A Review on Data Falsification-Based attacks In Cooperative Intelligent Transportation Systems

Sultan Ahmed Almalki *alma6989@vandals.uidaho.edu*
Computer Science Department
University of Idaho
Moscow, ID, 83844, USA

Jia Song *jsong@uidaho.edu*
Computer Science Department
University of Idaho
Moscow, ID, 83844, USA

Abstract

Cooperative Intelligent Transportation System (cITS) is one of IoT applications whose purpose is to enhance drive safety and efficiency. Several components constitute cITS including vehicles, road side units and backend systems. Like many IoT applications and systems, cITSs are susceptible to a wide-range of intruding or misbehaving attacks that could be launched by attackers from inside or outside of the network. Once a vehicle is compromised, it can be used to launch several types of attacks against other vehicles and/or components of cITS. They can also be used to send false information and messages to the neighboring vehicles, causing severe complications such as traffic congestions and accidents. Such attacks impede the momentum of the integration of cITS technology with existing infrastructure. In this paper, a comprehensive and deep analysis of the state-of-the-art solutions in intrusion and misbehavior detection for cITS have been conducted. This paper mainly focuses on the data falsification-based attacks that manipulate the mobility data and messages shared with the neighboring vehicles as it is more challenging and difficult to identify and mitigate. The paper can be of great use for research community to explore more opportunities and new avenues and propose more robust and effective security solutions that protect the potential applications in cITSs.

Keywords: Cooperative Intelligent Transportation Systems, Internet of Things, Intrusion Detection Systems, Misbehavior Detection Systems, Smart Car.

1. INTRODUCTION

Although the Internet of Things (IoT) technology plays a crucial rule in facilitating daily life and business, they pose several security challenges and concerns as well. The heterogeneity, internet accessibility and the enormous number of connected devices in IoT render applying traditional security measurements ineffective [1]. Although IoT devices vary from each other in several aspects such as functionality, computational capability, software specifications, and network connectivity, they need to work cooperatively to achieve a shared task [2]. As such a security breach to any of those devices can affect the entire system and hinder it from delivering the required mission. Several security countermeasures have been proposed to protect IoT systems which can be categorized into proactive and reactive measures. The proactive measures, also called preventive measures, try to prevent the attacks by protecting data and communications by means of cryptography and authentication [3]. Although preventive measures can prevent attackers from targeting data and information of other nodes, they are unable to stop a faulty or compromised node from sharing manipulated and tampered information with the other nodes [4]. On the other hand, the reactive measures aim to detect the attacks and/or mitigate the failure that they might cause. Intrusion detection is an example of reactive measures that identify the presence of suspicious activities and determines which devices have been compromised.

Smart vehicles, also called Cooperative Intelligent Transportation Systems (cITS), are one of IoT applications whose purpose is to improve road safety and traffic efficiency [4]. In cITS, the vehicles within a specific range become connected to one network, through which the data and information are exchanged between those vehicles. This has increased the performance, effectiveness and processes efficiency and maximized the productivity of these systems. However, such connectivity comes at the cost of several threats. These threat target could be categorized into threats system and threats against data [23]. While the former tries to disable or disrupt the function of one or more components in the vehicle's navigation system such as On-Board Unit, the later tries to corrupt, falsify, and/or manipulate the mobility data exchanged between the neighboring vehicles. These threats could come in the form of malware attacks or human crafted and organized attacks.

When connected to one network, vehicles in cITS become vulnerable to many threats that compromise the confidentiality, integrity, and availability of the data that they exchange [5]. To thwart such threats, several Intrusion Detection Systems (IDS) and Misbehavior Detection Systems (MDS) solutions have been proposed by the extant research. Nevertheless, these solutions assume that the information (data) shared between the nodes (vehicles) is reliable. Attackers could compromise such nodes, exploit and manipulate the information they share with other nodes. That is, a legitimate vehicle could be hijacked by attackers or infected by malware for the purpose of falsifying its data. The compromised vehicle will then share the false information with the other vehicles and make them react to false events and/or change their security parameters in a way that triggers vulnerabilities, through which the attackers can penetrate into the cITS system. Therefore, relying on such compromised information to build detection models adversely affects the accuracy of those solutions. Although some studies tried to address this issue, they have built their solutions based on the assumption that the attackers are able to compromise only a limited number of vehicles, which is not realistic. With the advanced attack strategies like botnets, attackers can hijack many nodes in the network and create a majority honest that can deceive the trustworthiness scheme that those detection solutions have proposed. As such these solutions inherit several limitations that need to be addressed. To overcome these challenges, it is necessary to identify the limitations of the existing research. To this end, this paper aims at studying the existing application of IDS in cITS in order to find their limitations and weaknesses and provide the research community with a set of potential research directions. The paper starts with an overview of cITSs as part of IoT technology. The threats and challenges are then elaborated with a description of the data and messages susceptible to this type of attack. The related state-of-the-arts were then discussed and analyzed with the emphasis on the limitations of those solutions. Based on the analysis, insights and recommendations for future works were suggested.

The rest of this paper is organized as follows. Section 2 gives a general background of cITS, its applications and security concerns. The state-of-the-art solutions are discussed in detail in Section 3, and the comparison between different detection approaches is provided at the end of the section. Experimental results are shown and analyzed in Section 4. Lessons learned from the literature review are elaborated in Section 5. In Section 6, research directions and suggestions for future works are discussed. Section 7 concludes the paper.

2. BACKGROUND

cITSs are designed to support the autonomous vehicles and improve road safety and traffic efficiency [4]. To achieve such a goal, several hardware and software components work collaboratively to observe, collect and analyze related data exchanged between the different components of cITS. Following subsections elaborate about such components and the methods they use to communicate with each other, the threats that these systems might encounter and the detection and prevention approaches used to thwart such threats.

