A Novel Framework for Misbehavior Detection in SDN-based VANET

Conference Paper · January 2021

DOI: 10.1109/ANTS50601.2020.9342778

3 authors, including:

Rukhsar Sultana
Malaviya National Institute of Technology Jaipur
7 PUBLICATIONS **80** CITATIONS
SEE PROFILE

Jyoti Grover
Malaviya National Institute of Technology Jaipur
59 PUBLICATIONS **839** CITATIONS
SEE PROFILE

2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) | 978-1-7281-9290-1/20/$31.00 ©2020 IEEE | DOI: 10.1109/ANTS50601.2020.9342778

A Novel Framework for Misbehavior Detection in SDN-based VANET

Rukhsar Sultana
Department of Computer Science and Engineering
Malaviya National Institute of Technology Jaipur, India
Email: 2019rcp9045@mnit.ac.in

Jyoti Grover
Department of Computer Science and Engineering
Malaviya National Institute of Technology Jaipur, India
Email: jgrover.cse@mnit.ac.in

Meenakshi Tripathi
Department of Computer Science and Engineering
Malaviya National Institute of Technology Jaipur, India
Email: mtripathi.cse@mnit.ac.in

***Abstract*—Vehicular Ad Hoc Networks (VANET) enables the communication between vehicles and Road Side Units (RSU) to execute numerous safety and non-safety applications. Insider nodes of VANET can misbehave by transmitting faulty and incorrect Vehicle-to-Everything (V2X) messages. Effective Misbehavior Detection System (MDS) is developed to detect such misbehaving insider nodes. MDS constantly monitors the transmitting messages to detect incorrect data packets by using plausibility and consistency checks. Based on these checks, MDS identifies misbehaving vehicles. However, existing detection systems are not adaptive to network changes. Hence, we propose a framework for misbehavior detection in Software-Defined Networking (SDN)-based VANET by exploiting the programmability and flexibility features of SDN. SDN allows the dynamic adjustment of input parameters for the detection process according to the varying network context. Consequently, the proposed framework provides effective and accurate detection performance in diverse VANET scenarios.**

***Index Terms*—SDN-based VANET, MDS, Security, VANET**

I. Introduction

Cooperative Intelligent Transportation System (C-ITS) introduced phenomena of Vehicular Ad Hoc Networks (VANET) to facilitate safety, non-safety, e-commerce and infotainment applications [1]. VANET enables direct communication between vehicles and infrastructure units, such as Road Side Units (RSU), base stations etc. Deployment of VANET applications lacks in flexibility and faces different network issues and challenges. Software-Defined Networks (SDN) can address these challenges and control the functionality of VANET in a flexible and systematic way [2]. Since VANET consists of a variety of network components and applications, it is threatened by external and internal security attacks. External attacks are performed by outsiders which do not have access to the network system. These types of attacks can easily be avoided using Public-key Infrastructure (PKI)-based asymmetric cryptography mechanisms. While internal attacks are performed by the insider nodes of VANET which are authenticated members and possess valid key credentials for network access. Insider nodes are able to transmit legitimate messages and communicate in the network. Therefore, it is difficult to detect them using cryptography-based solutions. These attacks can disrupt network services by performing various types of misbehavior like transmission of faulty information and wrong safety messages, packet replay, position forging, location spoofing etc.

Misbehavior Detection System (MDS) can be exploited for advance detection of misbehaving activities and entities through continuous monitoring of data semantics of transmitting V2X messages. Usually, two types of misbehavior detection mechanisms are used [3]:-(a) Data-centric, and (b) Node-centric. Data-centric mechanisms perform plausibility and consistency checks on data semantics to ensure the correctness and consistency of transmitted data. In node-centric mechanisms, MDS continuously monitors the forwarding behavior of VANET nodes by analyzing correctly formatted messages and packet frequency. Node-centric detection can be performed by applying behavioral mechanisms and trust-based mechanisms. Some detection systems [4] utilize a combination of both mechanisms for more accuracy.

