Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey

Alia Mohammed Alrehan , Fahd Abdulsalam Alhaidari
College of Computer Science and Information Technology,
Imam Abdulrahman Bin Faisal University,
P.O. 1982, Dammam, Saudi Arabia
alia55.m.j@gmail.com, faalhaidari@iau.edu.sa

***Abstract*— Road traffic accidents and their sequences increase dramatically worldwide and thus raising a demand for solutions to providing safety and control of vehicles on road when driving. This is one of the top priorities for modern countries focusing on enhancing citizens' quality of life by developing an Intelligent Transport System (ITS). Vehicular Ad hoc NETworks (VANETs) are recognized to be effective in realizing such a concept. VANET is potential in improving road safety and in providing travelers comfort. However, such technology is still exposed to many vulnerabilities led to numerous of security threats that must be solved before VANET technology is practically and safely adopted. One of the main threats that affects the availability of VANET is Distributed Denial of Service (DDoS) attack. In this paper, we focus on studying the main attacks along with DDoS attack on VANET system as well as exploring potential solutions with a focus on machine learning based solutions to detect such attacks in this field.**

Keywords*— *VANET, DDoS, Machine learning, SDVN, Security.

I. INTRODUCTION

Based on world health organization 2015 global status report of road safety, statistic shows that road accidents lead to 1.25 million deaths every year, and 45% of road traffic deaths in Eastern Mediterranean caused by car accident [1]. In the Kingdom of Saudi Arabia, the number of traffic accident is high, and the number of deaths and injuries cannot be ignored. Saudi government applied a lot of solutions to reduce the rate of the accidents aka imposing of traffic rules and applying monitoring system like Saher system. However, although these solutions are excellent and their results have been achieved, the traffic accidents rate remains high.

To reduce traffic accident many researchers proposed different solutions over the last few decades, like implement Intelligent Transport System (ITS) and Vehicular Ad-hoc NETworks (VANETs). VANET is a special wireless ad hoc which is subset of Mobile Ad hoc Network (MANET) and IoT application [2]. Fig.1 shows the relation between these technologies. The main objective of VANETs is to concentrating on the safety of drivers, passengers, and the vehicle itself by sharing confidential information about traffic and accident between vehicles [3]. The vehicles act as nodes in VANET, and each node is equipped with an On-Board Unit (OBU). In general, there are three types of communication in VANET: vehicle to vehicle communication (V2V), vehicle to infrastructure (V2I), and road side unit (RSU) to RSU (I2I) communication [4]. By the nature of VANET which is high mobility and large size of network, in addition to frequently exchange information between nodes. Based on these characteristics, if any node exchanging a malicious information, the whole network can be interrupted and compromised and thus becoming a life crucial.

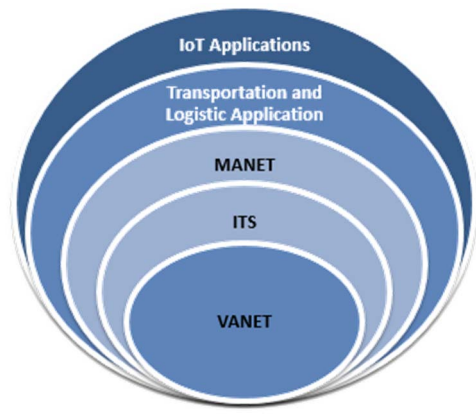

Figure 1: Relation between VANET and IOT

VANET environment has many variabilities inherent from the VANET structure and characteristics. Different attacks categorized under confidentiality such as Eavesdropping, traffic analysis. In addition, VANET has number of attacks under integrity like Masquerade, Black hole, and Replay attacks. Furthermore, some attacks targeting the VANET availability such as Jamming, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks. DDoS attacks occurs in VANET when many perpetrators target a common victim node by flooding it with abnormally large number of fake messages which lead to exhausting all the resources such that nodes no longer being able to deal with legitimate requests. Thus, it is important to protect such networks from being disabled to ensure their continuity and availability to serving the safety applications.