2.1 Components of Cooperative Intelligent Transportation Systems

Three main components constitute cITS, namely vehicles, backend systems and road side units (RSUs). The vehicles are equipped with a set of sensors that collect traffic-related data from the surrounding environment, such as velocity, acceleration, GPS, and density. The collected data carry information about road conditions and traffic situation on the vicinity of the vehicle. Backend systems are used to store and analyze the traffic data and send notifications/alerts to vehicles and/or road service providers. RSU is a backbone that connects vehicles on the road section with the backend systems [4]. The purpose of RSUs is to connect the vehicles with some backend systems like traffic control. These components work cooperatively and exchange different types of information. The context information includes, but is not limited to, lane change warnings, accident reporting, and cooperative adaptive cruise control. As such type of information is relevant to all vehicles in the same vicinity, point to point communication is not an efficient way to exchange this information among neighboring vehicles. Therefore, cITS utilizes the broadcasting approach to share the context data among different nodes [4].

2.2 cITS Context Information

cITS utilizes one of two standards as an information-sharing mechanism, namely the European standard [6] and the American standard [7] .

The cITS context information in the European standard consists of two messages, the Cooperative Awareness Message (CAM) and the Decentralized Environmental Notification Message (DENM). While CAMs are sent periodically, DENMs are event-driven that are only sent when an event has occurred. The CAM consists of information about the vehicles like position, size, speed and steering wheel angle. In contrast, DENM contains information about a certain event like a lane changing and sudden braking.

On the other hand, cITS context information in the American standard combines CAM and DENM into Basic Safety Message (BSM). BSM will be used when discussing the combination of CAM and DENM messages. The first part of BSM, as well as CAM in the European standard, carries information about position, heading, speed, acceleration, steering wheel angle, vehicle role, vehicle size and status of vehicle light [4]. Unlike the first part of BSM that is included with in all BSM messages, the second part of BSM (which corresponds to DENM in the European standard) is included only when an event happens, to carry information about such an event.

2.3 Threats Against cITS

As cITSs work in a highly dynamic and harsh environment, collecting accurate and sufficient context information is challenging [8]. As these messages are broadcasted among the vehicles within the same vicinity, information confidentiality is not the focus in this aspect. Instead, data integrity and authenticity are what should be guaranteed in such systems [4]. Many of the attacks that target smart vehicles come from adversaries who use sophisticated strategies to carry out sustainable attacks like malware and botnets [5, 9]. Such attacks could be originated from outside or inside of the network. While attacks from outside can be easily detected and thwarted at the perimeters of the network, insider attacks come from inside of the network and are usually carried out by legitimate, yet compromised vehicles.

Threats against cITS could be categorized as intrusion threats and misbehaving threats. Intrusion threats are mainly launched by intruders from outside of the network such as in replay attack, jamming attack, Sybil attack, and false data injection attacks. In jamming attack, the attacker sends a burst of messages to a specific vehicle causing a disruption in the communication between the targeted vehicle and other vehicles in the network. Replay attacks intercept the messages exchanged between the vehicles and later re-transmit them for the purpose of impersonation and/or stealing the identity. In Sybil attack, the attacker uses multiple identities in order to deceive other vehicles by reporting a fake road congestion. False data injection is another type of attack, in which attacker sends false information about current traffic situation on the road for the purpose of disrupting the traffic or triggering a congestion.

Misbehavior attacks, on the other hand, are launched from the inside of the network by hijacking a legitimate vehicle and using it to manipulate and share false information among the neighboring vehicles. That is, BSM of the compromised vehicle can be manipulated by attackers to include false information and share it with the neighboring vehicles [10]. Such false information might trigger severe reactions like sudden braking, lane changing, and speed-limit exceeding which could lead to life-threatening situations. Therefore, protecting BSM messages against the misbehaving attacks is crucial to ensure cITS security and road safety.

2.4 Threat Countermeasures in cITS

Several studies have been devoted to counteracting attacks in cITS. These solutions are categorized into intrusion detection and misbehavior detection. The intrusion detection solution focuses on protecting the network against the attacks launched from the outside of the network. IDSs look for patterns related to known attacks like Sybil, Malware, and Dos attacks and raise alert when matching is found. They can also compare the incoming patterns with the patterns of normal applications and raise alert when the matching is not found. Unlike IDSs, the purpose of misbehavior detection systems (MDSs) in cITS is to find out whether the BSMs sent/received by nodes are correct. In addition, misbehavior detection protects the system by detecting attacks launched from the inside of the network. The problem with insider attacks is that the attacker uses legitimate yet compromised nodes to launch a chain of attacks against the network, which makes it less suspicious to traditional intrusion detection solutions [11]. Even though several solutions have been proposed to mitigate these attacks, some underlying assumptions like stationary context and majority honest used for designing these solutions are not suitable given the highly dynamic and ephemeral nature of cITS. Building data-driven detection models on such stationary assumption renders these solutions unaware of the change in the driving situation in the road section. Therefore, these solutions become out of date quickly.

3. LITERATURE REVIEW

To safeguard cITS, the security solutions need to detect the attacks first. As such, detection solutions are imperative to notify the defense system about the presence of attack. To detect intrusion and misbehavior attacks against cITS, several solutions have been proposed, most of which are data-driven that rely on different types of data collected during the normal operations and/or attacks to build the detection models. Using such data, several statistical, machine learning and artificial intelligence techniques have been utilized to model the normal and attack profiles and calculate the detection thresholds and parameters. In the following subsections, the studies related to intrusion detection as well as misbehavior detection in cITSs are discussed.

3.1 Intrusion Detection in cITS

As pointed out previously, IDS focuses on preventing the attacks launched by attackers from outside of the participating vehicles. These solutions try to identify specific types of attacks such as jamming, replay, and sybil attacks. They are normally applied either globally at the main location in the cITS system like RSUs or locally on the vehicle’s level. Like IDSs that work on traditional networks, intrusion detection system on cITSs can work cooperatively such that vehicles can share the knowledge about new and emerging threats among each other.

