Machine Learning Based Approach to Detect Position Falsification Attack in VANETs

Pranav Kumar Singh(✉), Shivam Gupta, Ritveeka Vashistha, Sunit Kumar Nandi, and Sukumar Nandi

Department of Computer Science and Engineering, Indian Institute of Technology, Guwahati 781039, India
snghpranav@gmail.com, sunitnandi834@gmail.com, {shivam.gupta,ritveeka,sukumar}@iitg.ac.in

Abstract. VANETs is a major enabling technology for connected and autonomous vehicles. Vehicles communicate wirelessly with other vehicles, sensors, humans, and infrastructure, thereby improving decision making based on the information received from its surroundings. However, for these applications to work correctly, information needs to be authenticated, verified and trustworthy. The most important messages in these networks are safety messages which are periodically broadcasted for various safety and traffic efficiency related applications such as collision avoidance, intersection warning, and traffic jam detection. However, the primary concern is guaranteeing the trustworthiness of the data in the presence of dishonest and misbehaving peers. Misbehavior detection is still in their infancy and requires a lot of effort to be integrated into the system. An attacker who is imitating "ghost vehicles" on the road, by broadcasting false position information in the safety messages, must be detected and revoked permanently from the VANETs. The goal of our work is analyzing safety messages and detecting false position information transmitted by the misbehaving nodes. In this paper, we use machine learning (ML) techniques on VeReMi dataset to detect the misbehavior. We demonstrated that the ML-based approach enables high-quality detection of modeled attack patterns. We believe that the ML-based approach is a feasible and effective way of detecting such misbehavior in a real-world scenario of VANETs.

1 Introduction

Vehicular ad-hoc networks (VANETs) applications have great potentials to reduce the number of road accidents, diminish the carbon footprint, improve the traffic efficiency, and enhance the driving comfort and occupant's experience [1]. However, benefits usually come with challenges. Dealing with security threats such as fake data injections, messages alteration, replay attacks from insider attackers, and detecting such misbehaviors are the most significant challenges. Since the vehicular network is highly dynamic, the communicating vehicles are

S. Nandi et al. (Eds.): ISEA-ISAP 2018, CCIS 939, pp. 166–178, 2019.
https://doi.org/10.1007/978-981-13-7561-3_13

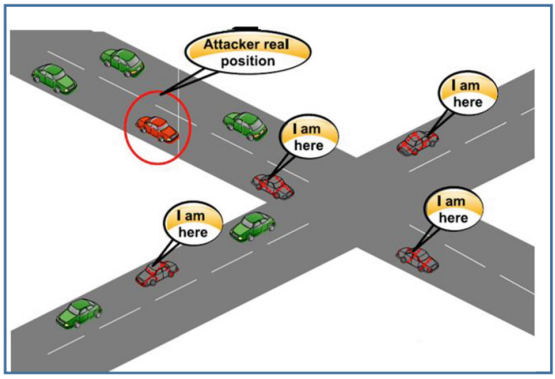

Fig. 1. Misbehavior in VANETs: position falsification

usually strangers and cannot fully trust each other. The problem becomes more dangerous when there are misbehaving/dishonest peers exist in the network. These peers may disseminate false/fake messages on purpose to gain something or to disturb normal functionalities.

Figure 1 demonstrates a scenario of position falsification attacks in VANETs [2]. Here, the misbehaving node uses the knowledge of the protocol semantics and create "ghost vehicles" in a particular road segment by broadcasting false position information in safety messages. In VANETs, the critical safety applications need to have reliable position information about its neighboring peers; thus, position falsification attack can create serious issues for road safety. Such attacks may also affect reliability for packet forwarding and lower the user acceptance of the system.

