Securing Software-Defined Vehicular Network Architecture against DDoS attack

1st Houda Amari
MIRACL Laboratory
FSEGS
Sfax, Tunisia
houda.amari@fsegs.u-sfax.tn

2nd Wassef Louati
REDCAD, Laboratory
FSEGS
Sfax, Tunisia
wassef.louati@redcad.org

3rd Lyes Khoukhi
GREYC Laboratory
ENSICAEN
Caen, France
lyes.khoukhi@ensicaen.fr

4th Lamia Hadrich Belguith
MIRACL Laboratory
FSEGS
Sfax, Tunisia
lamia.belguith@fsegs.usf.tn

2021 IEEE 46th Conference on Local Computer Networks (LCN) | 978-1-6654-1886-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/LCN52139.2021.9524953

***Abstract*—In the recent decades, Intelligent Transport Systems (ITS) attracted researchers' great attention. ITS plays a very important role in making citizens' lives easier in term of mobility, safety, quality of life and security. Vehicular ad-hoc networks (VANETs) became an inseparable component of ITS. The current architecture has been facing many issues due to VANET's characteristics such as high mobility of its nodes and it is still vulnerable to important security attacks which threatens its main security services such as availability, data integrity, authentication and privacy. We propose a new VANET architecture called FCSDVN-ML, in which we combine three emerging paradigms: Software-Defined Network (SDN), Fog Computing (FC) and Machine Learning (ML) to improve security in VANETs. In this paper, we described our architecture components and we discussed its potential performance against Distributed Denial of Service (DDoS) attack using the hierarchical firewalls.**

***Index Terms*—Intelligent Transport System (ITS), VANET, SDN, Fog computing, Machine Learning, DDoS attack.**

I. Introduction

Vehicular Ad-hoc Network (VANET) is a special category in mobile ad hoc networks (MANETs) with highly dynamic topology and intermittent connections [1]. The architecture of VANET is composed of three main elements that are On Board Unit (OBU), Road-Side Unit (RSU) and Application Unit (AU). VANET provides safety application (e.g., lane changing) and non-safety applications (e.g., infotainment applications).
The mobile nodes are smart vehicles. They are equipped with OBUs with which they exchange information with the RSUs or to communicate with other vehicles. Different services such as routing and network congestion control are provided by these OBUs. The next unit is the RSU which is an infrastructure or a device placed along the road-side or in intersections. This unit can be equipped with one or many network devices. Dedicated Short-Range Communication (DSRC) based on IEEE 802.11p can be used by this unit (RSU). The last unit is the Application Unit (AU) which represents a device on-board inside the vehicle, communicating with the network via OBU through wired or wireless connection in order to provide internet connectivity to other OBUs. VANET is still considered as a challenging form of wireless network which presents four types of communications. The first type is Vehicle to Infrastructure (V2I) Communications which consists of vehicles communicating to RSU to process applications (e.g., video streaming) after transmitting its parameters (e.g., position, speed, direction, etc..). The RSU will then collect these parameters and process the required service. Vehicle to Vehicle (V2V) [2] communications is the second type which provide new applications such as safety, infotainment services [3]. In V2V, vehicle communicates with other vehicle (one-hop communication), or via a routing protocol (k-hop communication) when there is no direct connection such as clustering-based [4] [5], route-discovery or broadcasting protocols [6]. The third type is Intra-Vehicle communication which means vehicles are equipped with Electronic Control Units (ECUs), e.g., sensors, actuators, etc.. Third Generation Partnership Project (3GPP) group defines new type called Vehicles-to-Everything (V2X) [7], supported by DSRC and cellular network communications, which includes V2I and V2V. This type provides vital services such as road safety, collusion warning, in-vehicle internet, etc.. Various kinds of services are expected to be supported by VANETs such as traffic alerts, route planning, cloud services, etc.. Some services are already deployed but VANET is still facing many difficulties in management and deployment because of less scalability, less intelligence, poor connectivity, etc..
The above-mentioned problems are very challenging because of the characteristics of VANETs such as high dynamicity of topology and the increasing number of mobile nodes which makes control plane's and data plane's management is very complicated. In order to address the challenges, we combine three emerging technologies; Software-Defined Network (SDN), Fog Computing (FC) and Machine Learning (ML) techniques/algorithms.
In fact, SDN's main concept is separating the control plane and the data plane [8]. A controller unit, called SDN Controller (SDNC), will be placed in the control plane and used for monitoring, managing and optimizing networking's resources. this latter aims to improve its performance (e.g., traffic control, efficient communications, etc..). The data plane is considered as a networking infrastructure composed of forwarding devices and wired/wireless links. SDN provides the ability to design a flexible, programmable networking architecture. OpenFlow (OF) is the mostly used interface which provides the communication between both planes (control and data). A third SDN plane is called application plane which consists of third-party