There can be various forms of misbehavior in VANET. Therefore, basic plausibility checks are not sufficient to detect these threats. Different features of attacks can be used to detect threat vector through machine learning classification algorithms [5]. Existing security solutions are not appropriate for VANET due to its inherent characteristics such as dynamic topology, high mobility and intermittent links. In such a case, SDN-based VANET can be useful to implement security solutions which are adaptive to present network context and varying attack forms. SDN controller keeps track of each network activity and provides real-time information regarding vehicle density, transmitted packets and various attacks features [6].

SDN-based VANET provides an appropriate environment to implement adaptive misbehavior detection systems. We propose a framework for misbehavior detection in SDN-based VANET which is based on a simulation framework (F^2MD) proposed in [7]. In our framework, the Global SDN Controller (GSC) is installed at the Certification Authority (CA) and it functions as a global misbehavior detection authority. The whole network area is divided into clusters according to the radio range of RSUs. Here, base station works as RSU and considered as CH of cluster created in its radio range. RSUs are provided with SDN capabilities and they are called RSU SDN Controllers (RSC). The vehicles (in the radio range of

978-1-7281-9290-1/20/$31.00 ©2020 IEEE

CH) known as cluster members (CM), perform misbehavior detection using plausibility and consistency checks and forward the results of plausibility checks to RSC. Based on the received results, RSC executes advance misbehavior detection process using fixed or learning algorithms and generate reports accordingly. These reports are forwarded to GSC. In accordance with the received reports, GSC decides the satisfactory reaction on misbehavior. As SDN has programmability and centralized control features, the proposed model for SDN-based VANET is aware of network changes and adaptive to those changes. Thus, the proposed model comes up with higher detection performance than usual static detection systems.

This paper is organized as follows. Section II describes the previous work related to misbehavior detection and reaction in VANET using machine learning and SDN paradigm. Section III presents the proposed framework along with its architecture and working mechanism. The performance of the proposed work is evaluated in Section IV. Finally, Section V provides a conclusion of the whole work.

II. Related Work

VANET is affected by various forms of internal security attacks. In order to detect these attacks, numerous mechanisms were proposed in the literature. Traditional security algorithms cannot detect all the attacks together. Therefore, author in [8] proposes a collaborative security attack detection mechanism. This mechanism can detect various types of attacks, such as DoS attack, probing attack by using multi-class Support Vector Machine (SVM) classifier. Based on the collected flow information from vehicles, Software Defined Vehicular Cloud (SDVC) controller trains the SVM classifier in a centralized manner. The classifier is distributed to vehicles so that they can detect different unexpected attacks accurately. This mechanism using SVM in vehicular cloud has better precision, recall and accuracy than the nearest neighbour SVM scheme and individual SVM scheme in terms of precision, recall and accuracy. However, it can cause bandwidth consumption and communication overhead at the time of flow collection by SDVC controller. A framework is proposed in [9] that uses plausibility checks as a feature vector for misbehavior detection and classification in VANET. This framework exploits VeReMi dataset (VDS) [10], built-in VEINS and provides five types of position forging attacks. It shows that overall detection performance can be enhanced using plausibility feature vector in K- nearest neighbours (K-NN) and SVM classifiers. This framework does not detect additional attacks, such as Sybil attack. Author in [4] proposes a misbehavior detection system using the SDN paradigm in a vehicular network. This system is context-aware and Sybil attack resistant. It can tune to various security parameters and provides a low false positive rate and high detection ratio in different contexts. Here, detection is based on trust computation on each control level. Clustering is also performed on the basis of trust values. This system higher performance than system without SDN, but it causes lots of computation overhead with the changes in network context.

III. Proposed Misbehavior Detection Framework

In this section, we describe the proposed misbehavior detection system architecture and its components.

A. Architecture of Misbehavior Detection System

Our architecture for misbehavior detection in SDN-based VANET is inspired from proposed hierarchical SDN vehicular network architecture in [11] and illustrated in Figure 1. In our proposed architecture, the whole network control is divided into two SDN levels. (i) At the first level, the network topology is partitioned into clusters, in accordance with base station radio range in the data plane. Base station works as Cluster Head (CH) of the cluster within its range. Base station RSUs are installed with SDN controller capabilities and they are called RSU SDN Controller (RSC). Vehicles are equipped with IEEE 802.11p interface for V2V and V2I communication. Base stations working as RSC are provided with 5G/4G LTE interface for wireless communication with Global SDN controller and a wired communication interface for communication among RSUs, and (ii) Second level SDN control is carried out by Global SDN Controller (GSC) installed at Certification Authority (CA). GSC provides global control over the network and constantly monitors the ongoing network activities.

