Machine Learning-Based Detection of Data Replay and Data Replay Sybil Attacks for Vehicular Communication Networks

Owana Marzia Moushi[1], Chamath Gunawardena[1], Feng Ye[2], Rose Qingyang Hu[3], and Yi Qian[1]

[1]Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Omaha, NE, USA
[2]Department of Electrical and Computer Engineering, University of Wisconsin-Madison, Madison, WI, USA
[3]Department of Electrical and Computer Engineering, Utah State University, Logan, UT, USA

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622192

***Abstract*—A vehicular network is susceptible to various security flaws and attacks. Cryptographic techniques are used in vehicular networks but these alone cannot provide proper security to the network. Identifying various types of attacks is necessary to secure vehicular communication networks. This work is focused on both binary and multi-class attack detection in vehicular networks. A publicly available dataset, VeReMi-Extension is used to detect these attacks. This dataset has been reformulated to generate novel features aimed at detecting attacks in vehicular networks accurately. Machine learning-based methods have been applied to the reformulated dataset for the detection of attacks in vehicular networks. The extensive simulation results show that the proposed scheme can detect more than 99% attacks both for binary and multi-class scenarios which is an impressive performance to enhance the security in vehicular networks.**

***Index Terms*—Data replay attack, data replay Sybil attack, vehicular networks, machine learning, security**

I. Introduction

A vehicular communication network is a dynamic and advanced communication system where vehicles can communicate through vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), vehicle-to-infrastructure (V2I), and vehicle-to-network (V2N), collectively termed as vehicle-to-everything (V2X). In vehicular networks, vehicles are considered as mobile entities to exchange real-time data that are vulnerable to security flaws and different types of attacks [1] [2]. Previously, dedicated short-range communications (DSRC) were used for establishing the communications between vehicles and also with Road Side Units (RSUs) [3]. Enhancing and improving road safety is one of the important concerns for passengers and drivers [4]. More recently, another popular communication technology, namely, cellular communication technology is being leveraged to achieve better vehicular network connectivity [5].

To ensure a safe and efficient transportation system, a vehicular network requires every updated Basic Safety Message (BSM) to be communicated in real-time [6]. A BSM contains details about the vehicle such as its position, speed, acceleration, heading, message identity, and sender type information. Different types of cryptographic schemes are used in vehicular networks during sharing the BSM to enhance secure communications [7]. However, this scheme is suffering from a few security issues because of the open environment and the wireless connections of vehicular networks. A combination of a misbehavior detection system (MDS) and a cryptographic system in a vehicular network can create a robust method to effectively enhance the security of vehicular communications [1] [5]. An MDS can analyze the behaviors of the insider attacker vehicles and identify the attacks. In a vehicular network, a vehicle can broadcast false or fake alerts which will pose a safety threat to the drivers and passengers. For instance, a couple of vehicles can be within a group and share messages whereas an attacker vehicle can also be within that group. The attacker's vehicle can broadcast a fake alert message to indicate that another vehicle is braking. The legitimate vehicle can consider this alert message seriously and behave accordingly which can lead to an accident. If an MDS is installed appropriately inside a vehicle, it could detect the false message and broadcast this alert to enhance the safety of drivers and passengers [8] [9].

Though several research activities aimed at identifying misbehavior in vehicular networks, it remains a challenging problem to detect misbehaviors quickly and accurately because of high-speed mobility, dynamic connections, and extensive data of these networks [5]. One of the prominent research areas in all the fields is machine learning (ML) which is achieving great attention because of its capability to handle large volumes of data from heterogeneous devices. Its noteworthy capability is decision-making and detection. ML provides powerful tools to leverage the stored and generated data of vehicular networks in a better form to decide on the reformed structure of data [10] [11]. ML-based MDS can effectively identify data replay and data replay Sybil attacks in vehicular networks which are important to make the network trustworthy and reliable. These types of attacks threaten the security and safety of vehicular networks. In a data replay attack, the attacker retransmits a previous message to disrupt the network flow whereas in a data replay Sybil attack, the attacker follows the same process by creating multiple fake identities in the system. ML-based approaches can detect these types of misbehavior in vehicular networks to increase the security [1] [12] [13] [14].