services and applications. The SDN applications requirements such as security, quality of Service (QoS), resources, etc.. are manipulated by the SDNC via an application-control interface. SDN presents two types of these interfaces; Control-Data Plane Interface called southbound Interface API (e.g., OpenFlow) and Application-Control Plane Interface called northbound API (e.g., REST API). SDN aims to improve the network security and simplify it managements. Also, it support heterogeneity and improve resource utilization by the use of OF. Essential information can be gathered by the SDN Controller while communicating with the OF-Switches. By the use of different anomaly-detection tools and performing various traffic analysis, OF-Switches can collect important information which leads the way for the SDNC to analyse these collected information. Then, it will update or create a new configuration or view of the whole network in order to install updated/new policies or rules to mitigate predicted security issue which provide a faster control of identified security vulnerabilities.

The second combined technology is the Fog computing. FC aims to improve the storage capability of end devices (vehicles) by providing an intermediate layer between them and the cloud. Also, it supports mobile networks protocols (e.g., Bluetooth, ZigBee) which result the ability to connect a wide range of heterogeneous end devices. Integrating such technology, will resolve essential problems such as the data centers congestion [9] and the degradation of the quality of service in the whole network. In fact, FC has a computing layer composed of heterogeneous devices such as access points, IoT gateways, switches called Fog Nodes. These nodes will store data before forwarding it to the cloud.

VANET is a large scale network depending on the dense urban areas (e.g., big cities, highways, downtown,etc..), so a large amount of data is being processed very fast from each node. Machine Learning is one of the most rapidly growing technical tools [10], it makes it a effective approach to process this huge amount of data with minimum time. This paradigm will lead the way to the system to automatically learn and improve its security based on previously processed data.

II. Related work

In [11], authors present four types of security services attacks in VANETs ; routing attacks (e.g., sybil, blackhole attack, etc..), data integrity attack (e.g., masquerading, illusion, etc..), confidentiality attacks (e.g., man in the middle, traffic analysis, etc..) and the availability attacks which include Jamming, Denial of Service (DoS) and DDoS attacks. In this paper, we focused on the DDoS attack. In fact, the DDoS attack is considered as the most common and long-lasting problem which affects basically all the networking architectures where attackers aim to launch attacks from different locations using different time slots [12] by injecting randomly false packets in the network until flooding its resources and targeting its availability.

In [13], authors provided a detection and prevention scheme using a model based on Group formation to give better path for the safe V2V communication by reducing the communication delay and communication loss. Also, in [14], authors provided mathematical formulation to ensure synchronized communication for attack mitigation and improved the MAC layer protocol using Enhanced Distributed Channel Access (EDCA) parameters and contention window control for safe communications.

A RSU monitored method was provided in [15] when false information traffic is recognized and based on analysis safety message is generated. In this work, RSUs monitored the communications between vehicles and infrastructure in order to observe the wrong node activities and the wrong packets too. However, authors in [13], [14] and [15] have not integrate any features of the SDN, Fog Computing or Machine Learning technologies.

Some researchers focused around to bring the SDN and ML innovation to VANET to mitigate the DDoS attack. For instance, an anomaly detection tool based on ML was presented in [16]. Yu. et al designed a platform to efficiently detect and rapidly reduce the response time to the DDoS attack in SDN, which determine all flow entry by the trained SVM. However, this work have not included the powerful features of the fog computing.

Another effort used ML to secure SDVN in [17]. Authors provide a mechanism, using a multi-class support vector machine (SVM) to dynamically detect four different attacks : DoS attack, probing attack, user to root attack, and remote to local attack. The results demonstrate that the effectiveness of this mechanism to classify the types of attacks, as well as good performance. No Fog Computing was integrated in this work.

