Misbehavior Detection using Machine Learning in Vehicular Communication Networks

Sohan Gyawali, Yi Qian
Department of Electrical and Computer Engineering
University of Nebraska-Lincoln, Omaha, NE, USA

***Abstract*—Vehicular networks are susceptible to variety of attacks such as denial of service (DoS) attack, sybil attack and false alert generation attack. Different cryptographic methods have been proposed to protect vehicular networks from these kind of attacks. However, cryptographic methods have been found to be less effective to protect from insider attacks which are generated within the vehicular network system. Misbehavior detection system is found to be more effective to detect and prevent insider attacks. In this paper, we propose a machine learning based misbehavior detection system which is trained using datasets generated through extensive simulation based on realistic vehicular network environment. The simulation results demonstrate that our proposed scheme outperforms previous methods in terms of accurately identifying various misbehavior.**

***Index Terms*—Vehicular communication networks, misbehavior detection, anomaly detection, vehicular security, machine learning.**

I. Introduction

Vehicular communications including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P) and vehicle-to-network (V2N) communications are collectively termed as vehicle-to-everything (V2X) communications. This V2X communications can enhance the efficiency and safety of transportation systems. V2X communications along with existing vehicle sensing capabilities provide support for enhanced safety applications, passenger infotainment and vehicle traffic optimization. In addition, V2X communications should support variety of applications like do not pass warning, forward collision warning, queue warning, parking discovery, optimal speed advisory and curve speed warning [1]. The V2X communications are mainly supported by DSRC technology but with the emergence of heterogenous wireless networks [2] and the enhancement in the system capacity of cellular network due to device-to-device communications [3] [4], there is an active research being conducted to support cellular and heterogenous technology based V2X communications.

In vehicular network systems, safety related messages along with traffic management and navigation messages are disseminated periodically. These messages are vulnerable to a number of attacks from passive eavesdropping to active interfering. For example, an attacker can impersonate other vehicles identity and send out false warnings that can disrupt the traffic flow. In addition, vehicular network relies on a trust between participating nodes and is more vulnerable to attack from participating nodes. To tackle these issues, several cryptographic based techniques are proposed [5]. However, this cryptographic based system alone cannot handle these security issues. Instead an effective way is the deployment of misbehavior detection system (MDS) along with the existing cryptographic based system.

However, there exist several challenges for the deployment of misbehavior detection systems in vehicular networks. Due to the high mobility of vehicles, there will be frequent change in the topology of the network. Mainly, routing, mobility and security is affected by this frequent topology change and misbehavior detection system should be able to withstand this dynamic topology. Similarly, deploying MDS only at traffic concentration points will not work for vehicular network due to its ad-hoc nature. In vehicular networks, traffic is dispersed over many routes and in order to analyze this traffic, MDS needs to be deployed at various points. In addition, vehicular communications are done over wireless medium which are susceptible to eavesdropping, jamming and other effects of physical layer. Thus, MDS in vehicular networks should be able to identify packet dropping or physical layer effects and actual attacks. Moreover, MDS in vehicular networks should overcome various resource constraints like limited communication capabilities, storage and processing power along with greatly varying throughput. In traditional scheme for anomaly or intrusion detection, detection systems are deployed at the communication endpoints whereas for vehicular networks, it is essential to deploy misbehavior detection at each intermediate points along with communication endpoints.

To overcome these various constraints, several decentralized MDS have been proposed for vehicular networks. In most of the existing decentralized MDS, detection is done by all participating nodes and then the decision is done based on aggregated results of all participating neighboring nodes. In all of this system, it is assumed that network activities are observable. An observed data or audit data is examined by the system and if this data deviates from normal behavior, then it is referred as an attack.

Misbehavior or anomaly detection system in vehicular networks are mainly classified into three categories. First category is referred to as signature based system. In this system, data is collected and then compared with database behavior of certain attacks. If data coincides with malicious behavior already registered, then it is identified as an attack. This system cannot detect unknown attacks. Second category is referred to as specifications based system. In this system,

978-1-5386-8088-9/19/$31.00 ©2019 IEEE

set of conditions are defined and a program or protocol must satisfy these conditions. If program or protocol does not meet these conditions then it is identified as an attack. Third category is referred to as anomaly detection system. In this system, machine learning technique is used to create a model of trustworthy and anomaly activity and the new behavior is compared against this model. This kind of system can identify unknown attacks.

