposes very challenge problems. Vehicles movement information is a reflection of the driving activities and driver status. Drivers' behaviors are unpredicted and varied from driver to driver based on many psychological features such as driver propensity, status, driving time, and many other complex features. Verify the correctness or the validity of any reporting situation could be impossible, without relating vehicle behavior to this situations and data. In addition, monitoring the historical behavior of individual vehicle or driver weaken the privacy requirements and increase the detection delays. However, one can benefit from the high dynamic topology change in VANET to build a system that can track vehicles behaviors temporary on the fly, and then, deduce the drivers' behaviors without violating their privacy. With presence of many threats such as localization errors and faulty vehicles as well as the attackers, mobility information is not reliable and the decision upon this information may be uncertain.

4.5 Event Verification

VANET applications have different requirements. For example, traffic efficiency applications are delay tolerant whereas safety applications are time critical. Most safety applications relay on single hope communications whereas traffic efficiency applications are multi-hop. Moreover, each application has different context. For example, electronic brake light application needs the deceleration information from vehicles in safety relevance area which is within single hope within an area located in front of the vehicles whereas, post-crash notification require several hops behind the sender. The plausibility of the event may not relate to the trustworthiness of the sender that most security techniques aim to provide. Vehicles must be confident about the information received from open and hostile environment such the case in VANET.

■5.0 DEFENSE AGAINST MISBEHAVIOR IN VANET

Misbehavior detection and data validation is open and active area of research in VANET, especially data related to safety and traffic efficiency [28]. To prevent spreading false information in the network proactive or reactive security mechanisms are used in the literature.

5.1 Proactive Security Mechanisms

Proactive mechanisms aiming to prevent spreading false messages by implementing security mechanisms such as Public Key Infrastructure (PKI) or/and digital signature with or without certificate along with tamper proof devices [29]. For example, the standard approach to provide secure communication in VANET is based on Entity-Trust, which is stablished by implementing public key infrastructure, signing the messages with digital signatures and verified through a certificate issued to vehicle by authority [8, 16, 30]. These mechanisms successes in preventing outsider attackers and prohibit some insider attackers from spreading fraudulent messages. However, insider attackers can generate legitimated false information for many reasons intentionally such as selfishness or malicious or a faulty vehicle may generate false messages unintentionally. Moreover, such mechanisms faced many challenges such as scalability and complex management and still open research problems. Generally, cryptographic signatures trust establishment does not guarantee the correctness of the content especially when the vehicles have not directly interacted before with each other’s e.g. multi-hop network. Moreover, the decision of the correctness of the information cannot be taken by knowing the trustworthiness of the originators. In addition, proactive security mechanisms may suffer scalability problem due its need for key management, revocation, and pseudonymous. However, it can be maintained through a combination of infrastructure and tamper proof hardware such solutions found in [16].

5.2 Threshold Based Authentication

Vehicle relays information only if it is true. One approach to endorse messages, a message is true if it’s reported by threshold number of authenticated vehicles (assuming majority honest) [31]. However, this approach increases the communication and computation overhead. For instance, in the congestions many vehicles may report the congestion and causing network to fail. Using multiple signatures such as concatenated signatures, onion signatures, and hybrid signatures may not suitable for time critical applications [32]. As noted by Douceur in [33], Sybil attack can make the mechanisms that use redundancy fails in distributed systems. Moreover, threshold based validation is inefficient for safety [28], because safety require quick and accurate validation algorithms. The need and challenge in how to employing a mechanism for validating safety on the fly. According to [28], threshold validation mechanisms consider a subset of the information to validate the messages which may introduce malicious information from misbehaving node. Employing methods based on the entity (Entity-Centric) is not enough to secure VANET against false information. The assumption that vehicle is responsible or reliable on theirs generated information may prohibit vehicles from claiming wrong information otherwise they will receive punitive actions from the authority.