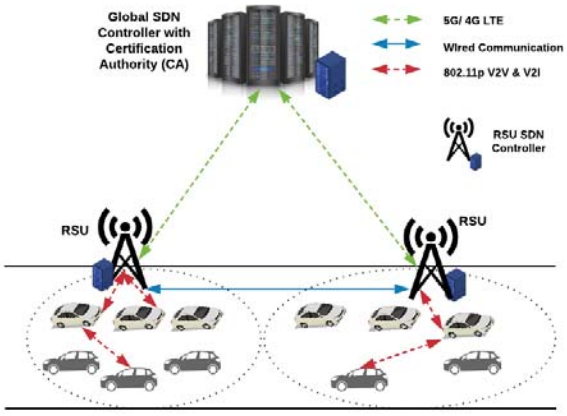

Fig. 1. Misbehavior Detection System Architecture

GSC provides the digital certificates (pseudonym certificates) to vehicles and RSUs on request. At GSC, the Public Key Infrastructure (PKI) is also exploited which is responsible for vehicle authentication globally. It also enables cryptography solutions to handle external attacks.

Our proposed model for misbehavior detection in SDN based VANET is based on a simulation framework for misbehavior detection (F^2MD) in a vehicular network. By using F^2MD, one can implement a new set of attacks, misbehavior detection algorithms, and can evaluate the performance of the newly implemented algorithm and effectiveness of various attacks. Based on this, our framework is divided into three phases as shown in Figure 2. These phases are (i) Clustering

in the data plane; (ii) Local misbehavior detection; and (iii) Global misbehavior detection. These phases are described in Section III-B.

B. Framework for Misbehavior Detection

Due to flexibility and programmability features of SDN based VANET, proposed misbehavior detection system can be adjusted as per the requirements of network. SDN controller continuously monitors the whole network traffic and activities. Hence, the proposed detection system is aware of the network changes and current network statistics like vehicle density, various types of attacks etc. In this section, we present a conceptual overview of different phases of the framework. The evaluation of our work is also presented in Section IV, which shows that the proposed system carries out misbehavior detection with high accuracy and efficiency according to the current network scenario. The working process of the proposed misbehavior detection framework is summarized in Algorithm 3. As shown in Figure 2, the detection process is carried out in the following phases:

1) Clustering in data plane: In SDN based VANET, one centralized SDN controller cannot coordinate and communicate with all of the vehicles together in case of a large network. Therefore, the whole network area is partitioned into clusters in the first phase prior to the local misbehavior detection. In VANETs, each vehicle periodically broadcasts short packets (beacons). At each regular time interval t, the clustering process is accomplished by RSC based on received beacons from the passing by vehicles. These vehicles are considered as a Cluster Members (CM). Since RSC is installed with SDN controller capabilities and equipped with additional resources, it works as CH for vehicles in its range.

2) Local misbehavior detection: Local misbehavior detection is performed by the data plane elements (vehicles and RSUs). This phase includes data-centric detection followed by node-centric detection. These detections are accomplished by using basic plausibility and consistency checks, and local detection application. After the data-centric detection, the results are sent to a local detection application for node-centric detection.