攻擊者藉由不當方式佔用系統分享資源 (例如： CPU 、網路、硬碟等 …) ，達到干擾正常系統運作的進行。不同於一般網路入侵， DoS 不一定需要取得系統使用的權力，即可達到目的。最常見的 DoS 方式即是透過所謂的訊息洪泛 (Message Flood) ，向攻擊對象送出大量且無意義的網路訊息，不管被攻擊對象是否回應，都會因網路頻寬被佔用，而導致服務無法如常運作。

利用網路上因為惡意程式而被控制的電腦作為跳板，集中向某一特定的目標電腦密集的送出大量且無意義的網路訊息，藉以把目標電腦的網路資源及系統資源耗盡。

The main contributions of this paper can be outlined as follows: Studying the main attacks on VANET system including DDoS attacks. Exploring the effectiveness of machine learning on mitigating attacks in VANET. Summarizing the contributions of recent researches on securing VANET as well as categorizing them. Finally, to the best of our knowledge, this is the first review focused on securing VANET based on machine learning.

The organization of the rest of the paper is as follows. Background knowledge of VANET is briefly introduced in Section 2. In Section 3, an overview of the existing mechanisms and techniques proposed to detect and prevent attacks in VANET environment. Section 4 discusses and analyses recent literature review in the field. Finally, Section 5 gives the conclusion of the study.

978-1-7281-0108-8/19/$31.00 ©2019 IEEE

II. BACKGROUND

The main system components in VANET are Application unit (AU), On-Board Unit (OBU), and Roadside unit (RSU). These three components communicate through a wireless access in vehicular environments called (WAVE), which is based on the IEEE 802.11p radio frequency channel [5]. Fig. 2 shows the main components of VANET system.

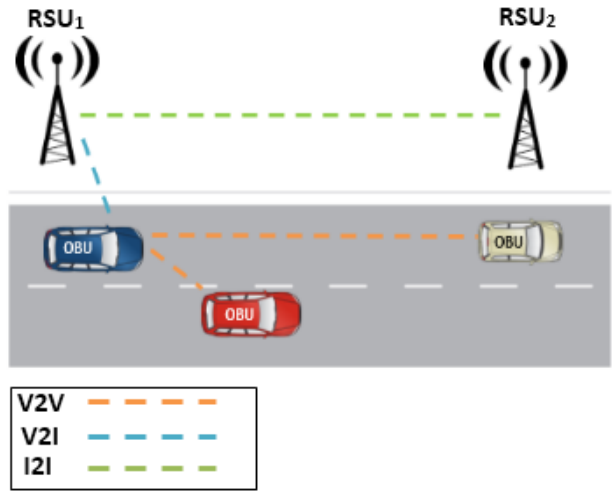

Figure 2: VANET Architecture

An OBU is a wave device usually mounted on-board a vehicle and used to exchange information with RSUs or with other OBUs. It is comprising of a Resource Command Processor (RCP) which contains a read/write memory used to store up and recover information. The core functions of the OBU are reliable message transfer, ad hoc and geographical routing, network congestion control, wireless radio access, data security, and IP mobility.

The AU is a device placed inside the vehicle includes an application or user interface that uses the communication abilities of the OBU through a wired or wireless connection. An example of AU the Personal Digital Assistant (PDA) to run the Internet.

The RSU is a fixed device along the roadside or in custom locations, for example at crossroads or near the parking area. The RSU has three core functions: 1) Extending the communication range, by sending the information to other RSUs to forward it to other OBUs. 2) Running safety applications, by using I2V and acting as an information source to send different types of warnings like an accident warning, work zone, and low bridge warning. 3) Providing Internet connectivity to OBUs.

VANET has its own unique characteristics when compared with other types of Ad hoc networks, the unique characteristics of VANET includes [5] [6] :

- Predictable mobility: nodes in VANET move in a haphazard manner because vehicles are constrained by road layout and by the follow the traffic lights, road signs.
- No power constraints: the power in VANET is not consider as a challenge
- Rapid changes in network topology: which due to the high speeds of the vehicles, especially at the highway.
- Large-scale network: which depends on the dense urban areas such as big cities, the downtown, highways.
- High computational ability: which refers to the number of nodes needs to exchange the information between them and RSU at the same time.