Aloqaily, et al. [12] proposed a cloud-based IDS for smart vehicles that guarantee user’s Quality of Service (QoS) and Quality of Experience (QoE). The vehicles are grouped into different clusters, and the vehicles in each cluster are connected to a cluster head whose purpose is to communicate with Trusted Third-Party entities, which act as mediators between service requestors and providers. The proposed IDS has three phases, namely traffic analysis, data reduction, and classification. In traffic analysis phase, the collected data are analyzed to identify the behavioral patterns and features. Irrelevant and insignificant features are then removed during the data reduction phase to reduce data dimensionality and prevent overfitting. The model is then built by training a deep learning classifier using the selected features. Deep Belief Networks was employed for data reduction and the Decision Tree for the classification. Dividing vehicles in a road section into clusters each with a cluster head increase the network homogeneity, which facilitate the identification of anomalous events and entities. However, dividing smart vehicles into clusters and appointing a cluster head for each cluster is challenging given the ephemeral nature of cITS networks. That is, cITS networks are highly dynamic, which renders the clustering approach ineffective as the rate of joining and leaving a particular cluster is very high. Moreover, the cluster head, as any other vehicle in the cluster has a short living time within the cluster, which makes it unreliable as a mediator between the cluster's vehicles and service provider.

To cope with the highly dynamic nature of cITS, a Trust-aware Collaborative Learning Automata-based IDS was proposed by Kumar and Chilamkurti [13]. The model integrates a Collaborative Trust Index (CTI) into a classification algorithm in order to cover as many types of attacks that target smart cITSs as possible. The CTI is a trustworthiness evaluation that each vehicle receives from the environment (the other vehicles in the surrounding). The proposed approach is adaptive as it employs a novel collaborative Learning Automata (LA) that makes decisions based on several parameters like density, mobility, and direction of motion that reflects the current state of the environment. The CTI is then determined for each process in the automaton. The automaton of each vehicle observes the activities carried out by other vehicles in its vicinity. However, the study assumes the completeness of information shared among neighboring vehicles. This does not hold for cITS systems as the vehicles communicate in a highly dynamic and harsh environment, which makes the communication between neighboring vehicles intermittent. Such sporadic causes a loss of context information. As such, the model could produce suboptimal accuracy when classifying the events as either legitimate or attacks.

To overcome the network instability and rapid topology change, Sedjelmaci and Senouci [14] proposed a secured clustering algorithm that takes into account the vehicle's mobility during cluster formation. Therefore, the clusters become more stable and each cluster head will be selected based on the vehicle's trust-level that can easily be determined in such a stable environment. By employing the clustering approach, communication overhead is reduced due to reducing the broadcasting, which in turn, decreases the data loss. The proposed model was tested on several attack types like selective forwarding, black hole, resource exhaustion, and Sybil attacks. Two levels of detection constitute the proposed solution, the Local IDS and Global IDS. Local IDS works on local nodes (vehicles) and monitors the neighboring vehicles. Global IDS, on the other hand, works on cluster head level and monitors the trustworthiness of cluster members. The decision is then taken globally at RSU level based on the Trust Level of each vehicle. However, the proposed model was built based on the assumption that the communication between vehicles within a certain cluster as well as across the clusters is stable, which might not be the case in the harsh environments similar to cITS networks.

The highly dynamic and intermittent connectivity of vehicular networks were investigated by Subba, et al. [15]. A game theory-based multi-layered IDS was proposed to detect attacks targeting vehicular networks. The solution relies on a set of pre-defined roles along with neural networks for classifying the traffic into either benign or malicious. The relationship between IDS and attacker was formulated as a non-cooperative game based on Nash Equilibrium. To guarantee to work on higher densities and improve the robustness of the IDS even with a small fraction of data, a distributed clustering approach was adopted to group the vehicles in the network into different stable clusters. However, the clustering approach is not suitable for the ephemeral nature of vehicular networks as the lifetime of these clusters is very short and unsuitable for neural networks-based classification as these classifiers become outdated very quickly.

A Privacy-Preserving Machine Learning-based Collaborative IDS for cITSs was proposed by Zhang and Zhu [16]. The model utilizes the knowledge-based, i.e. the attacks pattern database, of each vehicle to improve the accuracy of the IDSs in the other vehicles. Moreover, the model in each vehicle employs the labeled data of other nodes to boost the training data of its own. To preserve data privacy, the model utilizes the dynamic differential privacy to capture the privacy notation in the collaborative IDS and use it to build the dual variable perturbation that protects the privacy of the training data by perturbing the dual variable. However, the reliance on the labels acquired from the other nodes renders the entire IDS vulnerable to falsified labeling as the malicious vehicles might manipulate these labels, which adversely affects the validity of the knowledge-base of the other vehicles. In addition, sharing the entire knowledge-base among the vehicles in the network adds a massive overhead given the highly dynamic and ephemeral-nature of cITS networks. Such overhead might as well lead to loss of useful traffic data.

3.2 Misbehavior Detection In cITS

Unlike IDS, the misbehavior detection focuses on identifying the threats originated from the participation vehicles inside cITS. These threats come from several sources like hijacked, rogue, and/or faulty nodes. While hijacked and rogue vehicles disrupt cITSs operations intentionally, faulty nodes cause such disruption unintentionally. In addition, the faulty nodes might as well be the result of other types of threats like intrusion attacks. Misbehavior detection is further categorized into data-centric detection and node-centric detection [4]. The data-centric misbehavior detection observes the data and messages exchanged between the participating nodes and performs several checks to identify the false information and suspicious contents. The node-centric misbehavior detection monitors a vehicle within the cITS based on several aspects like the number of messages it sends in a certain time period and correctness of the message’s format. The following subsections elaborate more about data-centric and node-centric misbehavior detection in cITS .

3.2.1 Data-Centric Misbehavior Detection

As pointed out previously, data-centric misbehavior detection focuses on the data and messages exchanged among the neighboring vehicles in cITS. By utilizing the correlated packets from different sources, the newly received packet is vetted against several criteria like consistency and plausibility to determine its trustworthiness. Using the consistency check, for instance, the average of the previous speed readings recorded for a vehicle can be used to judge the newly reported speed value. Not only are readings from the same vehicle used to determine the consistency of the new information, but also those coming from the neighboring vehicles. One of the main characteristics of consistency-based detection is its limited reliance on domain knowledge, which makes it easy to design and implement [4]. Plausibility, on the other hand, employees a predefined model to verify whether the received message is in line with the underlying model. Vehicle’s speed, for instance, could be verified against the law of physics, which makes it impossible for a vehicle to travel at a speed of 1000 km/hour, which exceeds the upper limit of the known speed for a moving object.