There are mainly three categories of architecture for MDS in vehicular networks [6]. The first one is standalone MDS. In this system, each node collects data on its own using its local resources and apply misbehavior detection to detect anomaly. Each node has no information about the position of other nodes and make decision without any cooperation. The second one is cooperative and distributed MDS. In this system, different nodes cooperate with each other to detect an anomaly. Here, the information from different anomaly detection system is exchanged with each other and the decision is based on the aggregated result. The main problem in this system is the network traffic overhead. The third is hierarchical MDS. In this system, network is divided into set of groups or clusters and each cluster have one cluster head. Cluster head is identified by cooperative algorithm between nodes. In this system, there is cooperation between cluster head and cluster member only, which reduces the network traffic overhead. All cluster members send their data to cluster head. Cluster head aggregate the result and then make a final decision to decide whether there is an attack or not. However, cluster head management is the main problem in the vehicular network environment.

In this work, we propose a cooperative machine learning based scheme to detect two kinds of attacks: false alert attack that broadcasts false alert message and position falsification attack that falsifies the location information. In the proposed scheme, each vehicle is equipped with MDS and each vehicle broadcast the detection result to its neighbors, as shown in Fig. 1. On the basis of aggregated results from all neighboring vehicles, misbehaving vehicles are evicted from the system.

The rest of this paper is organized as follows. Section II summarises various related work. Section III discusses about vehicular network model. Section IV presents the misbehavior detection system. Section V discusses the methods employed in the proposed scheme. Section VI shows the experimental results and finally Section VII concludes the paper.

II. Related work

MDS is an effective way to detect misbehavior with high accuracy as compared to cryptographic mechanisms. There have been a lot of work to address misbehavior detection in vehicular networks. In [7], the authors proposed a method called LEAVE for locally evicting misbehaving vehicles from a vehicular networks. In this scheme, upon detecting an attacker, vehicle broadcasts warning messages to all vehicles in the range. Any receiving vehicle adds the warned device to an accusation list. Once nodes are added to

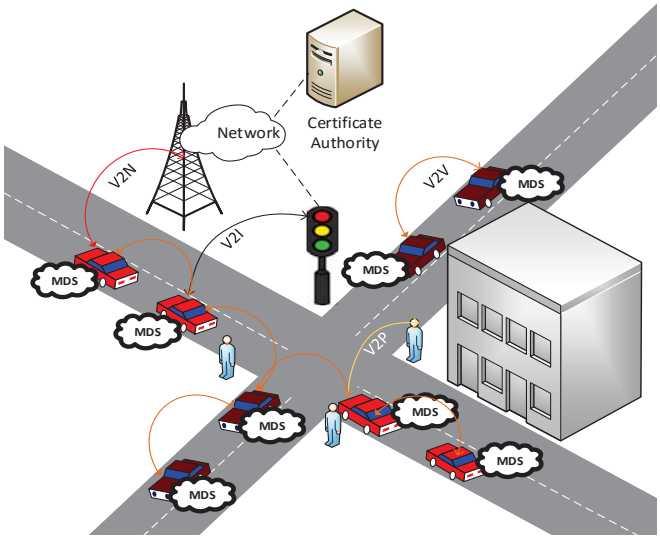

Fig. 1: General V2X communications model

black list, disregard messages are repeatedly broadcasted to local neighborhood instructing the receiving node to ignore attacker's message. This method provides a fast eviction of misbehaving vehicles without the need of central authority. In [8], the authors proposed a new method called Stinger, in which a device unilaterally removes a misbehaving neighbor by agreeing to limit its own participation. Authors also compared the security and performance properties of LEAVE and Stinger. They found that LEAVE is better at handling false positives whereas Stinger scales better when traffic density increases.