The public key infrastructure (PKI) is one of the highly recommended and used security framework. PKI facilitates the creation, management, distribution and revocation of keys and digital certificates for the proper and secure functioning of the system [3]. In the USA, Security Credential Management System (SCMS) is a leading candidate for the vehicular communication security which is based on PKI with unique features [4]. This security architecture was proposed by National Highway Traffic Safety Administration (NHTSA) for the vehicular network. The similar architecture was defined by European Telecommunications Standards Institute (ETSI) in Europe for intelligent transportation system (ITS). The specifications of these architecture are given in IEEE 1609.2 [5] and ETSI TS 102 940 [6] standards, respectively. However, the authenticity and verification process of these systems are not sufficient to guarantee the trustworthiness of the received message. Dealing with inside attackers or compromised entity and detection of any misbehaviors in the communication process are some of the biggest challenges of these security architectures.

Various data-centric and node-centric mechanisms for misbehavior detection can be found in the literature [7,8], however, most of them have their own set of challenges such as delay in detection, communication overhead, oversampling

and cascading, etc. Machine Learning (ML) can be one of the potential solutions to it. ML-based paradigm allows us to build models that can help us to detect any unexpected behavior based on its learning. This data-driven mechanism can allow the onboard unit (OBU) of the vehicle to learn various data-centric relationship and detect any misbehavior in the vehicular plane of the VANETs. Thus, we employ the reliable predictive power of the supervised learning to predict a category whether each incoming message sample is correct or false based on the training. To demonstrate the effectiveness of the approach, we use the Vehicular Reference Misbehavior Dataset (VeReMi) [9] and focus on a specific attack instead of considering a wide range of attacks.

The rest of this paper is organized as follows. In Sect. 2, we discuss related works. Section 3 provides an overview of the system, communication, and adversary models. Section 4 describes details of machine learning mechanisms used in this work. In Sect. 5, we discuss the results obtained, and finally, we conclude our work in Sect. 6.

2 Related Work

In SCMS, the misbehavior detection (MD) is defined as the "process of identifying devices that are either malfunctioned or misbehaving" [4]. It requires two types of detection: (1) Local MD in vehicles to identify anomalies and to report this by devices to the SCMS, and (2) Global MD by the SCMS to analyze the reports of misbehavior and to decide which devices to revoke. However, the implementation of these MD processes for PKI frameworks in the USA and Europe is still in its research phase. In [9], the authors define misbehavior detection process as follows: "the lack of correctness in authentic messages is referred to as misbehavior detection."

PKI based cryptographic approach has already shown its efficiency in handling attack attempts from outside and unauthorized attackers. However, dealing with attacks or misbehavior from insider remains the biggest challenge to be addressed. The MD approach deal with inside attackers where PKI-based security fails. To this end, various mechanism have been proposed, which are listed in some of the surveys [7,8,10–13].

These solutions are based on various mechanism such as probabilistic approach [14], threshold-based [15], holistic approach [16], cooperative trust [17], game-theoretic [18], Kalman filter [19], extended Kalman filter [20], Bayesian Inference [21] etc. However, research using one of the strongest contenders for misbehavior detection, machine learning are much more deficient. We found few good studies [22–26] in which authors have proposed ML-based solutions to detect misbehavior in VANETs.

In [22], the authors proposed an ML-based approach to classify the behavior of the node, i.e. whether the node is honest or malicious. Authors implemented various types of misbehaviors by modifying information present in the propagated messages and used Naive Bayes, J-48, IBK, Random Forest and Ada Boost1 classifiers to classify the behavior. However, in their position forging

attack, the attacker changes its ID randomly not the position. Kang et al. [23] proposed a deep neural network (DNN) based novel intrusion detection system (IDS) to detect attacks in a controller area network (CAN) network. In this work, the authors emphasize on the in-vehicle system rather than inter-vehicle communication. In the same line of thought, Loukas et al. [24] have proposed intrusion detection using deep learning to detect cyber-physical attacks inside the vehicle. However, their approach is cloud-based and consider attack vectors of the in-vehicle system only. Similarly, Taylor et al. [25] proposed Long Short-Term Memory (LSTM) neural network based anomaly detector to detect CAN bus attacks. This work also considers in-vehicle system vulnerabilities due to which CAN bus can be exploited. Ali et al. [26] proposed an intrusion detection system (IDS) to detect grey hole and rushing attacks in a vehicular network. The authors used both Support Vector Machines (SVM) and Feed Forward Neural Networks (FFNN) for attack detection.