Several models have been proposed for data-centric misbehavior detection in smart vehicles. In the study conducted by Hasrouny, et al. [17], a framework for the certificate revocation process within Vehicular Ad-Hoc Networks (VANETs) was proposed. The framework relies on the trustworthiness evaluation of the participating vehicles to identify and exclude the misbehaving vehicles from the network. Such trustworthiness is updated according to several trust metric values calculated based on the data received within BSM packets. However, the trust metric relies on the assessment of the neighboring vehicles that are assumed honest. This might not be necessarily true as a misbehaving vehicle can send false reports about its neighboring vehicles to reduce its trustworthiness level. In such a case, the trust metrics of an honest vehicle can be decreased, which allows the attackers to manipulate the context of the traffic situation within that vicinity.

As traffic density has an influence on several events and behavioral aspects of the vehicles, it can be used as a security indicator to assess the plausibility and consistency of the traffic information sent/received by the nodes within the cITS. As such, it is important to secure the traffic density computation. To address this problem, the study conducted by Zacharias and Fröschle [18] measured the local traffic density of vehicles in cITS using two independent sensors. The traffic density information is used as a security parameter to address the illusion attacks challenge when an attacker employs a ghost (hijacked) vehicle to send false information (event messages) using valid credentials and showing valid location information. These measurements are then combined and used to evaluate a certain traffic situation and detect misbehaving vehicles. The study calculated local traffic density as a ratio between the number of neighboring vehicles and the total distance between these vehicles. However, the study assumes that at least one of the two independent sensors remains intact and the attacker has no access to it, which does not hold for sophisticated attacks that can get hold of and manipulate all sensors.

To detect position falsification attacks, Singh, et al. [19] proposed a machine learning-based model that observes BSM and determine whether they contain false data or not. Two classifiers, Logistic Regression and Support Vector Machines are used to build the model. The Vehicular Reference Misbehavior Dataset is used to train the LR and SVM classifiers. After training the model offline, online testing is carried out by submitting the new messages into the model to decide whether they are falsified or not. However, the highly dynamic nature of the network topology in cITS and frequent vehicle disconnection may render it impractical to train a machine learning model.

CA-DC-MDS proposed by Ghaleb, et al. [9] is a multi-faceted context-aware misbehavior detection scheme for smart vehicles. The scheme utilizes the Spatio-temporal (this acronym is used in the literature to represent the combination of spatial and temporal) correlation of the consistency between the cooperative awareness messages to protect these messages against internal attacks. Dynamic thresholds are used as context references that reflect the non-stationary nature of such networks. These spatial and temporal contextual thresholds were calculated using both Particle and Kalman filters, respectively. However, the study assumes that the majority of the nodes (vehicles) are benign, which might not be realistic as attackers can exploit the compromised nodes to attack other nodes in a way similar to botnets.

In their study, Ghaleb, et al. [5] proposed the Hybrid and Multifaceted Context-aware Misbehavior Detection model to address the limitation of existing context-aware misbehavior detection which assumes stationary noise and ideal communication, which does not hold in the highly dynamic and harsh environments like cITS. The proposed model replaced the static plausibility and consistency thresholds with dynamic context references adaptable to the changes in the network topology. These context references are built online using several statistical techniques such as Kalman filter, Hampel filter, and Box and Whisker. However, the model was built on the premise that the majority of vehicles are honest, which does not hold in the case of botnet attacks that exploit the compromised vehicles to create a chain of rogue nodes to create a majority (of the compromised vehicles) in the neighborhood.

In another study, Ghaleb, et al. [20] proposed an ensemble-based misbehavior detection model that replaces the static thresholds of the context of driving situations used by the extant research into dynamic thresholds that are determined online. As such, the proposed model is able to cope with the dynamic nature of the network. Kalman and Hampel filters were used to spontaneously adjust these thresholds. The model was trained using the data coming from the statistical classifiers, context parameters, consistency, plausibility, and behavioral features. However, similar to the other studies, authors assume the majority are honest, which does not hold in case of massive attacks that used the botnet strategy to launch a chain of attacks.

3.2.2 Node-Centric Misbehavior Detection

Node-centric misbehavior detection assesses the vehicle based on its behavior and trustworthiness. For the behavioral aspect, the number of messages sent by the vehicle and the validity of the format of these messages are observed. The trustworthiness, on the other hand, relies on a vehicle’s reputation and the voting to determine whether the vehicle is misbehaving. Voting assumes the majority are honest. In the study carried out by Zhang, et al. [21], the trustworthiness was employed to evaluate the vehicle and determine whether it was misbehaving. Such evaluation was carried out in the fog layer of cITS based on both intrinsic and extrinsic factors. Intrinsic factors rely on the information collected about the vehicle in question like the number of accidents, engine statistics, mileage, and velocity. Extrinsic factors rely on the information about the environment in the vicinity of the vehicle like a roadmap, trajectory, and proximity to other vehicles. Principal Component Analysis is utilized to analyze these factors and calculate the trustworthiness of the vehicle. However, relying on the intrinsic factors might not be suitable in case of advanced attacks that manipulate the vehicle's own data. Those advanced attacks can also manipulate the context surrounding the vehicle by creating a collaborative illusion attack that falsifies driving situation information exchanged between the neighboring vehicles.

The study conducted by Zhang, et al. [22] proposed a solution that incorporates the data trust model and vehicle trust model to discover the falsified data and evaluate the vehicle's trustworthiness. Support Vector Machines and Dempster Shafer Theory are the main components of the model. Support Vector Machines is used to evaluate the message contents, vehicle's attributes, and credibility based on its data propagation behavior. Dempster Shafer Theory is then used to combine different multiple trust assessments about a certain vehicle, based on which the final trust value is calculated. However, the model is built based on the premise that the mobility information messages and vehicle's attributes are stationary. Such an assumption is not suitable for ephemeral environments like cITSs, in which the network is highly dynamic and the communication between vehicles is not necessarily reliable, which in turn, invalidates the model within a short period.