There are lot of research in signature or specification based misbehavior detection system in vehicular networks. In [9], the authors proposed a concept of guard vehicles which can monitor a link between any two vehicles. Guard vehicles monitor packets and other parameters to detect DoS attacks, integrity target attacks and false alert generation attacks. The proposed method is based on set of rules to detect malicious vehicle promptly and with high accuracy. In [10], the authors proposed a method which detects false alert messages and misbehaving nodes by observing their action after sending out the alert messages. In the proposed method, the decision is made based on consistency of recent messages and new alerts with reported and estimated vehicle positions. In [11], the authors employed a statistical technique to detect false information attack. They employed Green shield model to detect false information attack using statistical technique. In [12], the authors proposed the concept of acceptance range threshold (ART) for position verification scheme. They used ART based on the observation that all radio networks have a maximum communication range where packet sent by others can be successfully received. In [13], the authors introduced vehicular reference misbehavior dataset (VeReMi) for the evaluation of different misbehavior detectors. The authors also evaluated different detectors on their datsets using metrics such as precision and recall. Although rules

or specifications based misbehavior detection system can provide some sort of security from known attacks, they cannot identify the unknown attacks.

There is also an active research in machine learning based scheme to detect different misbehaviors in vehicular networks. In [14], the authors used features extracted from trace file to detect the attack. The intrusion/anomaly detection system used the trace file as auditable data to detect the attack. The proposed intrusion detection system uses artificial neural network and fuzzified data to detect black hole attacks. In [15], the authors proposed an intrusion detection system to protect vehicular network system from greyhole and rushing attack. They generated trace file using NS2. Generated trace file was used as an input to feed forward neural network (FFNN) and support vector machine (SVM) for data classification process. However, all of these machine learning based schemes are based on private datasets and are difficult to verify.

In our scheme, we generated labelled datasets through realistic vehicular network simulations. We evaluated our datasets using different machine learning model. In addition, we evaluated our machine learning based scheme in publicly available datasets and found superior performance compared to previous schemes.

III. Vehicular network model

A. System model

In the proposed scheme, each vehicle registers with the certificate authority (CA). During the registration, each vehicle obtains a unique identity I, pseudonyms identities, a pair of private S_k and public P_k cryptographic keys and a certificate $Cert_{CA}(I, P_k)$ issued by the CA. Basic safety beacons and alert beacons are considered in this scheme. Basic safety beacons are transmitted periodically every 300 ms whereas alert beacons are transmitted when triggered by some events. Basic safety beacons include various information such as sender id, message id, send time, position, speed and other application specific information. In addition to information included in basic safety beacons, alert message is also included in alert beacons.

B. Threat model

A vehicle is considered as a malicious or threat to a system if it deviates from the normal vehicular network protocol. A malicious vehicle or attacker can control number of nodes and can perform various attacks by falsifying the position information in safety message as well as broadcasting the false alert message. We consider two common categories of attacks:

1) False alert generation attack: In this case, the malicious vehicle sends false alert to its neighbors. Alert messages may include emergency electronic brake light, road hazard condition notification, road feature notification, cooperative collision warning or emergency vehicle approaching. False alert may cause disruption in the traffic or some traffic accidents. It is very crucial to detect these false alerts for the normal operation of vehicular network system.

2) Position falsification attack: In this case, the malicious vehicle falsifies the position information in broadcast beacons. Attacker can use this position falsification to perform sybil attack in which they create multiple identities with provided false locations. This position falsification attack may lead to traffic congestion as well as accident.

IV. Misbehavior detection system

Misbehavior detection system are more suitable mechanism to detect both internal and external attacks/misbehaviors. In our work, machine learning based MDS is used to identify attackers and cooperative scheme is used for the fast eviction of misbehaving vehicles.

A. Machine learning based misbehavior detection system

1) False alert verification scheme: In the false alert attack, the attacker broadcast false alerts such as accident ahead or traffic congestion to its nearby vehicles. To make alert plausible to others, attackers may lower the flow and speed value and transmit it to others. In our proposed scheme, we create a scenario in which attacker generates the false alert and broadcast low value of speed and flow to make it plausible. However, in case of normal traffic if the attacker transmits low value of flow and speed then it will be the only one to transmit low value and it can be easily flagged. We use Greenshield model [9] to verify whether the alert is real or not.