To sum up this section, we see that there are only two good studies available that have used ML-based approach to detect inter-vehicle communication attacks. However, we believe that more such contributions are required because machine learning has great potential to address such issues in VANETs. To this end, our proposal is one such contribution.

3 Models: System, Communication and Adversary

3.1 System Model

As shown in Fig. 2, a VANET system architecture consists of three planes: Vehicular Plane, roadside unit (RSU) plane and Service plane.

Vehicular Plane. In the VANETs, the OBU of the vehicle has wireless connectivity options and a navigation option using Global Positioning System (GPS). Vehicles can communicate with all other devices equipped with wireless communication systems in their proximity such as pedestrians, other vehicles, RSUs, etc. Such type of communication is also referred to as Vehicle-to-Everything Communication (V2X).

RSU Plane. The fronthaul of the RSUs is wireless communication that provides connectivity with vehicles, which can be either Vehicle-to-Infrastructure (V2I) or I2V mode. The backhaul connectivity of RSUs are wired, which is connected to the gateway via switches and routers for packet forwarding to the service plane. Thus, RSUs facilitates communication between the vehicular plane and the services plane.

Service Plane. Various services in this plane can be of type Internet, payment, infotainment, traffic-related, etc. The requests generated by vehicles in the vehicular plane reach to the service plane via V2I connectivity and services are provided via the I2V mode of communication. The PKI-based certificate authority (CA) for VANETs is also deployed at the services plane.

Fig. 2. VANET architecture

3.2 Communication Model

The Dedicated Short Range Communication (DSRC) is key radio access technology for V2V communication, specially designed for VANETs and standardized as IEEE 802.11p [27]. In the USA, 75 MHz frequency has been allocated to DSRC in 5.9 GHz frequency band. As shown in Fig. 3, the allocated spectrum is divided into seven channels of 10 MHz widths each. It supports data rates up to 27 Mbps (with 10 MHz) and can transmit up to 1000 m.

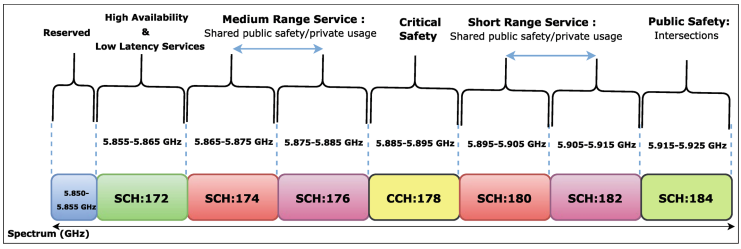

Fig. 3. DSRC frequency allocation in the USA for VANETs

Another very popular and emerging technology for VANETs is cellular-V2X (C-V2X), which is in its advancement phase. For V2I/I2V connectivity vehicles can use any available wireless access technology such as DSRC, Wi-Fi, mmWave, and LTE-A to which they are subscribed/authorized for access.

In the USA, Basic Safety Message (BSM) are defined in wireless access in vehicular environments (WAVE) protocol stack. BSM is periodically broadcasted (at 100 ms interval) over DSRC and contains information such as position, speed, direction, dimensions, and a pseudonym identifier to temporarily identifies the sender.

3.3 Adversary Model

In this work, we focus on an internal attacker that modify BSM to generate its false position and broadcast over DSRC. This malicious behavior is also known as position falsification attack.

As shown in the vehicular plane of the Fig. 3, the vehicle can overwhelm false information near intersections and create confusion for vehicles, which can severely affect critical safety applications of neighboring nodes. Since the message is from an insider, it gets accepted for processing by receiving vehicles. Thus, a wide variety of safety-related applications may get affected. Table 1 lists the types of attack modeled (parameters used) in the VeReMi dataset.

Table 1. Adversary parameters

Attack type	Description
Constant	Transmits a forged message with fixed position (pre-configured)
Constant offset	Transmits a forged message with fixed position by adding pre-configured offset
Random	Transmits a forged message with random position values from the simulation area
Random offset	Transmits a forged message with random position in a pre-configured rectangle around the node
Eventual stop	The vehicle behaves normally for a specified interval and then transmits the current position repeatedly

4 Proposed ML-Based Detection

In this section, we discuss our approach that includes ML-based models used, dataset, and feature description.