Message authentication raised very critical issue in VANET. Attackers can link multiple messages from a vehicle to track or extract valuable information about the drivers [34]. Therefore, privacy preserving should be adopted in the early stage of security design. Privacy can be provided through anonymity and unlinkability i.e. the message should resist to be linked together [32]. The stander way to preserve privacy is to provide vehicles with pseudonyms keys. Vehicles use different key in each time interval as described in the IEEE standard [30]. Accordingly, the attacker cannot link messages from the same vehicles. However, this in turn raised critical security and safety issues. Malicious vehicles can use its pseudonym keys to sign false messages and create illusion about the traffic. Anonymity encourages misbehaving nodes to send false information without fears of the liability. Number of efforts to balance security and privacy has been proposed in the literature such as in [35-45].

5.3 Reactive Security Mechanisms

A few solutions have been proposed in the literature aim to complement proactive countermeasures with reactive approaches such as in [1, 46-49]. Reactive security mechanisms can be grouped into two classes: Entity Centric detection approaches and Data plausibility and consistency approaches. First approach is called Entity-Centric, which can identify the misbehaving node. Identifying misbehaving node require a system be able to distinguish between node entities. Usually, trusted establishment based on authentication with trusted third party PKI or cooperatively e.g. group signature is used to issue public and private key for each node. Sender vehicle then can use digital signature to sign the message. Receiver on the other side can identify the sender node by verifying its signature. Some examples of Entity-Centric approaches have been proposed in [16, 50]. The second approach of detection mechanism is Data-Centric in which, the correctness of the received data is investigated instead of investigating the trustworthiness of the sender. Data plausibility and consistency check is used to detect incorrect messages. It is similar to intrusion detection systems in traditional networks in which vehicles correlate the received information with the information already known from pervious interaction or predefined thresholds such as speed limits. One of the critical problems of misbehavior detection in proactive security countermeasures, misbehavior detection mechanisms could be aggressive against abnormal vehicles during some unusual events such as accidents and braking. Thus, they will be classified as misbehaving nodes. Another problem related to data-centric misbehavior detection, that it encourage malicious vehicle to exploit the absence of entity verification to launch Sybil attack. So, balancing security and privacy is needed such that in [51]. From other side, in data centric security mechanisms, privacy can be maintained through anonymity but, it encourage vehicles to inject false data without fear of being tracked or punished.

■6.0 EXISTING WORKS IN MISBEHAVIOR DETECTION

The first existing work for verifying and correcting malicious data and detecting the misbehaving node in VANET has been introduced by Golle *et al.* [47]. A general approach has been proposed to validate VANET data based on assumption that each node has a model of VANET. Each node checks the validity of the received data based on local sensors such as camera, infrared, and radars. When inconsistencies are detected, based on parsimony argument an adversarial model is used to find the best explanation of this information to correct them. The approach can provide explanations to the incorrect information and find the source of this information, so it can be used in accountability and liability requirements applications. Authentication always happens among the neighboring nodes thus the nodes are authenticated using their security materials and the local sensors. In addition, to violate the privacy attacker needs to be close to the victims all the time during the tracking and this is costly attacks. Position of the vehicles is well verified using the local sensors such as cameras and infrared as well as the Sybil node will be detected easily. However, using redundant sensors to verify the data received may leads to degrade the performance of the detection through false reading and minimize the detection area to direct neighbours. VANET allow vehicles to sense a broader area than local sensors do. Moreover, how the models are crated and maintained is not present. The assumption of the high density in the road is not applicable for most of the roads so the approach will failed low density regions or from time to time based on the density at the particular time. There is no validation or performance testing for the proposed approach.

Raya *et al.*, [16] proposed a misbehavior detection scheme (MDS) to detect misbehaving or faulty nodes by comparing the behavior of each node with the average behavior of other nodes in its vicinity to build data models on the fly. The entropy is suggested as an effective solution to present data anomalies and normal behavior. By using the K-means clustering technique, they are able to identify the attacker whose data is outlier. Since the MDS can only deals with the data from its directs neighbors, the MDS cannot differentiate between the message originator and message forwarder which lead to false revocation. Moreover, if a real event appears on the low density then the event will consider wrong and this is very critical safety problem.