Also, another effort was introduced in [18]. Authors integrated the ML techniques to mitigate the DDoS attack in VANET by developing a mechanism based on K-means algorithm and depending on the variations of the relative speed between jammer and receiver nodes and generates a new metric namely the variations of the relative speed (RSV). This work did not integrate Fog Computing or SDN features.

Based on the above-mentioned works, none of them combine the Fog Computing, SDN and the Machine Learning techniques in one work. Our proposed architecture aims to combine all of them in one work to take advantages of the powerful features provided by these emerging paradigms explained in the previous section.

III. Proposed architecture

In this section, we introduce and discuss our proposed VANET architecture based on Fog Computing, SDN and Machine Learning. We describe briefly the role of each component and we discuss its potential performance against DDoS attack.

A. Architecture components

To deploy the system, the below components need to incorporate:

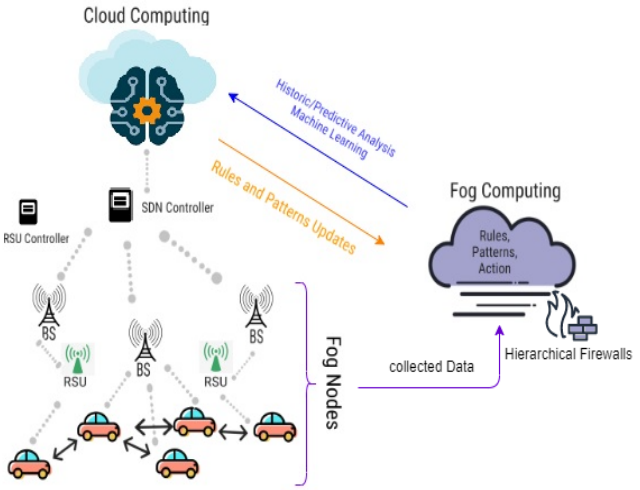

Fig. 1. FCSDVN-ML architecture.

- Cloud Computing (CC) : Attack detection and prediction rules will be generated and updated periodically by Machine Learning (ML) algorithms at the cloud level.
- Fog Computing Servers : The rules generated by ML in CC will be installed in Fog servers close to vehicles in order to accelerate the detection of attacks.
- Hierarchical Firewalls : They will defend against DDoS attack. Hierarchical Firewalls aim to inspect the incoming packets, according to network-level, in order to decide whether the packet has to be either blocked or forwarded to be inspected more deeply by the rules in the upper network-level. Then, the ML algorithms in the CC servers will be notified about the packet filtering decisions. Pseudo-code of this procedure is shown in Algorithm 1.
- SDN Controller : SDNC is the main component of our proposed architecture. In fact, it controls the entire SDN-VANET networking system.
- RSU Controller : It will control all the RSUs in the whole network. They communicate with other RSUC, SDNC, RSUs and BSs through Broadband communications (high-speed connections).
- Road Side Units (RSUs) : They will be controlled by RSUC. These components are running OpenFlow. RSUs are considered also as Fog nodes.
- Basic Cellular Stations (BSs) : In this architecture, BSs are similar to RSUs. They are running OpenFlow, controlled by SDNC and considered as Fog nodes. Beside carrying voice calls and data, BSs will provide fog services too.
- Fog nodes : all vehicles are considered as Fog nodes. Vehicles in this work are the main component of the Data plane. They are equipped with OBUs and supporting OpenFlow protocol.
- Fog Head node : One vehicle will be selected as the fog head node which will work as the intermediate interface between the road level among SDNC and IoT gateways.

B. FCSDVN-ML Communications

In the next figure, we illustrate our proposed architecture's components distributed in three main layers : The Data plane is composed of different end devices (e.g., vehicles, RSUs, humans, IoT gateways, etc..). The application plane composed of different services (e.g., QoS, security, etc..) which communicates with the Data plane. And the most important plane : the control plane composed of clusters of SDN Controllers, Data Centers, Cloud servers , Network Services (e.g., traffic engineering, cloud and fog computing, information gathering, etc..). The control plane communicates with the data plane through the Southbound APIs (e.g., OpenFlow protocol).