4.1 Machine Learning Models

Support Vector Machines (SVM). SVM is a supervised learning algorithm which is capable of solving both classification or regression challenges. However, it is more commonly used in classification problems. On a given training dataset

X, Y where X represents an input vector with n features and Y represents output data points are plotted on an n-dimensional plane with ith feature expressed as ith dimensional. Dataset is normalized to range 0 to 1 so that every feature are treated equally in the model and coefficients are not scaled differently according to the features magnitude. SVM tries to find a hyperplane to differentiate points into classes, and among different possible classification hyperplanes, it tries to find one which generalizes better to unseen test data by maximizing margin with the closest points.

Out of the whole dataset, only a few among them are close points, and hence only a subset of training points are required in actual classification process and needed to be kept in main memory which makes SVMs very efficient. SVM is mainly a 2-way Binary classifier, but it can be used for multiclass classification as well. In this paper, $|C|$ one-versus-rest binary classifiers are used to predict the class which gives maximum margin. Another strategy could be to use one-versus-one binary classifiers with all possible pairs of classes. At prediction time, class that is predicted by $(|C|(|C|+1))/2$. If the dataset is not linearly separable, then SVM transform these data points to a higher dimension using kernels such that data is separable by a hyperplane in the higher dimension. We used Radial basis function (RBF) kernel in our model, which is given by the following equation:

$$K(x, x') = exp(-||x - x'||^2/2\sigma^2) \tag{1}$$

Where $||x - x'||^2$ is the Euclidean distance between the two feature vector, original feature vector and feature vector with a higher dimension.

Logistic Regression. Logistic Regression is one of the basic algorithms to predict an classifying problem. The prediction is made using the logarithm of the "estimated odds of target variable". Given X as input vector, estimated probability is $p = 1/1 + e^{-(c+bX)}$. We have tried it by taking categorical features in one-hot representation.

4.2 VeReMi Dataset

The purpose of using the dataset is to have an initial baseline on which our detection mechanisms can be applied. We use open source dataset, which is made available for research studies. Use of existing dataset reduces the time required to perform simulation studies and makes things easier for us to apply the approach.

We used the VeReMi dataset [9] to train and test our models. This dataset is used as a reference for comparative studies between different ML-based misbehavior detection approach in VANETs. The dataset is based on Luxembourg traffic scenario (LuST) introduced by Codeca et al. [28] and used VEINS for the simulation of vehicles.

The VeReMi dataset consists of message logs for every vehicle in the simulation and a ground truth file that specifies the attacker's behavior. The local information from the vehicle is included through messages of a different type

(representing periodic messages from a GPS module in the vehicle). The log file consists of local messages generated from traffic simulator SUMO and messages from other vehicles. Each log entry contains a reception time stamp, the claimed transmission time, the claimed sender, a simulation-wide unique message ID, a position vector, a speed vector, the RSSI, a position noise vector and a speed noise vector. Each time a message is sent it is also updated in the ground truth file which contains actual position/speed values and the attacker type. 0 is used for legitimate vehicles and 1, 2, 4, 8, 16 for 5 different types of attackers listed in Table 1 in respective order.

The dataset consists of 225 individual simulations with

- Five different attackers.
- Three different attacker densities.
- Three different traffic densities.
- Five repetitions for each parameter set (with different random seeds).

The dataset consists of a total of 225 simulation executions, split into three density categories.

- Low density has 35 to 39 vehicles.
- Medium density has between 97 and 108 vehicles.
- High density has between 491 and 519 vehicles.

Out of these vehicles, a subset of the vehicle is malicious. The decision is made by sampling a uniform distribution ([0; 1]) and comparing it to the attacker fraction parameter. All of the vehicles classified as attacker execute the same attack algorithm.