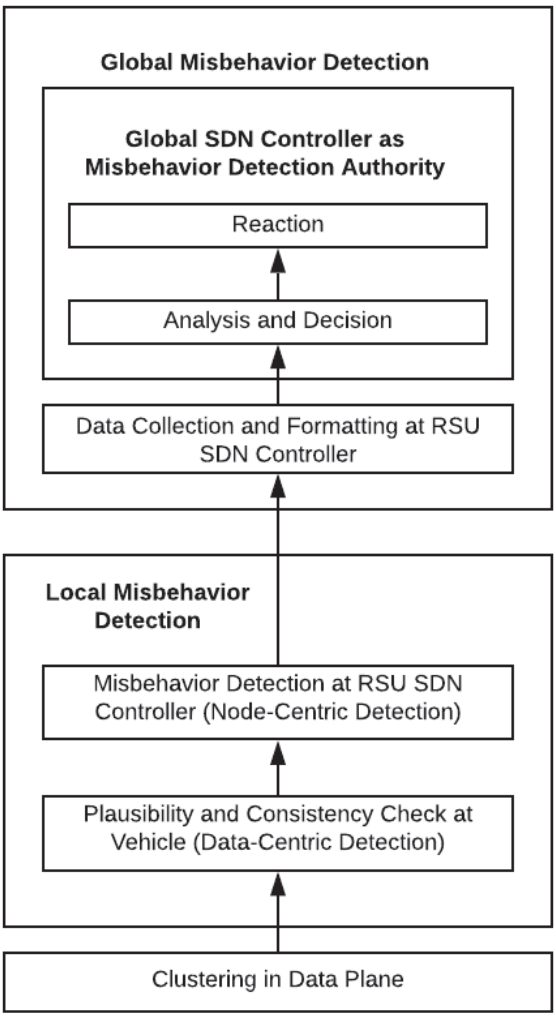

Fig. 2. Framework for Misbehavior Detection

1) **Plausibility and consistency check at vehicle (Data-centric detection):** Cluster members i.e. vehicles of each cluster perform plausibility and consistency checks on every receiving of beacons or Basic Safety Message (BSM). These checks can be implemented in various forms [12]. Major forms include plausibility and consistency checks for position, speed and range using predefined threshold values. Position plausibility checks whether the position of a sending node is at a plausible place or not. Range plausibility ensures that the sender location is in predefined radio range. Speed plausibility checks if the speed announced by the sender is under the predefined speed threshold. A consistency check is carried out on the basis of two successive BSMs. Position consistency confirms that the two continuous BSMs received from the same sender have separative plausible distance. In the same manner, speed consistency examines if the two successive received BSMs have plausible changes in their speed. Additional checks can also be performed, such as beacon frequency, intersection check, position heading consistency etc. After performing these checks, Plausibility Check Results (PCR) are produced and transmitted to RSC for node-centric detection. The major steps of data-centric detection phase are illustrated in Algorithm 1. If any of the sender fails in the message plausibility check, it is marked as a misbehaving node and results of these checks are transmitted to RSC for advance misbehavior detection.
2) **Misbehavior detection at RSU SDN controller (Node-centric detection):** If any of the sending vehicle fails in the message plausibility check, cluster members report that vehicle to their RSC for node-centric detection.

Algorithm 1: Data-Centric Detection

Data: Set of vehicles (V), Number of vehicles in the network scenario (n)
Result: Plausibility Check Results (PCR)
begin
  Each $V_m \epsilon V$ where $m = 1, 2, ...n$, performs plausibility and consistency checks for every received beacon from the other vehicles;
  if *received beacon fails in the plausibility check* **then**
    Mark the beacon sender node as implausible and generate the plausibility results;
  end
  Send the plausibility results to RSC;
end

Algorithm 2: Node-Centric Detection

Data: Plausibility Check Results (PCR)
Result: Misbehavior Report (MR)
begin
  Extract features from (PCR) for each of the sender-receiver pair in the PCR;
  for *Each feature vector f extracted from* (PCR) **do**
    Perform classification using a machine learning model for misbehavior detection;
    if *the sender in the PCR is detected as misbehaving vehicle* **then**
      Generates the Misbehavior Report (MR) in a format and add the MR to the database
    end
  end
end

For advance detection of a misbehaving node, fusion applications including fixed algorithms and learning-based algorithms can be implemented on RSC. Fusion applications need a fusion of multiple factors such as node history, plausibility results etc. Using fixed algorithms, various applications such as threshold, aggregation and behavioral applications can be executed. Learning algorithms are implemented by using a variety of machine learning models. For this purpose, features are extracted from the message plausibility checks results. These features are exploited to classify the genuine vehicles from misbehaving vehicles through classifiers like K-Nearest neighbour (K-NN), Support Vector Machine (SVM), Multi-Layer Perceptron (MLP) etc. However, the detection performance of learning algorithms remains better than the fixed algorithms. Learning algorithms are more adaptive to the network statistics and their input parameters can also be altered through SDN programming according to network scenario. Therefore, learning algorithms are preferred for advanced misbehavior detection in SDN based VANET. Algorithm 2 summarizes the phase of node-centric detection.