Fuzzy Misbehavior Detection System was proposed by Amirat, et al. [23] to identify selective forwarding attackers who behave normally and only drop the messages coming from the neighboring vehicles. It employs fuzzy clustering to categorize normal and attacker nodes into different clusters. To build these clusters, Fuzzy C-Means clustering algorithm was utilized. Membership to either cluster is determined by a threshold that indicates to which was empirically defined. However, relying on a static threshold to identify the membership degree is not suitable for cITS due to the dynamic nature of vehicles.

The selective flow sampling and entropy method was used by Sharshembiev, et al. [24] to detect the misbehaving vehicles in real-time. The purpose of the selective sampling was to extract the maximum amount of information from a small set of packets of a particular flow. This is helpful for real-time detection where the collected data are limited. The entropy was then used to calculate the change in the data collected previously. The study observed that with a small fraction of flows, a lot of information could be perceived and used for accurate misbehavior detection. However, entropy calculation might not be accurate in light of the number of flows available at the real-time deployment, which adversely affects the accuracy of the proposed model.

The major drawback of node-centric is the reliance on the behavioral aspects of the nodes (vehicles) and ignoring the semantical aspect of the data sent and/or received by these nodes. Moreover, the premise of majority honest that node-centric uses to calculate the trustworthiness of the nodes is not always true as some advanced attacks like those launched by botnets start by creating a majority in favor of the compromised vehicles. In addition, evaluating such trustworthiness is challenging due to the ephemeral nature of the cITS particularly at the initialization stage. Furthermore, the reputation mechanism used by node-centric misbehavior detection solutions is susceptible to sudden misbehaving or faulty vehicles [4].

3.3 Comparing IDS and MDS Solutions In cITSs

Table 1 summarizes some of the existing solutions using Intrusion Detection systems while Table 2 compares multiple Misbehavior Detection solutions in cITSs. It can be seen that most of these solutions assume that the data shared between the vehicles are reliable. However, attackers could compromise such vehicles, exploit and manipulate the information they share with other nodes as pointed out in Section 1.

Paper	Research Problem	Solution	Limitation(s)
[12]	Maintaining the integrity and authenticity of data exchanged between vehicles are not suitable for cITS as they are resource demanding, hence not suitable for QoS and QoE.	• A Cloud-based IDS, which communicates with several cluster heads. • Cluster heads are connected to a group of vehicles in the network.	• Dividing vehicles into clusters is not suitable for highly dynamic and ephemeral networks like cITS. • The cluster head, in cITS has a short living time within the cluster, which makes it unreliable as a mediator between the cluster's vehicles and service provider.
[13]	Most of the existing solutions are attack-specific that focus on limited types of attacks.	Integrates a Collaborative Trust Index (CTI) into a classification algorithm in order to cover many types of attacks.	Assumes the availability of all information about the neighboring vehicles which is not suitable in cITS because of: • The intermittent communication between vehicles due to the high dynamicity and harsh environment. • Insufficient information gathered due to the ephemeral nature of cITS.
[14]	Existing IDS solutions overlook network instability and high dynamicity of the smart vehicular networks.	• A secured clustering algorithm that considers vehicle's mobility. • Two levels, local IDS (LIDS) and global IDS (GIDS) for cluster stability.	• It assumes a stable communication between within cluster and between clusters. • Not suitable for dynamic and harsh environments like cITS.
[15]	Lack of tradeoff between gathering sufficient information and preventing the overburdening of IDS's logging component with a high volume of unnecessary IDS traffic.	A multi-layered game theory-based neural network IDS with a distributed clustering: • Groups vehicles into different stable clusters, to improve the robustness of the IDS.	The clustering is not suitable because cluster's lifetime is very short and become outdated quickly.
[16]	Due to privacy-preserving concern, existing IDS solutions ignore the sharing of detection knowledge among neighboring vehicles.	Shares the knowledge-based of each vehicle with other vehicles while preserving the privacy of each vehicle.	• Labels received from other vehicles could be falsified. • Additional overhead.

TABLE 1: Existing Research in IDS for cITS.

Paper	Research Problem	Solution	Limitation
[17]	Maintaining only the trustworthy vehicles and remove the misbehaving ones is challenging	A Certificate revocation framework based on the trustworthiness evaluation using trust metric values calculated on the data received within BSM packets.	• Revocation of the certificate from honest vehicles • Creating majority dishonest that can be used to manipulate the context of traffic situation.
[18]	Using the environment information around host vehicle to validate the plausibility of the information sent by a particular vehicle is ineffective when the misbehaving vehicle provides valid location information.	• Using two (independent) sensors to observe the environment surrounding the vehicle. • If one sensor got attacked, the information of the other sensor stays intact.	• Assumes that at least one of the two independent sensors remains intact. • Attacker could hijack both sensors.
[19]	Guaranteeing the trustworthiness of the data in the presence of dishonest and misbehaving vehicles that share false information is hard.	Using machine learning identify falsified BSMs.	The dynamic network topology in cITS and intermittent communication makes it challenging to keep an up-to-date model.
[9]	Existing solutions assume that the context of driving situation is stationary, which contradicts the dynamic nature of cITSs.	• Uses dynamic thresholds as context references. • Context reference copes with non-stationary nature of the networks.	• The study assumes that the majority of the nodes (vehicles) are benign, • Compromised nodes can be used to compromise other nodes and create a majority dishonest.
[5]	Existing context-aware misbehavior detection solutions assume stationary noise and ideal communication, which does not hold in the highly dynamic and harsh environments.	Dynamic plausibility and consistency thresholds are built online to be adaptable to the changes in the network topology.	Assumes majority honest, which does not hold in the case of botnet attacks that exploit the compromised vehicles to a majority of the compromised vehicles.
[20]	Existing research uses static thresholds for the context of driving situations.	Multi-faceted dynamic context thresholds that adapt to the change in the driving situation.	Assumes the majority are honest, which does not hold in case of massive attacks that used the botnet strategy to launch a chain of attacks.
[22]	Existing reputation based misbehavior detection solutions assume that vehicles with high reputation are always trustworthy, which might not be accurate once they got compromised.	Incorporates the data trust model and vehicle trust model to discover the falsified data and evaluate the vehicle’s trustworthiness.	• Not suitable for highly dynamic network. • The communication between vehicles is unreliable
[23]	Detecting misbehaving vehicles that behave normally and only carry out less suspicious actions like dropping some packets is challenging.	• Categorizes normal and attacker nodes into different clusters. • Identifies selective forwarding attackers who behave normally.	Relies on a static threshold to identify the membership degree, which is not suitable for cITS due to the dynamic nature of nodes (vehicles).
[24]	Existing solutions overlook the fact that the data acquired about driving situation at real-time are not sufficient, which degrades the detection rate and increases the false alarms.	Integrating a selective flow sampling with entropy to extract the maximum amount of information from a small set of packets of a particular flow and calculate the change in the data collected previously.	Entropy calculation might not be accurate due to limited number of flows available at the real-time deployment.