4.3 Feature Description

Feature selection plays a crucial role in machine learning classification accuracy can depend a lot on the features selected for training the model. Dimensionality relies on a number of features, it affects training time and is a powerful defense against overfitting.

We tried a different combination of features from the following set x, y, z position and speed coordinates, the difference between position and speed coordinates of sender and receiver. It is important to note that we only used those log entries which are received by a vehicle and not the ones generated by the vehicle itself. Various combination of features used in this work are listed in Table 2.

We used position as a feature because all the attacks are based on position falsification and hence attackers will have different trends of position values than legitimate vehicles. We added the difference of sender and receiver positions/speed to detect attackers of type 2 and 4. It should be considered because receiver cant receive signals from the certain physical threshold, hence if an attacker sends some random position which is beyond the theoretical range of communication, then the receiver would be able to detect that. We realized

Table 2. Combination of features used

Comb.	Features
1	a. x, y, z coordinates of a position
	b. x, y, z coordinates of speed
2	a. x, y, z coordinates of a position
	b. x, y, z coordinate difference of position between sender and receiver
3	a. x, y, z coordinates of a position
	b. x, y, z coordinates of speed
	c. x, y, z coordinate difference of position between sender and receiver
	d. x, y, z coordinate difference of speed between sender and receiver

that speed is not a useful feature because speed transmitted by both attackers and non-attackers is in a similar range. In the given dataset attacker tries doesn't make any falsification in its speed and hence it will not help the model distinguish between non-attackers and attackers. Our training time reduced significantly after removing speed from the features.

5 Results

In this section, we discuss the results that we achieved after the experiment. We used logistic regression (LR) without normalization and with normalization. We found that logistic regression achieves higher accuracy and works better with normalization. F1- the score is used as a metric for accuracy. The result graphs are shown in Figs. 4, and 5, respectively. Please note that we used logistic regression for binary classification (all attackers have attacker type 1 and 0 for non-attackers).

Our training time significantly reduced when we removed undesired features. As shown in Fig. 6, SVM binary classifier performed better than Logistic Regression. We achieved highest F1-score using SVM binary classifier, RBF() kernel and feature combination number 3.

F1 score is used for measuring accuracy when the distribution of positives and negatives in a dataset is highly skewed. F1 score is a combined metric as the harmonic average of both precision and recall. Precision is the ratio of correctly predicted positive (true positives) with total predicted positive data points (true positives + false positive). Recall is the ratio of correctly predicted positive values (true positives) with all data points that were actually in the positive class (true positive + false negative). In our experiments, we observed precision was slightly better than recall. Precision was close to 1 which means that out of vehicles predicted as attacker most of them were actual attacker which is a good sign that any non-attacker will not be discriminated in the network after getting misclassified. Recall in the observations were slightly lower

compared to a precision which can be improved by adding more features and making the model more complex. The overall model is able to classify attackers with good recall and precision.