978-1-7281-9054-9/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: Utah State University. Downloaded on December 26,2024 at 18:39:36 UTC from IEEE Xplore. Restrictions apply.

In this paper, we propose an ML-based scheme to detect both binary and multi-class attacks, namely, data replay and data replay Sybil attacks, in vehicular networks. A publicly available dataset, Vehicular Reference Misbehavior (VeReMi)-Extension [15], has been pre-processed and multiple features have been proposed from the given information of the dataset to identify misbehavior. To detect these attacks, MDS has been installed on each vehicle aimed at identifying misbehaving vehicles. By using the proposed and reformulated features, MDS will detect misbehaving vehicles that are replaying the BSM multiple times to generate data replay and data replay Sybil attacks in vehicular networks.

The rest of the paper is structured as follows. Section II discusses the existing work to detect replay-based attacks in vehicular networks. Section III presents a comprehensive discussion about data replay and data replay Sybil attacks. Section IV illustrates the model of the current vehicular network system. Section V presents the process of dataset formulation, proposed features, and model training of this work. Section VI shows the performance results of the proposed scheme by comparing it with the previous work. Section VII gives the conclusion and future work.

II. Literature Review

This section discusses the existing schemes for detecting data replay and data replay Sybil attacks in vehicular networks. These attacks have not been a well-studied research topic yet and a few studies have endeavored to detect those which are presented here.

In [5], the authors used ML-based methods to effectively identify data replay attacks in vehicular networks by focusing on two different approaches. The first approach extracted the top 23 features from the VeReMi-Extension dataset by removing the overlapping vehicles from the test dataset. In the second one, senderID, messageID, and senderPseudo features have been omitted and the rest of the features were used to train the model on the dataset for behavior analysis. Their methods got an accuracy of 99.72%, 99.73%, and 99.78% for lower, higher, and varying traffic densities, respectively.

In [15], the authors created a novel dataset named VeReMi-Extension to facilitate 19 different attacks in vehicular networks for various traffic densities. They have successfully detected both data replay and data replay Sybil attacks separately along with other types of attacks by using consistency and plausibility checks. Their model can detect 93.07% and 93.93% data replay attacks in case of lower and higher traffic densities, respectively. The detection rate of data replay Sybil attack is 79.48% and 80.11% for lower and higher traffic densities, in order.

The authors of [13] applied both ML and deep learning (DL)-based models on the VeReMi-Extension dataset to detect all 19 different attacks as shown in [15]. They proposed three distinct methods to extract the important features from the dataset and subsequently added ML and DL-based classification algorithms to detect these attacks in vehicular networks. They presented the result only for higher traffic density since the analysis shows that varying traffic density and time have no impact on the detection rate. Precision and recall were used for performance evaluation and the DL-based model achieved 65.98% precision and 6.53% recall for a data replay attack while 63.11% precision and 6.81% recall in case of a data replay Sybil attack. In contrast, the ML-based approach provides better results with 52% precision and 47% recall for the data replay attack and 73% precision and 72% recall in the case of a data replay Sybil attack. The lower recall of the DL-based approach shows that their DL-based method cannot effectively identify the attack.

In [14], the authors proposed a multi-class Sybil attack detection scheme for vehicular networks with a specific focus on data replay Sybil attack, grid Sybil attack, DoS random Sybil attack, and DoS disruptive Sybil attack. They generated data from the Luxembourg traffic scenario. They used BSM, map, and sensor data to formulate multi-dimensional features and subsequently applied ML-based approaches for detecting multi-class attacks. Their method can identify the location of the road where the attack happened without focusing on legitimate vehicles as a reference. They have rigorously tested the model for different attackers and traffic densities. Their model performs well and gives an overall accuracy of 97.69%. While their model exhibits remarkable accuracy and precision, their recall is lower at all times compared to the accuracy and precision for data replay Sybil attack.

In [16], the authors generated a dataset to detect data replay and Sybil attacks. To construct the dataset, the authors utilized SUMO, Veins, Omnet++, and OpenStreetMap software. They introduced their algorithm by leveraging the key factors - timestamps and velocity to identify these attacks. Their accuracy rate is 92% to find out these attacks. Though they didn't utilize the VeReMi-Extension dataset or ML-based approaches, their approaches are informative to detect data replay and data replay Sybil attacks since we are working on detecting similar types of attacks in vehicular networks.