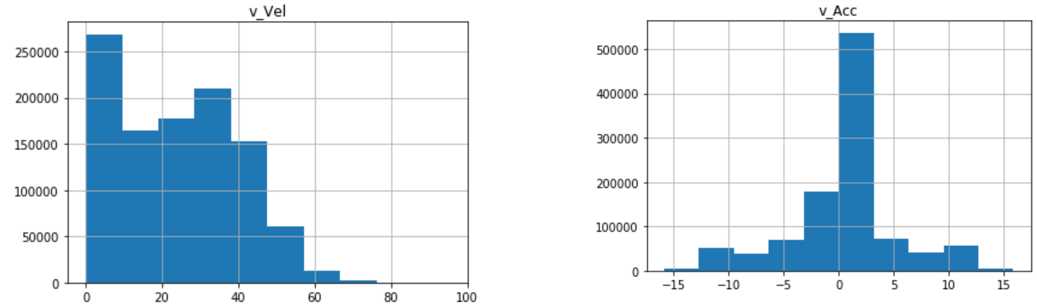
TABLE 2: Exiting research in MDS for cITS.

4. EXPERIMENTS

To examine the viability of using traffic mobility information data for misbehavior detection, the misbehavior detection model using the Artificial Neural Networks (ANN) proposed by Ghaleb, et al. [10] is applied in this paper. In the experiment, Next Generation Simulation Vehicle Trajectories (NGSIM) dataset was used. The NGSIM dataset contains detailed vehicle trajectory data on southbound US 101 and Lankershim Boulevard in Los Angeles, CA, eastbound I-80 in Emeryville, CA and Peachtree Street in Atlanta, Georgia [24]. Data in NGSIM were collected through a network of synchronized digital video cameras. NGVIDEO, a customized software application developed for the NGSIM program, transcribed the vehicle trajectory data from the video. This vehicle trajectory data provides the precise location of each vehicle within the study area every one-tenth of a second, resulting in detailed lane positions and locations relative to other vehicles.

To carry out the experiments, the data has been divided into two datasets, ground truth and test data. The ground truth has been used train the ANN classifier. The test dataset has further been divided into two subsets T1 and T2. T1 was kept intact. The falsified information was injected into T2. The experiments have been carried out using a machine with Intel(R) Core(TM) i7-4790 CPU @ 3.60 GHz and 16 GB RAM. The model components and results analysis were implemented using Python libraries, including Sklearn, Pandas, and Numpy.

Similar to Ghaleb, et al. [10], in our implementation only some the values in following attributes (velocity [v_Vel], acceleration [v_Acc]) have been falsified to make it difficult for the detection model to distinguish between the truth data and falsified ones. Before building the misbehavior detection model, exploratory experiments have been carried out to visualize some aspect of the NGSIM dataset. We have chosen two attributes, namely velocity (v_Vel) and acceleration (v_Acc) and built the histogram to get an idea about the data distribution of these attributes. Figure 1 shows the histogram of both v_Vel and v_Acc. Data distribution of both attributes shows a kind of tendency towards the normal distribution (especially v_Acc), which indicates that it is applicable to use it to distinguish whether the incoming data are falsified. The Figure 1 (a) shows that the velocity ranges between 0 and 80 km/hour. Similarly, Figure 1 (b) shows that the acceleration ranges between -15 and 15 and most of the cases fall between 0 and 5. Artificial Neural Networks (ANN) was used to build the detection model. The model was trained using the ground truth dataset.



(a) Velocity

(b) Acceleration

FIGURE 1: Histogram of (a) v_vel and (b) v_Acc attributes in NGSIM dataset.

The model was built in two phases, training and testing. During the training phase, the training dataset was used to build the ANN classifier using the attributes in NGSIM as input features. The ANN classifier consists of three layers, input, hidden and output. The input layer contains number of units (neurons) corresponding the attributes in the dataset. Output layer contains of two units (normal and misbehaving). The number of units in the hidden layer was adjusted (optimized) during the training phase so that the classifier provides the best possible accuracy. Then the accuracy of the model was tested using both T1 and T2 datasets during the testing phase. The performance of the model has been measured using four metrics, namely accuracy (ACC), detection rate (DR), false positive rate (FPR) and F1 measure (F). To compare the performance of the ANN-based misbehavior detection model, we implemented the SVM-based model proposed by So, et al. [25] and the LR-Based model proposed Singh, et al. [19] using the same training and testing datasets. In addition, the namely Support Vector Machines (SVM) and Logistic Regression (LR) have been trained and tested using the same training and testing datasets.

From the results shown in Figure 2, SVM outperformed both ANN and LR in all performance metrics. In particular, SVM's accuracy, detection rate and F1 were higher than those of ANN and LR. This is attributed to the kernel approach utilized by SVM (in the experiments the kernel used was RBF) that increases the ability of SVM to generalize well. Therefore, the model was able to detect the misbehaving vehicles more accurately. The low accuracy and high false positive rate of ANN and LR indicates that the data/features ratio play a vital role when building the classifiers. If the ratio is high, the model becomes biased due to the high number of instances with low number of features (attributes) as it is the case in NGSIM, which hinders the ability of ANN and LR model to generalize well. In contrast, the kernel approach employed by SVM transforms the data into higher order generates more features, which allows the model to perceive more intrinsic characteristics of the data and easily distinguish between the normal and anomalous boundaries more accurately.