After the local misbehavior detection process, if a misbehaving vehicle is detected, a Misbehaving Report (MR) is generated. The MR is generated in a particular format as described in [13]. These generated reports are added to the database at RSC.

3) Global misbehavior detection: This phase deals with the global reporting of misbehaving vehicles at the global SDN controller. On receiving a report, suitable reactions are decided by the global SDN controller. Three main functionalities of this phase are described as follows:

Algorithm 3: Misbehavior Detection in SDN-based VANET

Data: Set of vehicles (V), Number of vehicles in the network scenario (n)
Result: Misbehaving Vehicles, Reaction on misbehavior
begin
  Algorithm 1;
  Algorithm 2;
  At each time interval t, RSU SDN Controller RSC collect Misbehavior Report (MR) from the database ;
  Group the MRs which have same implausibly α ;
  Send the aggregated MRs to the Global SDN Controller (GSC) ;
  for *each of the received MRs from RSC* **do**
    Analyse the MR and decide the reaction level ;
    According to the reaction level, decide the misbehavior reaction;
  end
end

1) **Data collection and formatting at RSU SDN controller:** On the basis of predefined criteria, misbehavior data reports can be accessed from the database. As in our model, the network area is divided into cluster regions according to the radio range of RSC. At a fixed interval t, RSC aggregates all the misbehavior reports of its cluster region and categorises the reports according to the level of implausibly (α). Then, these aggregated reports are forwarded to the GSC for further analysis and decision.
2) **Analysis and Decision:** All the collected reports are analyzed in this phase to decide the reaction level. Reaction level is decided according to the level of implausibly (α) and number of misbehaving reports (k). These factors are given as output of this phase, which is used as the reaction level input for the next phase.
3) **Reaction:** Based on the reaction level received from the analysis phase, the global SDN controller decides the misbehavior reaction. If level 0 is received, then

no reaction is provided. Otherwise, the vehicles can be warned or its certificate can be revoked in accordance of reaction level.

Thus, various types of misbehavior can be detected by following these phases and appropriate reactions are decided according to reaction level.

IV. Evaluation and Results

The performance evaluation of a misbehavior detection system requires a suitable simulation scenario. Such simulation can be provided using VEhicles In Network Simulationsi (VEINS) [14] framework, which incorporates SUMO mobility simulator and OMNET++ network simulator. In order to evaluate the performance of proposed misbehavior detection framework, we have performed the simulation using VeReMi [10] dataset in Python programming language (using Scikit-learn). VeReMi dataset was generated using LuST SUMO network scenario [15] in VEINS framework. This labelled simulated dataset gives a wide range of internal attack implementation and traffic behaviors. The dataset comprises of a list of message logs for every vehicle and ground truth file defining the attacker's behavior. Message logs consist of speed vector, position vector, RSSI for each of the receivers, claimed transmission time, position and reception time [10]. Whereas, the ground truth file contains the sender ID, message ID, transmission time, speed vector, position vector and the type of attacker for each of the transmitted message. The dataset consists of the message logs for five different position forging attacks. These attacks are 1. Constant (Type 1), 2. Constant Offset (Type 2), 3.Random (Type 4), 4. Random Offset (Type 8), 5. Eventual Stop (Type 16). For the testing purpose, we have evaluated the performance of the proposed model only for Type 1 attack i.e. constant location attack in which the attacker transmits a fixed location in every BSM. The proposed framework is provided with flexibility by integrating SDN into VANET. SDN controller monitors the behavior of each vehicle in the network and keeps track of current vehicle density, attacker density and attacker's behavior.