In [12], the authors proposed an algorithm to detect four different types of Sybil attacks in vehicular networks. They generated a dataset from Luxembourg City and applied ML-based approaches to detect Sybil attacks. A three-phase approach was used where the first phase checked if there were any misbehaving vehicles existed or not, the second phase tried to link all the pseudonyms coming from the same type of vehicles, and finally, the third phase used those links to detect Sybil attacks. Their model accuracy is lower than 90% to detect the data replay Sybil attack in the linkage phase.

III. Attack Models

This section gives a brief overview of the data replay and data replay Sybil attacks in vehicular networks. The purpose is to get familiar with these attacks so that we can make better tactics to detect them from vehicular networks.

A. Data Replay Attack

In a data replay attack, an attacker vehicle sniffed the message that had been played before from a nearby legitimate

Authorized licensed use limited to: Utah State University. Downloaded on December 26,2024 at 18:39:36 UTC from IEEE Xplore. Restrictions apply.

vehicle. Later, the attacker's vehicle rebroadcasts the same message without changing any information about the vehicle's status. It only changes the sender information which is done

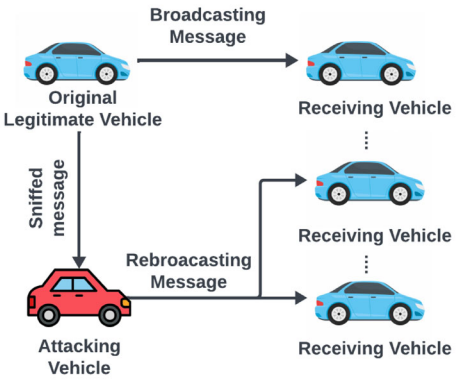

Fig. 1. Data Replay Attack

through signing a private key. An attacker's vehicle replayed the message to make the road busy and congested. In addition, by replaying the same information as a legitimate vehicle, it is becoming authenticated and later it will broadcast wrong information again [5] [13] [15] [16]. Fig. 1 shows one example where the attacking vehicle is sniffing and replaying the message.

B. Data Replay Sybil Attack

In a data replay Sybil attack, an attacker copied the legitimate BSM from a nearby legitimate vehicle and also created numerous fake identities in the network. Then, the attacker controls each of the fake identity vehicles and replays copied BSM by the fake identity vehicles. The major challenge for

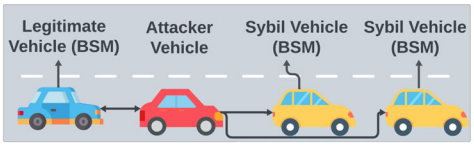

Fig. 2. Data Replay Sybil Attack

this attack is to detect the difference between a legitimate vehicle and an attacker-controlled vehicle. There is a chance that a legitimate vehicle can be identified as a fake identity vehicle [12] [13] [15] [16]. Fig. 2 is an example where the attacker vehicle copied a BSM from a legitimate vehicle and later broadcasts it through multiple fake identity vehicles.

IV. Vehicular Network Model

The vehicular network model considered for this study is shown in Fig. 3. The major components of a vehicular network are RSU, Certificate Authority (CA), On Board Unit (OBU), and vehicles themselves. Every CA works as a host for multiple RSUs where each RSU is responsible for the vehicular communications within that specific area. Each vehicle has one OBU installed inside, which can communicate seamlessly with other vehicles and RSUs. Before joining the network, each vehicle is required to be registered through a CA to get its identity credentials such as senderID, public keys, and private keys. Every vehicle uses its identity and credentials to broadcast BSM and it keeps the identity for multiple days to communicate with other vehicles and the RSUs. Every