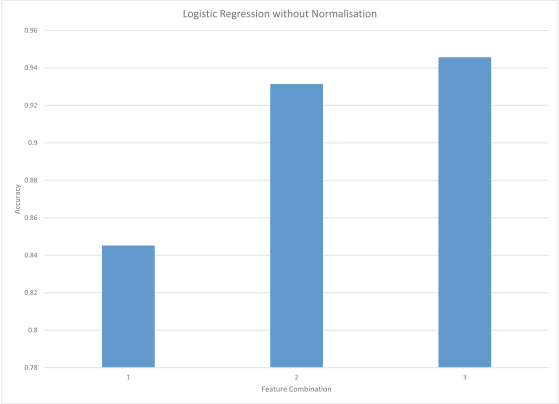

Fig. 4. LR without normalization

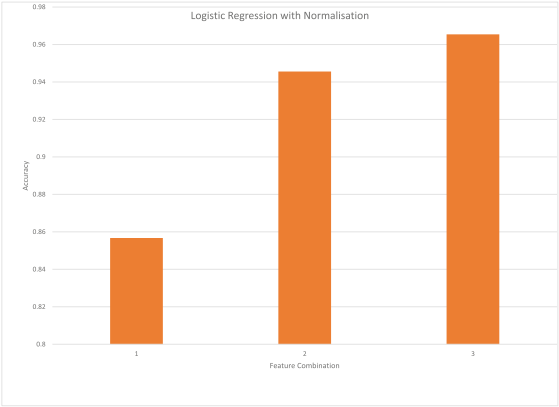

Fig. 5. LR with normalization

SVM performs better than logistic regression because it is less sensitive to outliers. A few outliers will significantly impact the loss function of logistic regression leading to distortion of the decision boundary with respect to general points. On the other hand, SVM tries to maximize the margin by taking a few points known as support vectors into consideration. Support Vector Machines generally trains faster than other regression models. And moreover, If a dataset

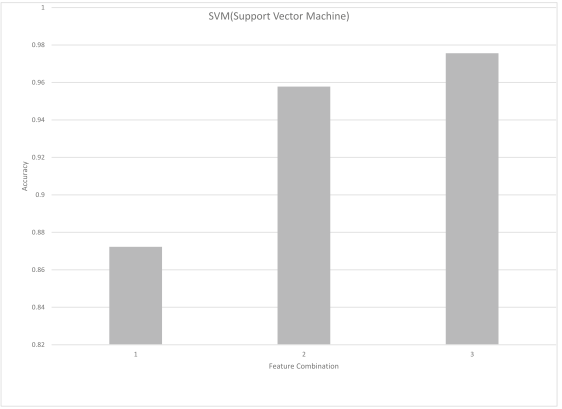

Fig. 6. SVM results

is not separable by a linear decision boundary then SVM outperforms linear regression. Different kernels can be used in SVM which transform data points to a higher dimensional space where transformed points can be linearly separable. We have used RBF (Radial Basis Function) kernel in our experiments which maps points to infinite dimensional space.

To further improve the performance of the model we can add features similar to simple speed check, which will train the model in such a way that vehicles which have inconsistencies between the rate of change of position and speed will be caught. We tested our model on the logs generated by the same simulation. We can test our model on a different dataset with different environmental conditions with the same log entries. Similar machine learning models can also be created for other types of misbehavior detection in VANETs.

6 Conclusion

In this paper, different machine learning methods are used to detect position falsification attack in VANETs. SVM with normalization performed better than logistic regression with or without normalization. Model accuracy depends a lot on feature selection. Further research work can be on multiple misbehavior modeling in VANETs and detection using the ML-based approach. Although traditional methods perform well, artificial neural networks can also be applied to evaluate the performance on the dataset.

Acknowledgments. The research work has been conducted in the Information Security Education and Awareness (ISEA) Lab of Indian Institute of Technology Guwahati. The authors would like to acknowledge IIT Guwahati and ISEA MeitY, India for the support.