Schmidt *et al.*, [52] introduced Vehicle Behavior Analysis and Evaluation Scheme (VEBAS) for calculating the trustworthiness of the messages based on the behavior of their sender. The evaluation result is shared with the other vehicles to build reputation system. The authors discussed some important requirement for the detection mechanisms. For example, the detection must be made locally in each node; the system must be coping with the lack of the information such as the loss of the beacons message. In VANET, the neighboring vehicles change quickly therefore establishing trust could be difficult. In addition, the trustworthy nodes might misbehave because of selfishness or due to faulty nodes. The first misbehaving of a trusted node will not be detected automatically accordingly; trustworthiness will not be degraded [14]. No specific applications are investigated in their work and no performance analysis or evaluation in various road scenarios has been performed.

Ghosh *et al.*, in [50] introduced a model for detecting false alerts in PCN application. The proposed method based on monitoring the driver behavior of the sender after sending the alert. If the alert is true, then the driver will take the necessary actions to avoid the crash location such as stopping the car or changing the current lane. If the alert is false then the driver will continue moving and will not response to the alert. The assumption that the position is always accurate and correct is not valid for the applications that relay mainly on the positions, i.e., the position itself must be verified. To avoid this assumption, Ghosh *et al.*, [13] enhanced the previous model by finding the root cause of the false data. Sender vehicle will follow free-flow mobility model until an alert is raised. Then, after the alert position, it is expected for the sender to follow the crash-modulated mobility model. Based on this, the receiver vehicle observed the behavior of the vehicle movement until some points after the reported crash position. If the alert is true, the receiver vehicle follows the free–flow model until the crash location then it will change to crash-modulated.

Kim *et al.*, [53] proposed a framework that introduced messages filtering model. They argued that when vehicles exchange warning messages, it is important that a receiver vehicle should validate the warning, and then only alert the driver once the system has determined that the messages are legitimate. Validate the warning based on two main components: a threshold curve and a Certainty of Event (CoE). A threshold curve denotes the importance of the event to the vehicle position. CoE represents the level of trust the warning. CoE can be calculated from six questions called source of information. By combining the results from all appropriate sources, if CoE curve intersected with threshold curve, then the OBU will notify the driver if the CoE exceed that threshold. The communication overhead only analyzed to endorse the EEBL applications and no farther applications has been tested or evaluated.

Ruj *et al.*, in [14] proposed a misbehavior detection model for verifying more general information compared to Ghosh *et al*. [50]. Several types of alerts can be detected by the model such as crash notification, emergency breaking, approaching emergency vehicles, road feature notifications, change of lanes, etc. Based on the alert type there are some possible events consider as invalid after the alert. The idea of collecting all valid events for each safety application and compared with the actual events taken by the alert sender after sending the alert is promising for generalization. However, the author left the validation for the future work. In addition, the model needs more security and privacy analysis as well as performance testing. Position verification need more mature approach rather than using sender and receiver time.

Yang *et al*., in [24] introduced MisDis which is a method for detecting misbehavers using state automata and supervision. MisDis implemented some ideas from PeerReview system described in [54]. PeerReview is a system that provides accountability in distributed systems. MisDis record all the messages have been sent or received for each peer (node) in a secure log. Therefore, any node can request the secure log of another node and independently can determine whether it has deviated from the expected behavior or not. But, accountability ensures whether the data is documented in the secure log or not regardless of the validity of this data. So, the records may have malicious data or falsified data about the location, event or other mobility information such acceleration and speed. Although, MisDis assume strong identification and authentication scheme, there is no discussion about how the privacy is preserved. In addition, there is no evaluation or testing the performance mentioned in their work.

■7.0 DISCUSSION

As mentioned earlier misbehavior detection in VANET can be categorized based on their detection objectives into two groups Entity-Centric (EC) and Data-Centric (DC). Entity-Centric detection aims to detect the entity that sends false information. A punitive action is taken against the misbehaving node such as revocation its security credentials to stop it from future participating in VANET or/and it will receive a fine from authority. Data-Centric approaches aims to detect the false information regardless of the source of this data. Data-Centric approaches try to investigate the correlation among the VANET data instances such as speeds profile and the message content.