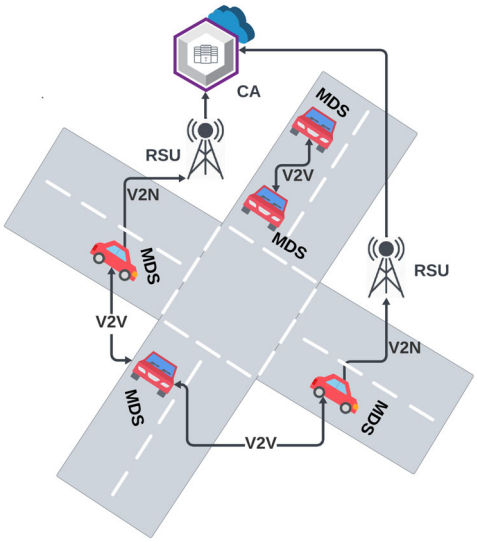

Fig. 3. Vehicular Network Model

vehicle has also installed one additional MDS with the OBU to effectively identify the misbehavior of the nearby vehicles. Since we are focusing on replay-based attacks, a vehicle is considered malicious if it is replaying the messages that are already broadcasted. A vehicle uses its OBU and MDS separately which is also supported by the trained ML-based models to scrutinize every BSM for effectively identifying malicious vehicles. Whenever the MDS of the vehicle finds any misbehaving vehicle, it reports this issue to the nearest RSU. After that, the RSU sends this message to the CA and provides the information they received from the MDS. The CA checks the information and categorizes it as an attacker or legitimate vehicle based on the report they receive. If the vehicle is an attacker, then CA takes the corresponding action which may involve revoking their credentials [1] [5].

V. Dataset

This work is focused on the publicly available VeReMi-Extension dataset [15]. This dataset was chosen because it is a standard dataset in this field to detect the selected misbehavior and seamlessly align with our objective. In this dataset, the authors provided a simulated result for 19 different types of attacks. We have used two specific types from the dataset, namely, data replay and data replay Sybil attacks. Each simulated dataset contains message logs per vehicle along with a corresponding ground truth file. Both the attacks yield three simulated results in data files and one of them does not have any corresponding ground truth file. This study does not consider that simulated file and focuses on the other two files

Authorized licensed use limited to: Utah State University. Downloaded on December 26,2024 at 18:39:36 UTC from IEEE Xplore. Restrictions apply.

which have corresponding ground truth files. Among the other two files, one file contains 1005 message logs; one message log is for ground truth and each of the other 1004 message logs is for each vehicle. Similarly, the other simulated file contains 686 logs where one of the logs is for the ground truth message and each of the other 685 is for each vehicle's message log.

A. Dataset Preprocessing

The dataset has been pre-processed before incorporating it into the model. The ground truth file contains information about the vehicle such as type, send time, sender, sender pseudo, messageID, position and position noise, speed and speed noise, acceleration and acceleration noise, and heading and heading noise. Among all the information, the features, namely, position and position noise, speed and speed noise, acceleration and acceleration noise, and heading and heading noise are given in $x, y,$ and z coordinates. In this dataset, the z coordinates values for all the different features are set as 0 and we removed this specific coordinate value from the reformulated dataset. In the BSM, they included receive time as an additional feature. The GPS message contains the receive time and all other information without the sender's information and message identity. The ground truth file has been considered as a reference to label the legitimate and attacker vehicles. To label this, the message identity from the vehicle's message log has been compared to the ground truth file. If any of the message IDs from the BSM do not match with the ground truth's message ID, then we label it as an attacker vehicle. In addition, if any message ID of the BSM matches with the ground truth but the other values do not match, then it is also labeled as an attacker vehicle. This work has considered the GPS data as well and they are labeled as legitimate vehicles. Since the GPS data does not have the sender's information and message identity, those values are assigned as 0. The message type has also been dropped from the dataset to keep only the useful features in the regenerated dataset.

B. Proposed Features

To formulate this model and get better performance, we have proposed a completely new feature and reformulated some of the existing features. This section describes those features.

- **Time Difference:** In a data replay attack, an attacker vehicle sniffs an actual message and replays it later which takes some time to complete this process. This work has proposed a completely new feature named "Time Difference" which is getting the time difference between the GPS and BSM data. Whenever it gets the first GPS message, this model sets them as initial until getting the next BSM data. It calculates the time difference between the previous GPS and subsequent BSM's receive time which gives a huge improvement to this work. The authors of [2] also used GPS data to create features for their model.
- **Standard Deviation:** Another important feature, namely, standard deviation has been included in this study. The standard deviation of the speed and speed noise, heading and heading noise, and acceleration and acceleration noise have been calculated by using Eq. 1 and added to the dataset. In addition, the actual values for those features have been dropped since it has been reformulated as new ones. The reason for considering the standard deviation is to take the distribution of those features for this work.

$$\sigma = \sqrt{\frac{\sum(x_i - \mu)}{N}} \tag{1}$$

where σ is the standard deviation, μ is the mean, and x_i is each data point from the whole data and N is the total number of data points.