Greenshield model is used to estimate and model uninterrupted traffic. Greenshield model assume a linear speed-density relationship and is given as:

$$v = v_f - (v_f/d_j) \times d \tag{1}$$

where, v is the mean speed at density d, v_f is the free speed and d_j is the jam density. The relation between flow, density and speed is given as:

$$q = d \times v \tag{2}$$

where, q is the flow of the vehicle. From equation (1) and (2), we obtain a relation

$$q = v_f \times d - [v_f/d_j] \times d^2 \tag{3}$$

In the proposed scheme, each vehicle can calculate the density of vehicles and the average speed of vehicles within its communication window. On the basis of average speed and density, each vehicle can calculate the value of flow. Each vehicle broadcast calculated value of this flow to its neighbor. On the receiver side, a vehicle may receive this value of flow from multiple vehicles within a certain time. On the basis of received value of flows from all neighbors, each vehicle can calculate the average value of flow. On the basis of calculated value of flow and received value of flow, each vehicle can derive a new feature name difference in flow which is the difference of average flow and received value of flow.

Each time a vehicle receives an alert beacon from its neighbor, it passes the information of alert beacon along with alert message to its local detection system. Each local

detection system uses either historical datasets or datasets generated through simulations to verify the authenticity of an alert.

2) Position falsification verification scheme: In the position falsification attack, the attacker changes the position information in the beacon. For the position verification scheme, various position falsification attacks such as constant, constant offset, random, random offset and eventual stop attacks are considered. In constant position attack, the attacker transmits fixed position information whereas in constant offset attack, the attacker transmits fixed offset added to their actual position. Similarly, in random attack, the attacker transmits random position from the simulation areas whereas in random offset attack, the attacker transmits random position from within the pre-configured area of the vehicle. In eventual stop attack, the attacker behaves normally for some time and then transmit the current position repeatedly.

Machine learning based MDS is used to identify these position falsification attacks. In the proposed scheme, MDS infers whether there is an attack or not based on the various features generated from the received beacon. Each time a vehicle receives a beacon from another vehicle, it compares its information with previous beacon and local information of its own detector. Based on these information, each vehicle can generate various features such as change in speed between two beacons, change in position between two beacons, receiving distance, RSSI, change in its own speed, change in its own position etc. These information along with other basis information are fed to its local MDS. MDS which is trained based on extensive simulation can verify about different attacks.

B. Fast exclusion of misbehaving vehicles

For the fast exclusion of misbehaving vehicles, a scheme similar to LEAVE protocol [7] is used. In this scheme, upon detecting an attacker, vehicle broadcasts warning messages to all vehicles in its vicinity. Each receiving vehicle adds the warned device to an accusation list. Once enough warning messages are obtained, warned vehicle's identifier is added to local blacklist. Disregard messages are then repeatedly broadcasted to local neighborhood, instructing receiving node to ignore attacker's message. Once the vehicle is in range of infrastructure such as RSU or base station, local blacklist is sent to CA which then permanently exclude the attacker's vehicle from the vehicular network.

V. Methodology

A. Mobility Model

For realistic demand and mobility patterns, Luxembourg SUMO traffic scenario (LuST) [16] is used. The LuST scenario is built with information from a real mid-size European city and the traffic demand is based on real information. The authors in [14] used simulation of urban mobility model (SUMO) for generation of real world traffic. They have shown that the speed distributions from the mobility traces in the simulations are similar to the real data set which motivated us to use this mobility traces for simulations.