The Entity-Centric approaches can be farther categorized into behavioral based, trusted based, or hybrid. Behavioral based aims to investigate the driver behavior and compare it with expected behavior in specific situation. In the behavioral based approaches e.g. [16], the misbehavior detection monitors the behavior of the node and compare it with the average behaviors of the others node in its vicinity. This approach is not useful in the low density cases where there are no enough nodes in the position of interest such as event position. Event based approaches e.g. [14, 50] start monitoring vehicle behavior of the individual vehicle after the alert is triggered. For example, they can use this information as transient matrix based on Marckov chain to predict the next expected behavior and thus, the alert can be validated. This approach can be useful for some specific applications where the behavior of the node can be expected e.g. [14]. The trusted based aims to assign a trust value for each vehicle based on its historical behaviors.

Reputation based approaches e.g. [52] are not effective because trusted values are slowly change can share false information if it’s compromised or have got faulty sensors. In addition, such models need stable topology whereas in VANET two vehicles might meet only for few seconds during their operating live. Moreover, reputations based model need access to huge data to retrieve the trustworthiness values of the vehicles during the communication. That requires RSUs available each time the need to retrieve this information. Another solution is to store all the trustworthiness values of the vehicles in the OBUs. Both choices are not valid assumptions for several reasons such as speed of retrieving and processing data in real time requirement applications as well as scalability and availability challenges. Instead of building trust on the vehicles, some approaches e.g. [53] put the trust on the data using some filtering models. These approaches are promising in data verification. However, due to the high mobility nature of VANET and frequent dis-connectivity, these approaches are not realistic.

Data-centric misbehavior detection that introduce by Ruj *et al.*, in [14] can be generalized for all misbehavior detection types. However, the proposed models solve event driven misbehavior detection which is the second step after verifying each piece of message content such as speed verification, position verification, identity verification, and so on. In hybrid based, the behaviors are used as the input to build reputations and assign trustworthiness values for each vehicle. A trust value for each vehicle is assigned based on its past behavior. The trust value is made locally and shared to others node to build a reputation system, e.g. [52]. This approach inherits the drawbacks of trust and behavioral based approaches.

Existing approaches focus on single hope data verification. Whereas if the event is beyond the transmission ranges of vehicles this verification methods is not suitable. For traffic efficiency or accident reporting applications, a different verification method should be developed to cope with multi hop communications. A holistic protocol is needed for cover both single hop and multi hop that will be based on cryptographic security measures and data consistency to defense against misbehavior in VANET.

Plausibility and consistency approaches complete each other and can be used interchangeably. Predefined Plausibility checks are considered as a prerequisite for checking data consistency. However, they are both not effective for detecting the malicious data because the fact that misbehaving nodes will try to inject plausible and consistent data.

To conclude the discussion, entity-Centric trust approaches are valuable to defend against misbehavior in VANET and most of the proposed solutions are based on entity centric trust. However, entity-centric are not enough. VANET Data must reflect a specific real world situation such as vehicle position or road situations e.g. accidents or congestion. Detection inconsistencies in data are important as the consistencies may not be made intentionally such as software or hardware shortages or faulty nodes. Data reliability is the most objectives of safety applications. Rational decision must be taken before vehicle reach event locations.