III. LITERATURE REVIEW

In this section, we briefly review the attacks in VANET. Then, Distributed Denial of Service (DDoS) attack in VANET. After that, we explore machine learning techniques used on VANET system especially for detecting DDoS attacks.

A. Vulnerabilities in VANET

In [4], authors analyzed various security attacks and their proposed solutions in VANET systems. They categories VANET attacks into four main categories: 1) Routing attack, that include gray/black hole attack, and Sybil attack. 2) Integrity attack, that includes alteration attack. 3) Confidentiality attack, eavesdropping is an example of attack under this category. 4) Availability, which include DOS, jamming, spamming attacks.

指的是一個惡意的節點非法地對外呈現多個身份。

An extensive overview of the most security challenges and their causes in VANET was done in [7]. Authors investigated most of the VANET security challenges as well as the existing solutions in a comprehensive manner. The VANET characteristics led to arise exclusive security challenges like network size, highly dynamic nature, frequent disconnection, usage of wireless channels to exchange messages, information verification, key distribution, and forwarding algorithms. So, these challenges imperil VANETs to various attacks. These attacks can be categorized into four main groups: 1) Attacks on the wireless interface, 2) Attacks on hardware and software, 3) Attacks on sensors input in the vehicle, 4) Attacks on infrastructure (CAs or vehicle manufacturer).

Different classification of attacks in VANET was presented in [8]. Authors categorized attacks in VANET based on the source of attacks (insider or outsider), type of attack (active or passive), and the last category based on security parameters i.e. confidentiality, integrity, availability, and authenticity. In addition, they discussed and categorized twenty of attacks in VANET like DoS/DDoS, Hidden vehicle, Sybil, Alternation attack …etc. Furthermore, the authors proposed a Bait based Intrusion Detection System called Honeypot based IDS (HPIDS). The HPIDS framework combine both IDS and honeypot making it capable of detecting both known as well as zero-day attacks. HPIDS provides more security and robust.

In [9], they proposed a new scheme for detecting Sybil attacks in VANET based RSUs. The proposed scheme uses routine communications between the RSUs and nodes to detect the attack, that means there is no need for extra hardware. In addition, authors tested the effectiveness of the proposed scheme by simulation experiment. They used different simulation tools: SUMO ,NS-3, and MATLAB. The experimental result shows that the proposed scheme get a very high accuracy of around 100%.

VANETs facing many attacks, which range from managing high node mobility to securing data transportation. The Software Defined Networking (SDN) paradigm has been identified as a proper solution for dealing with the highly

dynamic network environment like VANETs. Since 2014 numerous of SDN-based architectures for VANETs have been proposed. In [10] the authors studied the vulnerabilities in VANET and the impact of enabling SDN in VANET. Based on the nature of VANET makes it prone to different attacks like GPS spoofing, DoS / DDoS attack, replay attack, and much more. And to cope with these attacks and achieve cyber-safe, VANETs should meet the classical security requirements: Confidentiality, Integrity, Availability, Authenticity, and Non-Repudiation. In another hand when applying SDN in VANET will facilitate running and upgrading different applications in a scalable manner, without concern about network and hardware complexity. however, SDN comes with its own vulnerabilities, inherited from its architecture: centralized controller, abstraction and programmability, and flow-based forwarding.

In [11], authors focused on Software Defined Vehicular Networks (SDVN) from security perspective and provide taxonomy, requirements, and explore some open issues in this filed. They categorized attacks based on SDN layers. The SDN has three layers: 1) Application layer. 2) Control plan layer. 3) Data plan layer. Finally, they mention the prime concern which securing the controller, and potentially the controller targeted with flooding attacks such as Dos/DDoS attacks.

B. *Distributed Denial of Service Attack in VANET*

In [12], authors proposed a novel framework for real-time detecting and mitigating low and high rate DDoS attacks in ITS based on nonparametric statistical anomaly detection. They focus on communication from vehicles to RSU. RSU labors as the network center in a VANET and monitors it for possible threats. Online Discrepancy Test (ODIT) method was used in detecting phase, which based on two algorithms, Cumulative Sum (CUSUM) test and Geometric Entropy Minimization (GEM) and takes the combines the nonparametric nature of GEM with the timely detection capability of CUSUM. Simulation of the proposed model was done on real road scenario using three software, SUMO, OMNET++, and Veins. The experimental results show that the proposed method quickly detects low and high rate DDoS attacks, successfully identify the attack locations, and mitigates the attack by blocking the data traffic from attack locations.