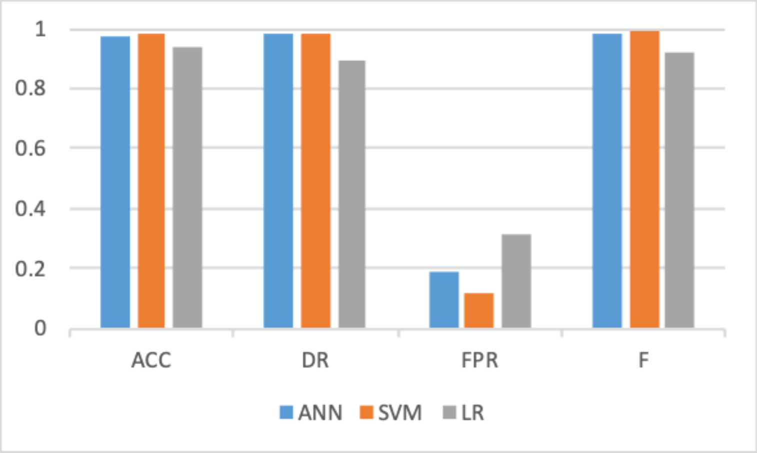


FIGURE 2: Performance comparison of ANN, SVM and LR using ACC, DR, FPR and F1 measure.

Although the accuracy of detecting the misbehaving nodes in cITS was relatively high when using the three algorithms, i.e. ANN, SVM, LR, the rate of false alarms was relatively high as well. This is due to the evasion approaches that attackers employ to carry out advanced and sophisticated misbehaving attacks, which makes it difficult for these machine learning algorithms to distinguish between the normal and misbehaving nodes. That is, misbehaving attacks are launched from within legitimate vehicles that have been previously compromised and hijacked by the attackers using several tools like malware and/or botnets. With such a strategy, the attackers can tailor evasive attacks that look like normal behavior by manipulating the mobility data exchanged within the network and deceive the other vehicles to change the boundaries of their normal profile to include the suspicious behavior. Consequently, these vehicles become unable to detect the misbehaving attacks that resemble the normal behavior and fall within the boundaries of the normal profile, which explains the high rate of the false alarms generated by the algorithms used in these studies. As such, it is necessary to count for these evasive benign-alike attacks to address the false alarms issue. In addition, the lowest false alarms rate was shown by the SVM thanks to the RBF kernel that allows the model to introspect the latent patterns in the data. These patterns facilitate the discrimination between the normal and suspicious behavior in the data.

5. LESSONS LEARNED

The aforementioned studies try to find discriminative patterns to distinguish the attack traffic from the normal one. Although such an approach is effective in detecting resource exhaustion and spoofing attacks, it is unable to detect the misbehaving nodes that share false information with the nodes in its vicinity. Such kind of misbehavior could be exploited by advanced attackers to manipulate the security thresholds and profiles. In addition, most of the studies assume that neither attack nor normal behaviors change, which does not hold as the IoT environment is dynamic. Therefore, such solutions suffer the concept drift, which invalidates the built defined profiles. Moreover, these solutions are not aware of the obfuscation techniques and strategies that sophisticated attackers and malicious software use to deceive the detection.

Based on the literature reviewed above, most of the existing IDSs and MDSs proposed for smart vehicles overlook the dynamic nature of the networks that these vehicles communicate with each other as well as the RSUs. These studies assume that the network is stationary, which is not realistic as the vehicles are always on the move and the lifetime of the connection is limited. Building security solutions on such assumption have a negative impact on the underlying thresholds and knowledge base that those models rely on for detection. Similarly, existing security solutions assume that the context of the driving situation is stationary, which is not true for cITSs as the context is stochastic due to the dynamic nature of such networks.

Communication reliability is another assumption that existing security solutions count on when building the detection models. However, the ephemeral nature and harsh environment that smart vehicles operate in make it challenging to collect noise-free and complete attack patterns. Therefore, the collected data might not be representative enough for building accurate detection solutions. Likewise, acquiring sufficient information from within the network in real-time is challenging as the attackers escalate the attacks gradually to divert attention and avoid the suspicion. In such a case, the complete attack trace might not be available until the attack comes to the end. To the best of our knowledge, no study has considered this attack attribute, which renders these solutions vulnerable to this type of attack.

Another limitation that existing solutions suffer from is the assumption of majority honest. The problem with this assumption is that it renders the security solutions susceptible to illusion attacks that employ a chain of compromised nodes (called botnets) to launch cascading attacks by employing the newly compromised vehicles to participate in this attack. This type of behavior creates majority dishonest, which invalidate the assumption of the majority honest that existing IDSs and MDSs have been built based on.

6. FUTURE WORK AND RESEARCH DIRECTIONS

Given the limitations of IDSs and MDSs in cITSs, there is still a need to design and develop more robust and accurate security solutions that take into account the fundamental characteristics of smart vehicular networks like the context dynamicity, communication unreliability, and data unavailability. In addition, proposed solutions need to deal with the sophisticated and massive attacks that try to create majority dishonest nodes and manipulate the driving context in the network. Similarly, such a solution needs to be aware of the false information that the compromised and rogue vehicles could share with neighboring vehicles. This could be achieved by involving robust situational assessment that takes into consideration the change of credibility and reputation of the vehicles based on the observed behavior and pattern within a certain context. In our future research, we are going to build a robust misbehavior detection model that takes into consideration the evasive nature of the sophisticated misbehavior attacks. We will also address the challenge that the advanced attackers pose when they try to carry out cascaded infections in order to create majority dishonest in the road section and deceive the detection mechanisms.