C. Training the Model

ML-based approaches have been used to train the dataset in this work. Multiple ML models have been used in this study to effectively identify the attacker vehicles. A dataset has been split into the training and testing datasets where 80% is used to train the dataset and the next 20% is used to test the dataset. By using the proposed features and dropping the unused ones, the model is trained to find the attacker vehicles. Then, finally, the training dataset has been used on the testing dataset to make the prediction. To train this model, various ML-based models such as Decision Tree (DT), Random Forest (RF), Extra Tree Classifier (ET), and K-Nearest Neighbors (KNN) have been used and they are also applied to make predictions on the testing dataset. Additionally, Ensemble Voting has been applied, utilizing three different individual models more specifically DT, ET, and RF, with a focus on soft voting. In soft voting, the weighted average probability of each base model is used to calculate the weighted probability for making the final prediction. This approach gives more accurate results than any single method because it can reduce overfitting, increase accuracy, and enhance robustness.

VI. Experimental Results and Analysis

This section presents the experimental results of this work to detect the data replay and data replay Sybil attacks in both binary and multi-class classification-based approaches. The VeReMi-Extension [15] dataset has two different traffic densities 1) lower traffic (14 h - 16 h), 2) higher traffic (07 h - 09 h), for all 19 types of attacks. In addition, one test bench is included by combining all the attacks throughout the day (0 h - 24 h). This work is focused on the lower traffic section of the dataset since traffic density does not impact the detection rate [13].

A. Evaluation Metrics

To evaluate this work, accuracy and F1 scores have been used from the confusion matrix which is shown in Table I. Since precision and recall are used to compute the F1 score, they are not presented here separately.

- **Accuracy** represents the ratio between correctly predicted observations over the total observations as shown in Eq. 2.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{2}$$

Authorized licensed use limited to: Utah State University. Downloaded on December 26,2024 at 18:39:36 UTC from IEEE Xplore. Restrictions apply.

TABLE I
CONFUSION MATRIX

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

where TP correctly finds the positive values, TN correctly identifies negative values, FP incorrectly labels negative values as positive, and FN incorrectly represents positive values as negative.

- **Precision** represents the ratio between the correct prediction of the malicious vehicles and the total predicted number of malicious vehicles as shown in Eq. 3.

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

- **Recall** is the ratio between the correct prediction of the malicious vehicles over the total actual number of malicious vehicles as shown in Eq. 4.

$$Recall = \frac{TP}{TP + FN} \tag{4}$$

- **F1 Score** presents the weighted mean value of precision and recall by using Eq. 5.

$$F1\ Score = \frac{2 \times Recall \times Precision}{Recall + Precision} \tag{5}$$

B. Results

This section illustrates the performance of this study to detect both binary and multi-class attacks in vehicular networks. The data replay attack detection results are shown in Table II. All the performance values of the ML-based models for the detection of the data replay attack have been listed here. The performance of DT, ET, and RF models is approximately equal both for accuracy and F1 score. All the ML-based models have successfully identified the data replay attack more than 99% except the KNN model where the neighbor is selected as 3. The ensemble voting has detected 99.76% attack accurately where F1 score is 99.53%. This highlights that the performance of the proposed scheme has been improved by combining multiple models.

TABLE II
DATA REPLAY ATTACK DETECTION RESULTS IN VEHICULAR NETWORK

Models	**Accuracy**	**F1 Score**
DT	0.9974	0.9949
ET	0.9971	0.9944
RF	0.9973	0.9947
KNN	0.9422	0.8860
Ensemble - Voting	0.9976	0.9953

The performance of the ML-based data replay Sybil attack detection is shown in Table III. ML-based methods such as DT, ET, RF, and KNN-3 give approximately the same result both for accuracy and F1 score. All the ML-based models have successfully identified the data replay Sybil attack of more than 99%. We got the best result from the ensemble voting where the accuracy rate is 99.78% and F1 score is 99.56%. The ensemble voting provides the best result as achieved in the data replay attack detection as well.