Multivariant Stream Analysis (MVSA) for detecting and mitigating the DDoS attack on VANET was proposed in [13]. In MVSA the communication between V2V done through RSU. The detecting of DDoS attack starts by reading the network trace and calculates an average measure of payload, the frequency for each stream class at different time windows, and time to live which is done by vehicle. After that, the method computes the stream weight with the help of traces. Finally, MVSA will classify the packet into either malicious or genuine. The performance of the MVSA was evaluated using an NS2 simulator, and the simulation results demonstrate the efficiency and effectiveness of the MVSA.

In [14], authors studied the impact of DDoS attack on the controllers in Software-Defined Internet-of-Vehicles. They highlighted the impact of three levels of attack rates in terms of throughput and controller load. Two experimental scenarios were done using Mininet-WiFi emulator. The first scenario study parked vehicles and the second study mobility vehicles. The experimental result in both scenarios shows that stations suffered a decrease in average throughput during the attack interval. On another hand, the Impact on controller load observes how an increasing attack rate leads to almost 99% of attacker Packet-Ins at the controller. As a result, the DDoS attacks demonstrated the success of against the control plane.

Another proposed scheme was introduced in [15] to secure VANET form DDoS attack. They focused on detection and prevention DDoS by using the available resources and with least overhead on VANET. The proposed scheme differentiates between an attacker and a normal node by comparison of their communication time with a threshold time. In another word, if the comparison result found that sender's IP greater than the threshold value, the alarm message module will be activated. This module is responsible for two tasks, the first one is sending a message to vehicle's, to immediately end communication with that attacker node and sends a message to RSU to alarm it about the attacker node so that the RSU notify all vehicles on the network to avoid communication with the attacker node. Finally, the authors simulate the proposed scheme using NS, AWK scripts and achieved a satisfactory result.

C. *Usage of Machine Learning for VANET*

In VANET a large amount of data should be processed fast from each node. And to handle the huge amount of data and process them with minim time, several machine learning techniques have been applied to cope up this issue in VANET environment.

Machine learning has not been studied extensively in misbehavior detection in VANET. However, in [16], they proposed a new effective misbehavior detection model based on machine learning techniques for VANET applications. The proposed model consists of four phases: data acquisition, data sharing, analysis, and decision making. Authors evaluated the proposed model by simulating real-world traffic dataset namely NGSIM. NGSIM contains both attacker and normal traffic data. They used Artificial Neural Network (ANN) techniques to train the dataset. the experiment result shows very high accuracy with an average of 99%, in addition to the effectiveness of the proposed model in comparison with the existing baseline model.

Another effort used machine learning to secure Software Defined Vehicular Networks (SDVN) in [17]. The proposed mechanism detects four categories of attacks: DoS attack, probing attack, user to root attack, and remote to local attack. Authors used multi-class support vector machine (SVM) to dynamically detect different attacks. The proposed mechanism was conducted with simulation. They used MATLAB with multi-class SVM toolbox as the simulation tool and KDD CUP 1999 intrusion detection dataset which is general intrusion dataset not real/synthetic from VANET environment. However, the results demonstrate that the effectiveness of the proposed mechanism to classify the types of attacks, as well as good performance regarding high precision, recall, and accuracy.

Authors in [18] focused on context changes which are rife in VANETs. They proposed a context-aware security framework for VANETs based on SVM algorithm. The objective of the proposed framework is to automatically differentiate between malicious nodes from abnormal nodes due to contextual reasons. like movement speed, temperature, and transmission range. The proposed framework has three

functional modules, start with behavior data collection, then context sensing and processing, finally the misbehavior detection. In the experiment, they generated a dataset to train SVM classifier by using simulation tools and GloMoSim 2.03 as the experimental platform. the results demonstrate that the proposed framework achieves a good performance in accuracy, recall values, and an acceptable value of communication overhead. in addition, and it is more flexible to context changes which are suitable for VANETs environments compared with other existing security solutions for VANETs.