For the simulation purpose, we have used the vehicle density network parameter n. We assume that SDN controller records the network density regularly and updates the infrastructure elements (RSC and vehicles) on the changes in the present vehicle density. The proposed model was simulated for two different vehicle density cases i.e. low vehicle density and high vehicle density. VeReMi dataset consists of message logs for 35-39 and 491-519 number of vehicles in case of low and high vehicle density scenario respectively. The dataset records the mean speed of 24.36m/s for vehicles in low density scenario and 12.81m/s for vehicles in high density scenario.

We assume that at each time t, the network region is divided into clusters according to RSC radio range. During the simulation for both vehicle densities, plausibility checks are performed and six features are extracted from these checks for the node-centric detection phase. As described in [9], first two features location plausibility and movement plausibility is calculated to examine the correctness of sender data and movement of sending vehicle respectively. Remaining four features define the vehicle behavior.

Plausibility check output i.e. plausibility score is determined on the basis of the predicted position of vehicles. The range for predicted vehicle position is dependent on the Confidence Interval (CI) for acceleration in both of the directions X and Y. This CI is calculated by observing all of the data transmitted in the network. Thus, CI has different values in case of different network density scenarios. Static algorithms cannot be exploited for misbehavior detection for all varying network density. Therefore we have used a local detection mechanism which is adjusted according to the network parameters provided by SDN controller.

For the advance detection, K-NN algorithm was used to detect the attacker among the legitimate one. On the basis of previously transmitted position based on Euclidean distance, K-NN analyzes the behavior of the data point. If the data point is farther away from its previous positions then it is labelled as an outlier. K-NN classifier was trained with the dataset for the two vehicle densities separately as they have varying CI and range of predicted positions of vehicles. These classifiers are exploited in real-time simulation for misbehavior detection according to the context of the network scenario updated by the SDN controller.

TABLE I
Attack detection results

Context	Precision	Recall
Low vehicle density	0.92	0.79
High vehicle density	0.95	0.99

As observed in Table I, two parameters, $precision$ and $recall$ are calculated to evaluate the performance in both the cases of network densities. $Precision$ gives the proportion of correctly detected as misbehaving out of all detected misbehaving messages and calculated as $TP/(TP + FP)$. If an attacker is detected as attacker then it is True Positive (TP). False Positive (FP) is a genuine vehicle detected as an attacker. Whereas $recall$ provide the proportion of correctly identified as misbehaving out of all received misbehaving messages and calculated as $TP/(TP + FN)$. False Negative (FN) is an attacker which is not detected as an attacker. K-NN performs the classification with a higher $precision$ and $recall$ value in both cases.

Figure 3 and Figure 4 shows the Receiver Operating Characteristics (ROC) curve by using K-NN for low and high vehicle density respectively. As shown in the ROC curve, the true positive rate remains higher whereas the false positive rate increases slightly with the increase in the number of interactions in case of both the densities. Thus, the proposed framework is adaptable to network changes (vehicle density in our simulation) and shows the best performance for all of the varying contexts.

V. Conclusion

VANET is susceptible to internal attacks that can disrupt the VANET services and threaten to the safety of VANET users.