B. Simulation environment

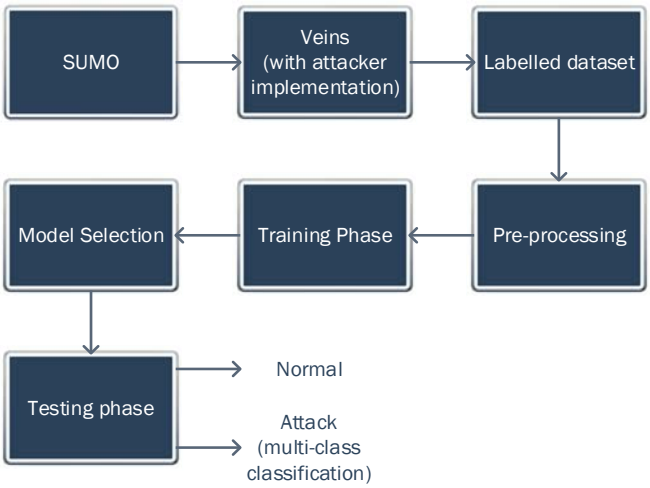

Fig. 2: Methodology of misbehavior detection system

TABLE I: Simulation Parameters

Parameters	Values
Mobility	SUMO LuST (DUA static)
Simulation duration	100s
Attacker density	0 - 40%
Signal interference model	Two-Ray Interference
Obstacle shadowing	Simple
Fading	Jakes
Shadowing	Log-Normal
MAC implementation	802.11p
Thermal noise	-110 dbm
Bit rate	6 Mbps
Sensitivity	-89 dBm
Antenna model	Monopole on roof
Beaconing rate	1 hz

Veins 4.7 framework is used to make vehicular network simulations as realistic as possible. Veins is an open source framework and is based on two simulators: OMNET++ and SUMO. OMENT++ is an event based network simulator and SUMO is road traffic simulator for generation of mobility traces. Veins couples both simulators bi-directionally which helps to examine complex interaction between both domains.

For false alert analysis, Veins source code is modified to model false alert attacker which broadcast false alert messages. Simulation parameters as shown in Table I is used for the generation of datasets and analysis of false alert verification scheme. In the proposed model, attackers will constantly broadcast false messages to its neighbors and lower the value of flow and speed to make it plausible. Labelled datasets are generated through simulation in OMNET++, in which, if there is an attack then it is labelled as

an attack and if not then it is labelled as normal. Labelled datasets consists of various features such as receive time, send time, sender position, sender speed, sender change in speed, sender change in position, receiving distance, receiver change in speed, receiver change in position, receiver calculated flow, sender sent flow etc. Preprocessing and feature engineering are then applied to lower the dataset size. Preprocessed datasets are passed through training phase for model selection. Selected machine learning model is used for multi-class classification in testing phase as shown in Fig. 2.

For position falsification analysis, VeReMi dataset [13] is used. VeReMi is the public extensible dataset in which authors have modeled various position falsification attacks. Datasets from VeReMi were combined into single csv file. In addition, various features such as distance between sender and receiver, sender change in position, sender change in speed, receiver change in position, receiver change in speed etc. were derived by importing VeReMi datasets into our python program.

VI. Performance Analysis

A. Evaluation Metrics

In general, we evaluated the performance of the proposed scheme in terms of precision, recall and f1 score. The proposed misbehavior detection system requires high detection rate and low false alarm rate. Confusion matrix as shown in Table II is used to calculate various parameters.

TABLE II: Confusion matrix

		Predicted result	
		Negative	Positive
Actual result	Negative	True Negative (TN)	False Positive (FP)
	Positive	False Negative (FN)	True Positive (TP)

- Accuracy is the ratio of correctly predicted observations to the total observations.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

- Precision shows the ratio of correctly predicted malicious vehicles to the total predicted malicious vehicles.

$$Precision = \frac{TP}{TP + FP} \tag{5}$$

- Recall shows the ratio of correctly predicted malicious vehicles to the total actual malicious vehicles.

$$Recall = \frac{TP}{TP + FN} \tag{6}$$

- F1 score is the weighted average of precision and recall.

$$F1\,score = 2 \times \frac{precision \times recall}{precision + recall} \tag{7}$$

Accuracy is a great measure when there is a symmetric dataset, but for asymmetric datasets, accuracy tends to give biased results. For imbalanced datasets such as the datasets used in the proposed scheme, precison and recall tends to give more accurate analysis.