Table 1 Methods and drawbacks of existing misbehavior approaches (DC: Data-Centric EC: Entity-Centric)

MDS	Type	Objectives	Detection Method	Drawbacks
Golle *et al* [26]	Cooperative	DC	• Framework based on the assumption that VANET model and all possible events already exist in the in the vehicles OBUs. Detection aims to detect Sybil Nodes	• Use line of sight sensors for detection and verification. • Assume each node has a VANET model. • No validations or performance test is conducted
Raya *et al*., [33]	Stand-Alone	EC	• Anomaly Detection, the average behaviour is the normal model and any node deviate from the average behaviour considered anomalies. Kullback-Leibler distance and Key-Means clustering are used.	• Can wrongly accuse innocent nodes and drop important safety messages. • No validations or performance test is conducted
Schmidt at al., [20] VEBAS	Cooperative	EC	• Build reputation through vehicle behaviours evaluation modules, Each module consist of several sensors. A trusted value calculated based on the output of the modules. Trusted value is assigned to each vehicles in the transpiration ranges.	• Reputation system is not efficient for VANET due to its characteristics. • Trusted node could misbehave for selfishness before its trusted value is modified. • No validations or performance test is conducted
Ghosh *et al*., [31]	Stand-Alone	EC	• Compare actual vehicle trajectories with a model of expected trajectories created by Markovian transition probability matrix. If the alert true then the driver crash modulated trajectories flow free flow model.	• Detect the misbehaviour after vehicles reached event locations is not sufficient for safety, it demands detecting the events before vehicles reach event location.
Ruj *et al*., in [14]	Stand-Alone	DC	• Vehicles that send safety message will be monitored and compared to expected behavioural model if such events are actually happened.	• No validations or performance test is conducted. • Position verification need more mature approach rather than using sender and receiver time.
Yang *et al*., in [17]	Cooperative	EC	• A combination of state automata, supervision, and security log to record the behavioural characteristics of the target vehicle. If a node violated the established policies, then it will be reported to Department of Transportations (DoT) • Detection will be performed in centralized location such as DoT.	• Cooperation detection is not valid for ephemeral networks. As the communication will last for few seconds. As no time to maintain secure log for each node. • Communications overhead will be common during exchange secure log of each vehicle. • No validations or performance test is conducted.

Misbehavior detection can be also categorized based on their detection approaches into cooperative detection type or stand-alone detection type. In cooperative type to detect an attacker a misbehavior in one vehicles need collaboration with other misbehavior detection installed on other vehicles. Whereas stand-alone mechanisms type detect the misbehavior based on its collected data and did not affected by other vehicles detection mechanisms. Although, stand-alone is preferable from security stand view, it can produce inaccurate results especially when the vehicles don’t have enough information to evaluate the presence of misbehavior. On the other hand, cooperation mechanisms can give more accurate results than stand-alone approaches but many security threats are possible. In addition, communication and computational overhead can be the bottleneck of these approaches. An idea to implement both type in one system stand-alone for safety applications and cooperation for other applications hence they are delay tolerant. However, more work is needed to enhance their security and efficiency.

Reactive security countermeasures which include Entity-Centric and Data-Centric approaches have been studied in a smaller scale [29]. We emphasis that more work is needed to complete proactive security countermeasures with a data-trust countermeasures. As shown in Tables 1 and 2 existing misbehavior detections approaches either incomplete or insufficient for VANET expected applications. Table 2 shows that most propose models are Entity-Centric whereas Data-Centric can be the second part of the solution. According to Rens *et al.*, [55] no single mechanisms can address all forms of misbehavior. The combination between the mechanisms is highly recommended since they use the same knowledge-base for detecting the incorrect data.

Table 2 Summary of the covered requirements in existing misbehavior detection approaches

MDS	Authentication	Privacy	Position Verification	Time Verification	Movement Analysis	Application Context
Golle *et al* [26]	Assume Short-Period Public/Private Keys	Assume attacker cannot link data over longer time periods	Assume Physical Sensor detect the neighbours.	Assume synchronized times	Not maintained	General - Set of all possible events
Raya *et al*., [33]	PKI/Certificate Authority	Not maintained	Assume Position is correct Not maintained	Assume time is synchronized through GPS	Kullback-Leibler distance	PCN
Schmidt at al., [20] VEBAS	Assume ECDSA-256 Signature	Not maintained	Redundant Sensors such as radar, lidar and road map	Not maintained	Speed Profile	General – Reputation Based on the previous behaviours of the nodes.
Ghosh *et al*., [31]	Not maintained		Not maintained	Not maintained	Hidden Markov Model	PCN
Ruj *et al*., in [14]	Public Keys Infrastructure (PKI)	Pseudonymous Keys	The difference between sending and receiving time and light speed	Not maintained	assumed	PCN, EEBL, RHCN, RFN, SVA, CVW, CL, EVA
Yang *et al*., in [17]	RSU-Ranom Key generation and OBU random key generation (Check-Token)	Not maintained	Not maintained	Assume time is synchronized through GPS	Not maintained	Accountability and provide evidence in secure logs.