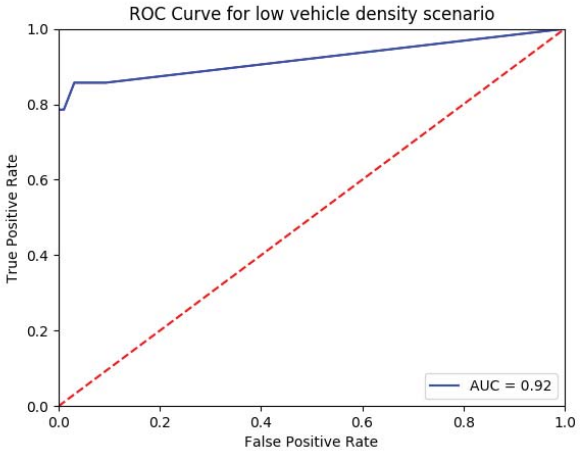

Fig. 3. ROC curve for low vehicle density scenario

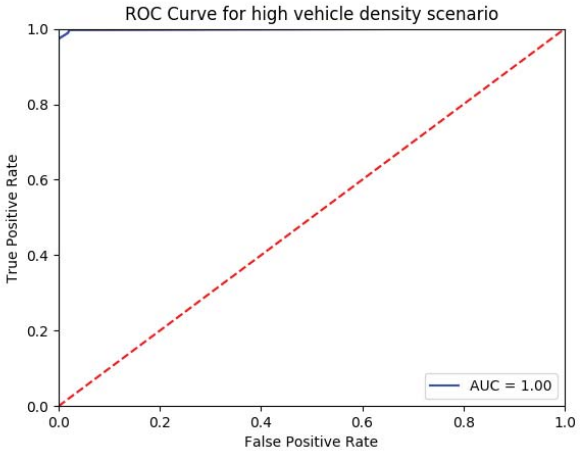

Fig. 4. ROC curve for high vehicle density scenario

In this paper, we have proposed a framework for misbehavior detection in SDN-based VANET that leverages the SDN characteristics. SDN capabilities make the detection mechanism adaptive to changes in the network context. We have evaluated the performance of the proposed work in two different network density scenarios for constant location attack. Results showed that the proposed framework has higher performance in terms of precision and recall. As a part of future work, we would construct a more adaptive detection framework that considers additional network parameters to provide the best detection performance. We would also implement the global detection phase and evaluate the performance of whole framework for other types of attacks too.

REFERENCES

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of network and computer applications*, vol. 37, pp. 380–392, 2014.

[2] I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro, and E. Cerqueira, "Towards software-defined vanet: Architecture and services," in *2014 13th annual Mediterranean ad hoc networking workshop (MED-HOC-NET)*, pp. 103–110, IEEE, 2014.

[3] R. W. van der 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, 2018.

[4] A. Boualouache, R. Soua, and T. Engel, "Sdn-based misbehavior detection system for vehicular networks," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–5, IEEE, 2020.

[5] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in vanet," in *International conference on advances in computing and communications*, pp. 644–653, Springer, 2011.

[6] R. Sultana, J. Grover, and M. Tripathi, "Security of sdn-based vehicular ad hoc networks: State-of-the-art and challenges," *Vehicular Communications*, pp. 100284, https://doi.org/10.1016/j.vehcom.2020.100284, 2020.

[7] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa, and P. Urien, "Simulation framework for misbehavior detection in vehicular networks," *IEEE Transactions on Vehicular Technology*, 2020.

[8] M. Kim, I. Jang, S. Choo, J. Koo, and S. Pack, "Collaborative security attack detection in software-defined vehicular networks," in *2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 19–24, IEEE, 2017.

[9] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in vanet," in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 564–571, IEEE, 2018.

[10] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "Veremi: A dataset for comparable evaluation of misbehavior detection in vanets," in *International Conference on Security and Privacy in Communication Systems*, pp. 318–337, Springer, 2018.

[11] A. Alioua, S.-M. Senouci, S. Moussaoui, H. Sedjelmaci, and A. Boualouache, "Software-defined heterogeneous vehicular networks: Taxonomy and architecture," in *2017 Global Information Infrastructure and Networking Symposium (GIIS)*, pp. 50–55, IEEE, 2017.

[12] J. Kamel, A. Kaiser, I. ben Jemaa, P. Cincilla, and P. Urien, "Catch: a confidence range tolerant misbehavior detection approach," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–8, IEEE, 2019.

[13] J. Kamel, I. B. Jemaa, A. Kaiser, and P. Urien, "Misbehavior reporting protocol for c-its," in *2018 IEEE Vehicular Networking Conference (VNC)*, pp. 1–4, IEEE, 2018.

[14] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata, "Veins: The open source vehicular network simulation framework," in *Recent Advances in Network Simulation*, pp. 215–252, Springer, 2019.

[15] L. Codeca, R. Frank, and T. Engel, "Luxembourg sumo traffic (lust) scenario: 24 hours of mobility for vehicular networking research," in *2015 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, IEEE, 2015.