B. False Alert Verification Scheme

For false alert verification scheme, the model was evaluated on various attacker density scenarios. Machine learning algorithms such as decision tree classifier, k-nearest neighbor, logistic regression, random forest and bagging were used as shown in Table III. Pre-processing and feature engineering were also performed using various library of scikit package to increase the precision and recall score. First, for 30% attacker density scenario, various machine learning algorithms were evaluated. As shown in Table III, random forest gave high score and was used for further analysis.

The effect of attacker density on the score of precision, recall and f1- score was evaluated using random forest classifier. From the Fig. 3, we can see that when the attacker density is only 5%, we obtain very high score for precision, recall and f1-score. With the increase in the attacker density, precision, recall and f1-score decreases gradually. Even in the worst case of 40% attacker density, the proposed scheme has high precision, recall and f1-score of 93.8%, 92.3% and 93.1% respectively.

TABLE III: Simulation Results - False alert verification

Model	Precision	Recall	F1-score
Logistic Regression	0.84	0.74	0.78
K-Nearest Neighbor	0.94	0.93	0.94
Decision Tree classifier	0.97	0.91	0.94
Bagging	0.98	0.92	0.94
Random Forest	0.98	0.92	0.95

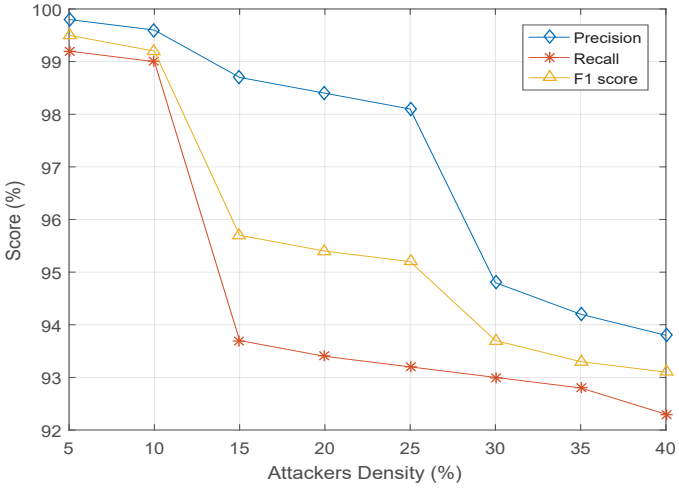

Fig. 3: Precision, recall and f1 score for false alert verification scheme

C. Position Verification Scheme

For position verification scheme, labelled datasets were derived using VeReMi datasets. The derived datsets were divided into training and testing datasets. For position verification scheme, various machine learning algorithms were

implemented. As shown in Table IV, bagging classifier gave the high score and was used to compare the proposed scheme with VeReMi scheme as shown in Table V.

TABLE IV: Simulation Results - Position verification scheme

Model	Precision	Recall	F1-score
Logistic Regression	0.71	0.80	0.72
K-Nearest Neighbor	0.94	0.85	0.89
Decision Tree classifier	0.96	0.95	0.96
Random Forest	0.98	0.93	0.96
Bagging	0.98	0.94	0.96

TABLE V: Comparison of the proposed scheme with VeReMi scheme

Attacks	Proposed		VeReMi	
	Precision	Recall	Precision	Recall
Constant position attack	1	0.99	1	1
Constant offset attack	0.94	0.80	0.4	1
Random attack	1	0.99	1	0.99
Random offset attack	0.97	0.95	0.70	0.95
Eventual stop	0.98	0.93	0.8	0.90

In VeReMi, the authors have evaluated their datasets using various detectors such as acceptance range threshold (ART), sudden appearance warning (SAW), simple speed check (SSC) and distance moved verifier (DMV). We compared the result of our scheme with the result of their best detector for each position attacker types.