■8.0 CONCLUSION

Misbehavior detection and data verification in VANET are essential for implementing safety and traffic efficiency applications. In this paper, we reviewed and discussed the existing approaches for misbehavior detections with respects to different assumptions. The significance of detecting malicious data in VANET are described with identifying the challenges faced the implementation.

Finally, the detection approaches are categorized based on their objectives into two categories: Entity-Centric or Data-Centric approaches. Each category is discussed and analyzed. We are currently studying the misbehavior detection in broader scope. The aim is to generalize the detection mechanisms to cover wide range of VANET applications.

Acknowledgement

The authors would like to express their appreciation to Ministry of Education (MOE) and Universiti Teknologi Malaysia for supporting this research under Research University Grant (RUG) vote 06H03.

References

[1] Raya, M., *et al*. 2008. On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.

[2] Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Resource Manager. IEEE Std 1609.1-2006, 2006. 1–71.

[3] Administration, N.H.T.S. Vehicle Safety Communications Project Task 3 Final Report, Identify Intelligent Vehicle Safety Applications Enabled by Dsrc. US Department of Transportation. Technical Report DOT HS 809 859 2005.(Technical Report DOT HS 809 859 2005).

[4] Consortium, C.C.C., Car 2 Car Communication Consortium Manifesto. Http://car-to-car.org/index.php?id=31.

[5] Al-Sultan, S., *et al*. 2014. A Comprehensive Survey on Vehicular Ad Hoc Network. *Journal of Network and Computer Applications*. 37(0): 380–392.

[6] Hartenstein, H. and K.P. Laberteaux. 2008. A Tutorial Survey on Vehicular Ad Hoc Networks. *Communications Magazine, IEEE.* 46(6): 164–171.

[7] Xiaodong, L., *et al*. 2008. Security in Vehicular Ad Hoc Networks. *Communications Magazine, IEEE.* 46(4): 88–95.

[8] Raya, M., P. Papadimitratos, and J. P. Hubaux. 2006. SECURING Vehicular Communications. *Wireless Communications, IEEE.* 13(5): 8–15.

[9] Hubaux, J.-P., S. Capkun, and J. Luo. 2004. The Security and Privacy of Smart Vehicles. *IEEE Security & Privacy Magazine, 2 (LCA-ARTICLE-2004-007).* 49–55.

[10] Zeadally, S., *et al*. 2012.Vehicular ad Hoc Networks (VANETS): Status, Results, and Challenges. *Telecommunication Systems*. 50(4): 217–241.

[11] Nai-Wei, L. and T. Hsiao-Chien. 2007. Illusion Attack on VANET Applications-A Message Plausibility Problem. In Globecom Workshops, IEEE.

[12] Kounga, G., T. Walter, and S. Lachmund. 2009. Proving Reliability of Anonymous Information in VANETs. *Vehicular Technology, IEEE Transactions on.* 58(6): 2977–2989.

[13] Ghosh, M., *et al*. 2010. Detecting Misbehaviors in VANET with Integrated Root-cause Analysis. *Ad Hoc Network*s. 8(7): 778–790.

[14] Ruj, S., *et al*. 2011. On Data-centric Misbehavior Detection in VANETs. in Vehicular Technology Conference (VTC Fall), 2011 IEEE.

[15] Muriel, M., A. Busson, and V. Veque. 2009. Performance Evaluation of VANET Under Realistic Vehicular Traffic Assumption. Traffic and Granular Flow '07, ed. C. AppertRolland, *et al*. 739–744.