TABLE III
DATA REPLAY SYBIL ATTACK DETECTION RESULTS IN VEHICULAR NETWORK

Models	**Accuracy**	**F1 Score**
DT	0.9977	0.9954
ET	0.9977	0.9955
RF	0.9977	0.9955
KNN	0.9973	0.9948
Ensemble - Voting	0.9978	0.9956

Finally, we have detected the data replay and data replay Sybil attacks together in vehicular networks. We have used a multi-class classifier to detect these attacks together. The overall performance for the detection of multi-class attacks is shown in Table IV. As we have discussed previously, the best result is achieved from the ensemble voting classifier. Similar to the data replay attack detection, DT, ET, and RF show approximately equal results both for accuracy and F1 score except for KNN-3. The best accuracy rate is 99.77% and the F1 score is 99.65% for the multi-class classifier.

TABLE IV
MULTI-CLASS (DATA REPLAY AND DATA REPLAY SYBIL ATTACK) DETECTION RESULTS IN VEHICULAR NETWORK

Models	**Accuracy**	**F1 Score**
DT	0.9974	0.9961
ET	0.9976	0.9963
RF	0.9975	0.9962
KNN	0.9705	0.9547
Ensemble - Voting	0.9977	0.9965

C. Analysis and Discussions

In this section, we compare the proposed scheme with the existing work for the detection of data replay and data replay Sybil attacks. Since the VeReMi-Extension dataset is comparatively new than the VeReMi dataset [17], we have a limited number of previous works that are exactly focused on this dataset. In addition, the detection of data replay and data replay Sybil attacks have not been studied extensively. We have separately compared each attack and represented them in tabular form. From Table V, we can see that our result gives a much better performance than [13] and [15]. However, the accuracy of our scheme is higher than [5] while the F1 score is lower. The attacker density is an important reason behind this as mentioned in [15]. In [5], the attacker density is 30% and the legitimate vehicles are 70% whereas we have 25.45% attackers and 74.55% legitimate vehicles. There is a difference in the attacker density because we have considered both GPS and BSM data while they only considered the BSM data. For lower attacker densities, our model has better accuracy. Similarly, if the attacker density is increased, our model will give better performance. To confirm that we have analyzed

Authorized licensed use limited to: Utah State University. Downloaded on December 26,2024 at 18:39:36 UTC from IEEE Xplore. Restrictions apply.

the model with only one simulation file (1005) as an example, with a specific focus on the data replay attack. This gives 99.98% accuracy and 99.97% F1 score by applying an ML-based DT model where the attacker density is 26.15% and the legitimate vehicle is 73.85%. Therefore, if the attacker density increases the performance of our model will improve. Additionally, though the authors of [14] and [16] did not use the same dataset, our model still gives better performance than theirs.

TABLE V
DATA REPLAY ATTACK COMPARISON WITH THE PREVIOUS WORK

Approach	Accuracy	F1 Score
Proposed	0.9976	0.9953
Paper [15]	0.9307	0.8798
Paper [13]	-	0.4937
Paper [5]	0.9972	0.9974

The proposed scheme's data replay Sybil attack detection also performs better than the previous work as shown in Table VI. The performance of this work is far better than [13] and [15]. The authors of [13] didn't add any accuracy results both for the data replay and data replay Sybil attack. In [12] and [14], the authors didn't use the VeReMi-Extension dataset and got around 90% and 97.79%accuracy, respectively to detect data replay Sybil attack which is lower than our result. At last, to the best of our knowledge, we have first worked on the multi-class detection of data replay and data replay Sybil attacks and the performance of the model is much better which is more than 99%.