根據特徵（速度偏向、距離、收到的訊號強弱、封包生成傳送丟棄碰撞）

Authors in [19] designed a framework for differentiating between legitimate and malicious nodes in VANET. They used a machine learning approach to classify multiple misbehaviors node in VANET using behavioral features of each node. These features are speed deviation, distance, received signal strength (RSS), the number of packets generated, delivered, dropped, collided. They used two types of classification to measure the accuracies, the first one is Binary and the second one is Multi-Class. In Binary classification, all types of misbehaviors considered as single misbehavior class whereas, Multi-class classification can categorize misbehaviors into misbehaving classes. In addition, authors extracted the features of packets by performing experiments in NCTUns-5.0 simulator with various simulation scenario and calculated by nearby observer nodes. Also, they used WEKA to classify the misbehavior, with different classifier namely: Random Forest (RF), J-48, Naive Bayes, Ada Boost1, and IBK. Experiment result shows that RF and J-48 classifiers perform better compared to other classifiers. The RF and J-48 classifier gives better classification due to the boosting and bagging properties.

D. *Usage of Machine Learning for DDoS in VANET*

Machine learning based anomaly detection on VANET was presented in [20]. They designed a framework to effectively detect the DDoS attack in SDVN in a fast manner. The proposed framework contains three models: ① detection trigger module, ② flow table item collection module, ③ attack detection module. In the first module, a detection trigger mechanism based on the PACKET_IN message was proposed. In the flow table entry collection module, they designed a flow-table feature-based DDoS attack detection method by merge the feature of the DDoS attack and OpenFlow protocol. In the attack detection module, the SVM classification used to train the samples and build a detection model to figure out if the DDoS attack in the network. Furthermore, the authors generated DDoS attack traffic through the Scapy and hping3. Also analyzed the features of DDoS attack under the three protocols: UDP, ICMP, and TCP. The simulation results show that the classification recognition has a lower false alarm rate and proposed scheme effectively decreases the time for starting attack detection.

Another effort using unsupervised machine learning to detect a specific type of DDoS attack in VANET, namely the RF jamming attack was presented in [21]. Authors developed an algorithm, that depending on the variations of the relative speed between jammer and receiver nods and generates a new metric namely the variations of the relative speed (RSV). The goal of this is to evaluate whether this new metric enhance the detection results under different situations without adding extra complexity to their model at same time. By using k-means algorithm they able to distinguish the intended from unintentional jamming, in addition, identify the unique characteristics of each jamming attack. The proposed method was applied to three different real-life scenarios, two of them with a moving jammer present and one with interference only. In the simulation, they collected the data in different situation of jammer, the first one while the jammer was active and a second when it temporarily idle. The experimental result shows the capability of establish the crucial role of the relative speed and its variations in detection jamming efficiently.

在行動計算中，干擾器是一種行動通信設備，它在與手機相同的頻率範圍內進行傳輸，以產生強烈的手機信號塔干擾並阻止手機信號和呼叫傳輸。

IV. Discussion and Analysis

In this section, we will summarize Section III in tabular format, which is presented in Table 1, and Table 2. In addition to discussing and analyzing recent literature reviews in this field.

From Table 1, we can observe that current research proposes different solutions to securing VANET environment, and three research out of five provide detection and prevention solutions, where the rest of studies focusing only on attacks detection. Researchers used various simulation tools to simulate their proposed solution on VANETs environment and most of them used NS-2/3 and SOMO.

Table 2 summaries studies used ML techniques to secure VANETs. Four out of six studies focusing on detection attacks on VANET environment, where the rest provide detection attacks solution based on SDVN. In general, all studies providing detection solution only and the average of accuracy around 93%. The highest accuracy was 99 %, which presented in [16] where they used ANN to detect misbehavior in VANET environment.