7. CONCLUSION

In this paper, existing security solutions for smart vehicular networks were reviewed. Throughout this survey paper the extant misbehavior detection in cITSs were analyzed to highlight the different issues related to the detection of misbehavior attacks and how the extant solution deal with them, and the pros and cons of each of these solutions in light of the characteristics of the cITS systems. The nature, characteristics and hierarchy of mobility and safety messages exchanged within the cITS system was elaborated. The different types of the cITS system and their safety and mobility data are explained. The solutions to detect these attacks were discussed. These solutions can be categorized into Intrusion Detection Systems and Misbehavior Detection Systems. The paper started with a general introduction about the smart vehicular networks and the security concerns in cITSs. A background was then provided to introduce the security threats against cITSs with an overview of the solutions that have been proposed so far. Existing IDSs and MDSs solutions for cITSs were then analyzed and elaborated in detail. Based on the analysis, the lessons learned, future work and research directions were discussed. As a future work, this research will be extended by including the implementation of some related works to show the different parameters and factors that govern developing these solutions and determine potential improvement avenues based on the limitations discussed above.

8. REFERENCES

[1] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018/05/01/ 2018, doi: https://doi.org/10.1016/j.future.2017.11.022.

[2] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015, doi: 10.1109/COMST.2015.2388550.

[3] Y. Chen, S. Kar, and J. M. F. Moura, "The Internet of Things: Secure Distributed Inference," IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 64-75, 2018, doi: 10.1109/MSP.2018.2842097.

[4] R. W. v. d. Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 779-811, 2019, doi: 10.1109/COMST.2018.2873088.

[5] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. S. Al-Rimy, F. Saeed, and T. Al-Hadhrami, "Hybrid and Multifaceted Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network," IEEE Access, vol. 7, pp. 159119-159140, 2019, doi: 10.1109/ACCESS.2019.2950805.

[6] T. ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5," ETSI TS, vol. 102, pp. 636-4, 2013.

[7] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," Proceedings of the IEEE, vol. 99, no. 7, pp. 1162-1182, 2011.

[8] A. F. Ghaleb, A. Zainal, A. M. Rassam, and F. Saeed, "Driving-situation-aware adaptive broadcasting rate scheme for vehicular ad hoc network," Journal of Intelligent & Fuzzy Systems, no. Preprint, pp. 1-16, 2018.

[9] F. A. Ghaleb, M. Aizaini Maarof, A. Zainal, M. A. Rassam, F. Saeed, and M. Alsaedi, "Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between

the cooperative awareness messages," Vehicular Communications, vol. 20, p. 100186, 2019/12/01/ 2019, doi: https://doi.org/10.1016/j.vehcom.2019.100186.

[10] F. A. Ghaleb, A. Zainal, M. A. Rassam, and F. Mohammed, "An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications," in 2017 IEEE Conference on Application, Information and Network Security (AINS), 13-14 Nov. 2017 2017, pp. 13-18, doi: 10.1109/AINS.2017.8270417.

[11] T. Pandiangan, I. Bali, and A. Silalahi, "Early Lung Cancer Detection Using Artificial Neural Network," Atom Indonesia, vol. 45, no. 1, pp. 9-15, 2019.

[12] M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," Ad Hoc Networks, vol. 90, p. 101842, 2019/07/01/ 2019, doi: https://doi.org/10.1016/j.adhoc.2019.02.001.

[13] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," Computers & Electrical Engineering, vol. 40, no. 6, pp. 1981-1996, 2014/08/01/ 2014, doi: https://doi.org/10.1016/j.compeleceng.2014.01.009.

[14] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," Computers & Electrical Engineering, vol. 43, pp. 33-47, 2015/04/01/ 2015, doi: https://doi.org/10.1016/j.compeleceng.2015.02.018.

[15] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi layered intrusion detection framework for VANET," Future Generation Computer Systems, vol. 82, pp. 12-28, 2018/05/01/ 2018, doi: https://doi.org/10.1016/j.future.2017.12.008.

[16] T. Zhang and Q. Zhu, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," IEEE Transactions on Signal and Information Processing over Networks, vol. 4, no. 1, pp. 148-161, 2018, doi: 10.1109/TSIPN.2018.2801622.

[17] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Misbehavior detection and efficient revocation within VANET," Journal of Information Security and Applications, vol. 46, pp. 193-209, 2019/06/01/ 2019, doi: https://doi.org/10.1016/j.jisa.2019.03.001.

[18] J. Zacharias and S. Fröschle, "Misbehavior detection system in VANETs using local traffic density," in 2018 IEEE Vehicular Networking Conference (VNC), 5-7 Dec. 2018 2018, pp. 1-4, doi: 10.1109/VNC.2018.8628321.

[19] P. K. Singh, S. Gupta, R. Vashistha, S. K. Nandi, and S. Nandi, "Machine Learning Based Approach to Detect Position Falsification Attack in VANETs," Singapore, 2019: Springer Singapore, in Security and Privacy, pp. 166-178.

[20] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. S. Alrimy, A. Alsaeedi, and W. Boulila, "Ensemble-Based Hybrid Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network," Remote Sensing, vol. 11, no. 23, p. 2852, 2019. [Online]. Available: https://www.mdpi.com/2072-4292/11/23/2852.

[21] X. Zhang, C. Lyu, Z. Shi, D. Li, N. N. Xiong, and C. Chi, "Reliable Multiservice Delivery in Fog-Enabled VANETs: Integrated Misbehavior Detection and Tolerance," IEEE Access, vol. 7, pp. 95762-95778, 2019, doi: 10.1109/ACCESS.2019.2928365.

[22] C. Zhang, K. Chen, X. Zeng, and X. Xue, "Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs," IEEE Access, vol. 6, pp. 59860-59870, 2018, doi: 10.1109/ACCESS.2018.2875678.

[23] H. Amirat, N. Lagraa, C. A. Kerrach, and Y. Ouinten, "Fuzzy Clustering for Misbehaviour Detection in VANET," in 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT), 27-31 Oct. 2018 2018, pp. 200-204, doi: 10.1109/SaCoNeT.2018.8585454.

[24] K. Sharshembiev, S. Yoo, E. Elmahdi, Y. Kim, and G. Jeong, "Fail-Safe Mechanism Using Entropy Based Misbehavior Classification and Detection in Vehicular Ad Hoc Networks," in 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 14-17 July 2019 2019, pp. 123-128, doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00042.

[25] So, Steven, Prinkle Sharma, and Jonathan Petit. "Integrating plausibility checks and machine learning for misbehavior detection in vanet." 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2018.