TABLE VI
DATA REPLAY SYBIL ATTACK COMPARISON WITH THE PREVIOUS WORK

Approach	Accuracy	F1 Score
Proposed	0.9978	0.9956
Paper [15]	0.7948	0.5235
Paper [13]	-	0.7250

VII. CONCLUSION

Vehicular network security is crucial to protect the drivers and passengers' lives and also for the safety of the road. Cryptographic mechanisms alone can not make a vehicular network secure. The incorporation of MDS with cryptographic systems can enhance the security of a vehicular network. Among all of the attacks, data replay and data replay Sybil attacks are dangerous as they are insider attacks and difficult to detect. In this study, we have applied ML-based methods to detect both of these attacks in binary and multi-class scenarios from vehicular networks. A publicly available dataset, VeReMi-Extension, has been utilized to detect these attacks and our proposed and reformulated features have given better performance than the existing works. Our model can detect around 99.76% and 99.78% binary attacks for the data replay and data replay Sybil attacks, respectively, and 99.77% multi-class attacks which is an improvement on the existing works. For future studies, we will work on detecting other types of attacks to make the vehicular networks more secure. We will focus on both the single and multi-class detection of various types of attacks in vehicular networks.

ACKNOWLEDGMENT

This work was partially supported by the National Science Foundation under grants CNS-2008145, CNS-2007995, CNS-2319486, CNS-2319487, CNS-2344341.

REFERENCES

[1] S. Gyawali and Y. Qian, "Misbehavior Detection using Machine Learning in Vehicular Communication Networks," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2019.
[2] S. Ercan, M. Ayaida, and N. Messai, "New Features for Position Falsification Detection in VANETs using Machine Learning," in *ICC 2021 - IEEE International Conference on Communications*, pp. 1–6, 2021.
[3] Y. Qian and N. Moayeri, "Design of secure and application-oriented vanets," in *VTC Spring 2008 - IEEE Vehicular Technology Conference*, pp. 2794–2799, 2008.
[4] A. Sharma and A. Jaekel, "Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 1–14, 2022.
[5] A. Kumar, M. A. Shahid, A. Jaekel, N. Zhang, and M. Kneppers, "Machine learning based detection of replay attacks in VANET," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–6, 2023.
[6] H. Peng, L. Liang, X. Shen, and G. Y. Li, "Vehicular Communications: A Network Layer Perspective," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1064–1078, 2019.
[7] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.
[8] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 779–811, 2019.
[9] M. Amoozadeh, A. Raghuramu, C.-n. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015.
[10] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine Learning Paradigms for Next-Generation Wireless Networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 98–105, 2017.
[11] H. Ye, L. Liang, G. Ye Li, J. Kim, L. Lu, and M. Wu, "Machine Learning for Vehicular Networks: Recent Advances and Application Examples," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 94–101, 2018.
[12] J. Kamel, F. Haidar, I. B. Jemaa, A. Kaiser, B. Lonc, and P. Urien, "A Misbehavior Authority System for Sybil Attack Detection in C-ITS," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pp. 1117–1123, 2019.
[13] O. Slama, B. Alaya, S. Zidi, and M. Tarhouni, "Comparative Study of Misbehavior Detection System for Classifying misbehaviors on VANET," in *2022 8th International Conference on Control, Decision and Information Technologies (CoDIT)*, vol. 1, pp. 243–248, 2022.
[14] Y. Chen, Y. Lai, Z. Zhang, H. Li, and Y. Wang, "MDFD: A multi-source data fusion detection framework for Sybil attack detection in VANETs," *Computer Networks*, vol. 224, p. 109608, 2023.
[15] J. Kamel, M. Wolf, R. W. van der Hei, A. Kaiser, P. Urien, and F. Kargl, "VeReMi Extension: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2020.
[16] N. R, N. Chaitanya, N. S. M, and N. Vineeth, "Implementation of a Methodology for Detection and Prevention of Security Attacks in Vehicular Adhoc Networks," in *2020 IEEE International Conference for Innovation in Technology (INOCON)*, pp. 1–6, 2020.
[17] R. W. Van Der Heijden, T. Lukaseder, and F. Kargl, "Veremi: A dataset for comparable evaluation of misbehavior detection in vanets," in *Security and Privacy in Communication Networks: 14th International Conference, SecureComm 2018, Singapore, Singapore, August 8-10, 2018, Proceedings, Part I*, pp. 318–337, Springer, 2018.

Authorized licensed use limited to: Utah State University. Downloaded on December 26,2024 at 18:39:36 UTC from IEEE Xplore. Restrictions apply.