[16] Raya, M., *et al*. 2007. Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. Selected Areas in Communications. *IEEE Journal on.* 25(8): 1557–1568.

[17] Samara, G., W.A. Al-Salihy, and R. Sures. 2010. Security issues And Challenges of Vehicular Ad Hoc Networks (vanet). In New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on. IEEE.

[18] Yang, X., *et al*. 2004. A Vehicle-to-vehicle Communication Protocol For Cooperative Collision Warning. In Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on. IEEE.

[19] Thompson, J. P. and C. D. Wang. 1997. Apparatus and Method for Motion Detection and Tracking of Objects in a Region for Collision Avoidance Utilizing A Real-time Adaptive Probabilistic Neural Network. Google Patents.

[20] Gongjun, Y., S. Olariu, and M. C. Weigle. 2009. Providing Location Security in Vehicular Ad Hoc Networks. *Wireless Communications.* IEEE, 16(6): 48–55.

[21] El Defrawy, K. and G. Tsudik. 2011. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs. *Mobile Computing, IEEE Transactions on*. 10(9): 1345–1358.

[22] Leinmuller, T., E. Schoch, and F. Kargl. 2006. Position Verification Approaches for Vehicular Ad Hoc Networks. *Wireless Communications, IEEE*. 13(5): 16–21.

[23] Drawil, N. M., H. M. Amar, and O. A. Basir, GPS Localization Accuracy Classification: A Context-Based Approach. *Intelligent Transportation Systems, IEEE Transactions on.* 2013. 14(1): 262–273.

[24] Yang, T., *et al*. 2013, MisDis: An Efficent Misbehavior Discovering Method Based on Accountability and State Machine in VANET, in Web Technologies and Applications, Y. Ishikawa, *et al*. Editors. Springer Berlin Heidelberg. 583–594.

[25] Yu, B., C.Z. Xu, and B. Xiao. 2013. Detecting Sybil Attacks in VANETs. *Journal of Parallel and Distributed Computing.* 73(6): 746–756.

[26] Bibhu, V., *et al*. 2012. Performance Analysis of Black Hole Attack in VANET. *International Journal of Computer Network and Information Security (IJCNIS).* 4(11): 47.

[27] Yih-Chun, H., A. Perrig, and D. B. Johnson. 2006. Wormhole Attacks in Wireless Networks. Selected Areas in Communications, IEEE Journal on. 24(2): 370–380.

[28] Kakkasageri, M. S. and S. S. Manvi. 2014. Information Management in Vehicular Ad Hoc Networks: A Review. *Journal of Network and Computer Applications*. 39: 334–350.

[29] Karagiannis, G., *et al*. 2011. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *Communications Surveys & Tutorials, IEEE.* 13(4): 584–616.

[30] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. IEEE Std 1609.2-2006, 2006. 0_1-105.

[31] Qianhong, W., J. Domingo-Ferrer, and U. Gonzalez-Nicolas. 2010. Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications. *Vehicular Technology, IEEE Transactions on.* 59(2): 559–573.

[32] Daza, V., *et al*. 2009. Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks. Vehicular Technology, IEEE Transactions on. 58(4): 1876–1886.

[33] Douceur, J. 2002. The Sybil Attack, in Peer-to-Peer Systems, P. Druschel, F. Kaashoek, and A. Rowstron, Editors. Springer Berlin Heidelberg. 251–260.

[34] Biswas, S., M.M. Haque, and J. Misic. 2010. Privacy and Anonymity in VANETs: A Contemporary Study. *Ad Hoc & Sensor Wireless Networks.* 10(2-3): 177–192.

[35] Amro, B., Y. Saygin, and A. Levi. 2013. Enhancing Privacy in Collaborative Traffic-Monitoring Systems Using Autonomous Location Update. *Iet Intelligent Transport Systems.* 7(4): 388–395.

[36] Chim, T.W., *et al*. 2014. VSPN: VANET-Based Secure and Privacy-Preserving Navigation. *Ieee Transactions on Computer*s. 63(2): 510–524.