From Table V, we can see that for constant position attack and random attack, detectors used in VeReMi and our machine learning scheme gave similar performance. However for other position attack scenarios, our scheme outperforms the VeReMi scheme. VeReMi used four different detectors in parallel to detect these attacks. However, a single machine learning model is used in our scheme to identity all attacks i.e, multi-class classification. Performance of detectors in VeReMi varies with different threshold value. However, our scheme is free of any threshold values and is only based on datasets and learning model.

VII. Conclusions

Vehicular networks are susceptible to variety of attacks and misbehavior detection system is found to be very effective against these attacks. In this paper, we discussed different approaches used for identifying these attacks. We showed how machine learning based misbehavior detection is more effective to detect internal attacks as compared to other schemes. One of the advantages of using machine learning based scheme is the identification of both existing and new attacks. For false alert verification scheme, we generated our own datasets and analyzed the datasets using different machine learning model. We obtained high precision, recall and f1 score for false alert verification scheme. Similarly, for position verification scheme we analyzed our scheme on publicly available datasets and found superior performance compared to previous schemes. As part of our future work, we plan to examine our scheme with new or unknown attacks.

References

[1] CISCO, "Optimizing 5G for V2X - Requirements, Implications and Challenges, *IEEE VTC Mission-Critical 5G for Vehicle IoT*, Sept. 2014.

[2] S. Gyawali, S. Xu, F. Ye, R. Q. Hu and Y. Qian, "A D2D Based Clustering Scheme for Public Safety Communications," *Proceedings of 87th IEEE Vehicular Technology Conference (VTC Spring)*, Porto, pp. 1-5, 2018.

[3] Q. Li, Y. Xu, R. Q. Hu, and Y. Qian, "Optimal Fractional Frequency Reuse and Power control in the Heterogeneous Wireless Networks," *IEEE Transactions on Wireless Communications*, Vol.12, No.6, pp.2658- 2668, June 2013.

[4] D. Wu, J. Wang, R. Q. Hu, Y. Cai, L. Zhou, "Energy-efficient resource sharing for mobile device-to-device multimedia communications," *IEEE Transactions on Vehicular Technology*, Vol.63, No.5, pp.2093-2103, June 2014.

[5] F. Qu, Z. Wu, F. Wang and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985-2996, Dec. 2015.

[6] S. Chadli, M. Emharraf, M. Saber and A. Ziyyat, "The design of an IDS architecture for MANET based on multi-agent,"*Proceedings of third IEEE International Colloquium in Information Science and Technology (CIST)*, Tetouan, pp. 122-128, 2014.

[7] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[8] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson and J. Hubaux, "Fast Exclusion of Errant Devices from Vehicular Networks," *Proceedings of 5th annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks,* San Francisco, CA, pp. 135-143, 2008.

[9] H. Sedjelmaci, S. M. Senouci and M. A. Abu-Rgheff, "An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks," *IEEE Internet of Things Journal*, vol. 1, no. 6, pp. 570-577, Dec. 2014.

[10] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak and I. Stojmenovic, "On Data-Centric Misbehavior Detection in VANETs," *Proceedings of IEEE Vehicular Technology Conference (VTC Fall)*, San Francisco, CA, pp. 1-5, 2011.

[11] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703-6714, Aug. 2016.

[12] T. Leinmuller, E. Schoch, F. Kargl, C. Maihofer, "Decentralized position verification in geographic ad hoc routing," *Security and Communication Network*, Wiley online library, Aug. 2008.

[13] R. W. van der Heijden, T. Lukaseder, F. Kargl, "VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs", arXiv preprint arXiv:1804.06701, 2018.

[14] K. M. A. Alheeti, A. Gruebler and K. D. McDonald-Maier, "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars," *Proceedings of sixth International Conference on Emerging Security Technologies (EST), Braunschweig*, pp. 86-91, 2015.

[15] K. M. A. Alheeti, A. Gruebler and K. D. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," *Proceedins of 7th Computer Science and Electronic Engineering Conference (CEEC), Colchester*, pp. 231-236, 2015.

[16] L. Codeca, R. Frank, S. Faye and T. Engel, "Luxembourg SUMO Traffic (LuST) Scenario: Traffic Demand Evaluation," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 2, pp. 52-63, Summer 2017.