By analyzing the current literature using ML in VANET to detect misbehavior or specific attack, we can observe that different datasets have been used and most of the datasets were generated from a simulation environment [18] [19] [20] [22]. In [16], they used areal dataset called NGSIM dataset where researchers injected dynamic noises to data to simulate harsh environment. Also, they simulated the dataset in a simulation environment with 80% of vehicles normal and 20% of vehicles are simulated as misbehaving vehicle. Another study presented in [17] with which they used KDD CUP 1999 dataset and referred for the reason of using this dataset is no real security dataset in VANET are available. A study presented in [23] analyzed 30 studies in intrusion detection techniques for Cyber-Physical Ssystems (CPS), which is closely related to VANETs and they found that only 4 studies used a public dataset, 22 papers did not release their dataset, and 4 did not use any dataset at all. The distinguishing characteristics of CPS and IT system presented in [24].

Lacking of dataset in securing VANET field, encourage researchers to generate a synthetic dataset for VANET environment [25]. And the only public datasets have been recently published for IDS which contain different misbehavior attack called VeReMi [23]. The VeReMi dataset aims at being the common dataset for evaluating security solution approaches [26]. Furthermore, researchers from a similar field generated their own dataset by using well-known simulation tools that simulate the intended environments [27]. As a summary, most of the security solutions proposed for WSN or MANET are not appropriate for VANET because of the special and unique characteristics of VANET [16] and hence using a general traffic dataset for evaluating and validating the security of VANET environment will not give accurate results.

Finally, machine learning has not been applied extensively to detect and prevent DDoS attack in VANET. As illustrated in table 2, one study proposed a detection solution of DDoS attack in SDVN which is the next generation of VANET environment. Accordingly, there is a need to propose a solution to detect and prevent DDoS attack in VANET and SDVN based on ML using a dataset from VANET environment which is a point often overlooked by studies in this field.

Table 1: Solution to Secure VANETs System

Ref.	Year	Attack	Proposed Solution	Security Goal		Simulation Tools
				Detection	Prevention	
[8]	2018	Known, Zero-day attacks	Honeypot HPIDS	✓		MOVE, SOMO, NS-2
[9]	2018	Sybil	IOAC	✓		SOMO, NS-3, MATLAB
[12]	2018	DDoS	framework	✓	✓	SUMO, OMNET++, Veins
[13]	2018	DDoS	MVSA	✓	✓	NS-2
[15]	2016	DDoS	Algorithm	✓	✓	NS, AWK scripts

Table 2: ML Techniques to Secure VANETs System

Ref.	Year	Attack	Algorithm	Used Dataset	Environment	Simulation Tools	Accuracy
[16]	2017	Misbehavior	ANN	NGSIM	VANET	MATLAB	99%
[17]	2017	DoS, probin	SVM	KDD CUP 1999	SDVN	MATLAB	>85%
[18]	2015	Misbehavior	SVM	Generated dataset	VANET	GloMoSim 2.03	NA
[19]	2011	Misbehavior	RF, NB, IBK, J-48, Ada- Boost1	Generated dataset	VANET	NCTUns-5.0 WEKA	93%
[20]	2018	DDoS	SVM	Generated dataset	SDVN	Floodlight	>97%
[21]	2018	DDoS	k-means	Generated dataset	VANET	NA	NA

V. Conclusion and Future Work

This paper highlighted the VANET environment which aims to improve road safety, driving experience, navigation, and other roadside services. Due to the architecture of VANET system and its characteristics, VANET is highly prone to attacks. Therefore, security solutions for VANET are required to be developed. Many efforts have been made to provide security on VANET but are restricted in providing a holistic solution as they applied the same traditional security solution without considering the special aspects of VANET environment. In this paper, we studied VANET architecture and its characteristics as a background for our literature review study that selected recent studies in this field from the security perspective on VANET focusing more on DDoS attacks. In addition, this paper studied the usage of ML to provide security providing security solutions for different attacks in VANET.

As part of our future work, we propose to provide a solution for detecting and prevent DDoS attacks in VANET along with its design and consideration for better detection and prevention rate. Also, we intend to generate a dataset for such environment by using simulation tools considering the aspects and features related to VANET system rather than using a public and general dataset.

REFERENCES

[1] "WHO | Global status report on road safety 2015," *WHO*, 2018.