[37] Li, J.S. and K.H. Liu. 2013. A Lightweight Identity Authentication Protocol for Vehicular Networks. *Telecommunication Systems*. 53(4): 425–438.

[38] Ganan, C., *et al*. 2014. PPREM: Privacy Preserving Revocation Mechanism for Vehicular Ad Hoc Networks. *Computer Standards & Interfaces.* 36(3): 513–523.

[39] Ganan, C., *et al*. 2013. COACH: Collaborative Certificate Status Checking Mechanism for VANETs. *Journal of Network and Computer Applications.* 36(5): 1337–1351.

[40] Hussain, R., *et al*. 2013. Privacy-Aware Route Tracing and Revocation Games in VANET-based Clouds. 2013 Ieee 9th International Conference on Wireless and Mobile Computing, Networking and Communications (Wimob). 730–735.

[41] Mikki, M., Y.M. Mansour, and K. Yim. 2013. Privacy Preserving Secure Communication Protocol for Vehicular Ad Hoc Networks. 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (Imis 2013). 188–195.

[42] Taha, S. and X.M. Shen. 2013. A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-Based VANETs. *Ieee Transactions on Intelligent Transportation Systems.* 14(4): 1665–1680.

[43] Ying, B. D., D. Makrakis, and H. T. Mouftah. 2013. Privacy Preserving Broadcast Message Authentication Protocol for VANETs. *Journal of Network and Computer Applications*. 36(5): 1352–1364.

[44] Zhu, H., *et al*. 2013. PPAS: Privacy Protection Authentication Scheme for VANET. *Cluster Computing.* 16(4): 873–886.

[45] Zhuo, X. J., *et al*. 2009. Removal of Misbehaving Insiders in Anonymous VANETs. Mswim09. Proceedings of the 12th Acm International Conference on Modeling, Analysis, and Systems. 106–115.

[46] Dietzel, S., *et al*. 2013. Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols. *Ieee Transactions on Vehicular Technology*. 62(4): 1505–1518.

[47] Golle, P., D. Greene, and J. Staddon. 2004. Detecting and Correcting Malicious Data in VANETs. In Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks. ACM: Philadelphia, PA, USA. 29–37.

[48] Harit, S. K., G. Singh, and N. Tyagi. 2012. Fox-Hole Model for Data-centric Misbehaviour Detection in VANETs. 2012 Third International Conference on Computer and Communication Technology (Iccct). 271–277.

[49] Lo, N.W. and H.C. Tsai. 2007. Illusion attack on VANET Applications-A Message Plausibility Problem. 2007 Ieee Globecom Workshops, Proceedings. 69–76.

[50] Ghosh, M., *et al*. 2009. Misbehavior Detection Scheme with Integrated Root Cause Detection in VANET. Sixth Acm International Workshop on Vehicular Inter-Networking-Vanet 2009. 123–124.

[51] Burmester, M., E. Magkos, and V. Chrissikopoulos. 2008. Strengthening Privacy Protection in VANETs. 2008 4th Ieee International Conference on Wireless and Mobile Computing, Networking and Communications (Wimob). 508–513.

[52] Schmidt, R. K., *et al*. 2008. Vehicle Behavior Analysis to Enhance Security In Vanets. In Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008).

[53] Kim, T.H.-J., *et al*. 2010. Vanet Alert Endorsement Using Multi-source Filters. In Proceedings of the Seventh ACM International Workshop on VehiculAr InterNETworking. ACM.

[54] Haeberlen, A., P. Kouznetsov, and P. Druschel. 2007. PeerReview: Practical accountability for distributed systems. In ACM SIGOPS Operating Systems Review. ACM.

[55] Heijden, R.W.v.d. and F. Kargl. 2014. Open Issues in Differentiating Misbehavior and Anomalies for VANETs. In 2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication, FG-IVC 2014. Vehicular Lab, University of Luxembourg: Luxembourg City, Luxembourg. 24–26.