References

1. Santa, J., Pereñíguez, F., Moragón, A., Skarmeta, A.F.: Experimental evaluation of CAM and DENM messaging services in vehicular communications. Transp. Res. Part C: Emerg. Technol. **46**, 98–120 (2014)
2. Kerrache, C.A., Calafate, C.T., Cano, J.C., Lagraa, N., Manzoni, P.: Trust management for vehicular networks: an adversary-oriented overview. IEEE Access **4**, 9293–9307 (2016)
3. Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A.: VANet security challenges and solutions: a survey. Veh. Commun. **7**, 7–20 (2017)
4. Brecht, B., et al.: A security credential management system for V2X communications. IEEE Trans. Intell. Transp. Syst. (99), 1–22 (2018)
5. IEEE: IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages. IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1–240, March 2016
6. ETSI, T.: 102 940: Intelligent Transport Systems (ITS). Security; ITS communications security architecture and security management. Technical specification, European Telecommunications Standards Institute (2012)
7. Lu, Z., Qu, G., Liu, Z.: A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans. Intell. Transp. Syst. (2018)
8. Soleymani, S.A., et al.: Trust management in vehicular ad hoc network: a systematic review. EURASIP J. Wirel. Commun. Netw. **2015**(1), 146 (2015)
9. Van der Heijden, R.W., Lukaseder, T., Kargl, F.: VeReMi: a dataset for comparable evaluation of misbehavior detection in VANETs. arXiv preprint arXiv:1804.06701 (2018)
10. Van der Heijden, R.W., Dietzel, S., Leinmüller, T., Kargl, F.: Survey on misbehavior detection in cooperative intelligent transportation systems. arXiv preprint arXiv:1610.06810 (2016)
11. Khan, U., Agrawal, S., Silakari, S.: A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks. In: Mandal, J.K., Satapathy, S.C., Sanyal, M.K., Sarkar, P.P., Mukhopadhyay, A. (eds.) Information Systems Design and Intelligent Applications. AISC, vol. 339, pp. 11–19. Springer, New Delhi (2015). https://doi.org/10.1007/978-81-322-2250-7_2
12. Zhang, J.: A survey on trust management for VANETs. In: International Conference on Advanced Information Networking and Applications (AINA), pp. 105–112. IEEE (2011)
13. Ma, S., Wolfson, O., Lin, J.: A survey on trust management for Intelligent Transportation System. In: Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science, pp. 18–23. ACM (2011)
14. Rawat, D.B., Bista, B.B., Yan, G., Weigle, M.C.: Securing vehicular ad-hoc networks against malicious drivers: a probabilistic approach. In: 2011 International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), pp. 146–151. IEEE (2011)
15. Hsiao, H.C., Studer, A., Dubey, R., Shi, E., Perrig, A.: Efficient and secure threshold-based event validation for VANETs. In: Proceedings of the Fourth ACM Conference on Wireless Network Security, pp. 163–174. ACM (2011)
16. Zhuo, X., Hao, J., Liu, D., Dai, Y.: Removal of misbehaving insiders in anonymous VANETs. In: Proceedings of the 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, pp. 106–115. ACM (2009)

17. Leinmüller, T., Schmidt, R.K., Held, A.: Cooperative position verification-defending against roadside attackers 2.0. In: Proceedings of 17th ITS World Congress, pp. 1–8 (2010)
18. Bilogrevic, I., Manshaei, M.H., Raya, M., Hubaux, J.P.: Optimal revocations in ephemeral networks: a game-theoretic framework. In: 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), pp. 21–30. IEEE (2010)
19. Stubing, H., Jaeger, A., Schmidt, C., Huss, S.A.: Verifying mobility data under privacy considerations in Car-to-X communication. In: 17th ITS World CongressITS JapanITS AmericaERTICO (2010)
20. Stübing, H., Firl, J., Huss, S.A.: A two-stage verification process for Car-to-X mobility data based on path prediction and probabilistic maneuver recognition. In: 2011 IEEE Vehicular Networking Conference (VNC), pp. 17–24. IEEE (2011)
21. Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V.C.: Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things J. (2018)
22. Grover, J., Prajapati, N.K., Laxmi, V., Gaur, M.S.: Machine learning approach for multiple misbehavior detection in VANET. In: Abraham, A., Mauri, J.L., Buford, J.F., Suzuki, J., Thampi, S.M. (eds.) ACC 2011. CCIS, vol. 192, pp. 644–653. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22720-2_68
23. Kang, M.J., Kang, J.W.: Intrusion detection system using deep neural network for in-vehicle network security. PloS One **11**(6), e0155781 (2016)
24. Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., Gan, D.: Cloud-based cyber-physical intrusion detection for vehicles using Deep Learning. IEEE Access **6**, 3491–3508 (2018)
25. Taylor, A., Leblanc, S., Japkowicz, N.: Anomaly detection in automobile control network data with long short-term memory networks. In: 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), pp. 130–139. IEEE (2016)
26. Ali Alheeti, K.M., Gruebler, A., McDonald-Maier, K.: Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks. Computers **5**(3), 16 (2016)
27. IEEE Std.: IEEE Standard for Information technology – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, pp. 1–51, July 2010
28. Codeca, L., Frank, R., Faye, S., Engel, T.: Luxembourg SUMO traffic (LuST) scenario: traffic demand evaluation. IEEE Intell. Transp. Syst. Mag. **9**(2), 52–63 (2017)