[2] M. R. Jabbarpour, A. Nabaei, and H. Zarrabi, "Intelligent Guardrails: An IoT Application for Vehicle Traffic Congestion Reduction in Smart City," *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, pp. 7–13, 2017.

[3] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars," *Proc. - 2015 6th Int. Conf. Emerg. Secur. Technol. EST 2015*, pp. 86–91, 2015.

[4] M. Jain and R. Saxena, *VANET : Security Attacks , Solution and Simulation*. Springer Singapore, 2018.

[5] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *J. Netw. Comput. Appl.*, vol. 37, no. 1, pp. 380–392, 2014.

[6] H. Shafiq, R. A. Rehman, and B. S. Kim, "Services and Security Threats in SDN Based VANETs: A Survey," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018.

[7] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, 2017.

[8] S. Sharma and A. Kaul, "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Veh. Commun.*, vol. 12, pp. 138–164, 2018.

[9] H. Hamed, A. Keshavarz-Haddad, and S. G. Haghighi, "Sybil Attack Detection in Urban VANETs Based on RSU Support," *Electr. Eng. (ICEE), Iran. Conf.*, pp. 602–606, 2018.

[10] A. Di Maio *et al.*, "Enabling SDN in VANETs: What is the impact on security?," *Sensors (Switzerland)*, vol. 16, no. 12, pp. 1–24, 2016.

[11] A. Akhunzada and M. K. Khan, "Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 110–118, 2017.

[12] A. Haydari, "Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems," no. September, 2018.

[13] R. Kolandaisamy *et al.*, "A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks," vol. 2018, 2018.

[14] A. J. Siddiqui and A. Boukerche, "On the Impact of DDoS Attacks on Software-Defined Internet-of-Vehicles Control Plane," *2018 14th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2018*, pp. 1284–1289, 2018.

[15] M. Shabbir, M. A. Khan, U. S. Khan, and N. A. Saqib, "Detection and Prevention of Distributed Denial of Service Attacks in VANETs," in *Proceedings - 2016 International Conference on Computational Science and Computational Intelligence, CSCI 2016*, 2016, pp. 970–974.

[16] F. A. Ghaleb and F. Mohammed, "An Effective Misbehavior Detection Model using Artificial Neural Network for Vehicular Ad hoc Network Applications," pp. 13–18, 2017.

[17] M. Kim, I. Jang, S. Choo, J. Koo, and S. Pack, "Collaborative security attack detection in software-defined vehicular networks," *19th Asia-Pacific Netw. Oper. Manag. Symp. Manag. a World Things, APNOMS 2017*, pp. 19–24, 2017.

[18] W. Li, A. Joshi, and T. Finin, "SVM-CASE: An SVM-based context aware security framework for vehicular ad-hoc networks," *2015 IEEE 82nd Veh. Technol. Conf. VTC Fall 2015 - Proc.*, pp. 1–5, 2015.

[19] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in VANET," *Commun. Comput. Inf. Sci.*, vol. 192 CCIS, no. PART 3, pp. 644–653, 2011.

[20] Y. A. O. Yu, L. E. I. Guo, Y. E. Liu, J. Zheng, and Y. U. E. Zong, "An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks," *IEEE Access*, vol. 6, pp. 44570–44579, 2018.

[21] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Veh. Commun.*, vol. 13, pp. 56–63, 2018.

[22] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Veh. Commun.*, vol. 13, pp. 56–63, 2018.

[23] R. W. Van Der Heijden, T. Lukaseder, and F. Kargl, "VeReMi : A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs."

[24] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security : Analysis , challenges and solutions," *Comput. Secur.*, vol. 68, pp. 81–97, 2017.

[25] V. Belenko and M. Kalinin, "Synthetic datasets generation for intrusion detection in VANET," 2018.

[26] S. So and J. Petit, "Integrating Plausibility Checks and Machine Learning for Misbehavior Detection in VANET," *2018 17th IEEE Int. Conf. Mach. Learn. Appl.*, pp. 564–571, 2018.

[27] L. Arnaboldi and C. Morisset, "Generating Synthetic Data for Real World Detection of DoS attacks in the IoT."