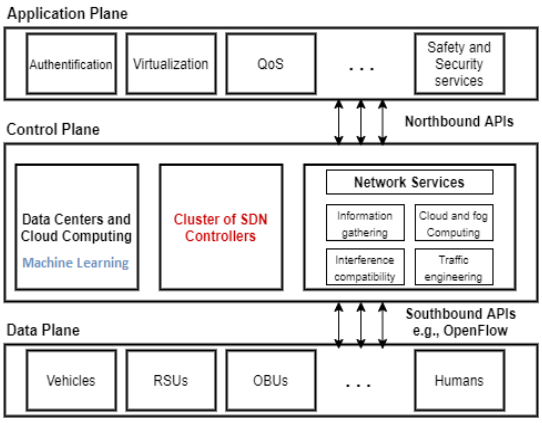

Fig. 2. FCSDVN-ML different layers.

Algorithm 1: Algorithm at level i in the hierarchy of firewalls

```
Update rules (about i^th network-level) from the ML
  algorithms in Cloud servers;
Receive packet P from level i-1 in the hierarchy;
Perform the i^th network-level based inspection of
  packet P;
if P matches a specific rule then
    drop P;
    else
        if level i = 5; application-level inspection then
            Accept P ;
        end
        else
            Forward P to the next level (i+1) ;
        end
    end
end
Notify ML algorithms in Cloud servers about the
  packet filtering decision (for supervised learning);
```

IV. Performance against DDoS attack

Our proposed architecture FCSDVN-ML aims to detect the DDoS attack in a rapid way before it the Cloud level. In fact, Fog computing has a hierarchical architecture which make it a good approach to defend against security attacks in a

hierarchical way. Our rules will be installed in the fog nodes near to the fog vehicles.

For instance, When the attacker inject false packets targeting the switches flow tables, our prediction and prevention rules; which are generated periodically in the CC and installed in the fog servers; will defend against this attack by inspecting packets according to network-level.

As long as we go up in the hierarchy, a deeper inspection is required and the rules require more time to inspect the traffic. In fact, deeper traffic inspection require more resources (e.g., CPU, memory, etc..). For instance, traffic inspection in the application-layer requires more resources than the physical-layer.

As a future work, we plan to estimate the fog nodes resources (CPU, memory, etc.) that should be allocated in the different levels of the hierarchy, in order to inspect the packet with respect to QoS requirements.

REFERENCES

[1] M. Ren, J. Zhang, L. Khoukhi, H. Labiod and V. Vèque, A Unified Framework in Vehicular Ad Hoc Networks, in IEEE Transactions on Intelligent Transportation Systems, vol.19, no.5, pp.1401-1414, May 2018.

[2] Ren, M., Zhang, J., Khoukhi, L. et al. A review of clustering algorithms in VANETs. Ann. Telecommun, 2021. https://doi.org/10.1007/s12243-020-00831-x

[3] M. A. Togou, L. Khoukhi and A. Hafid, "IEEE 802.11p EDCA performance analysis for vehicle-to-vehicle infotainment applications," 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1-6, doi: 10.1109/ICC.2017.7996759.

[4] M. Ren, L. Khoukhi, H. Labiod, J. Zhang and V. Veque, "A new mobility-based clustering algorithm for vehicular ad hoc networks (VANETs)," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 1203-1208, doi: 10.1109/NOMS.2016.7502988.

[5] Mengying Ren, Lyes Khoukhi, Houda Labiod, Jun Zhang, Véronique Vèque,"A mobility-based scheme for dynamic clustering in vehicular ad-hoc networks (VANETs)",Vehicular Communications,Volume 9,Pages 233-241, 2017. https://doi.org/10.1016/j.vehcom.2016.12.003.

[6] A. Tahmasbi-Sarvestani, Y. P. Fallah and V. Kulathumani, "Network-Aware Double-Layer Distance-Dependent Broadcast Protocol for VANETs," in IEEE Transactions on Vehicular Technology, vol. 64, no. 12, pp. 5536-5546, Dec. 2015, doi: 10.1109/TVT.2015.2487998.

[7] S. U. Bhover, A. Tugashetti and P. Rashinkar, "V2X communication protocol in VANET for co-operative intelligent transportation system," 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2017, pp. 602-607, doi: 10.1109/ICIMIA.2017.7975531.

[8] A. Ydenberg, N. Heir and B. Gill, "Security, SDN, and VANET technology of driver-less cars," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018, pp. 313-316, doi: 10.1109/CCWC.2018.8301777.

[9] H. A. Khattak, S. U. Islam, I. U. Din and M. Guizani, "Integrating Fog Computing with VANETs: A Consumer Perspective," in IEEE Communications Standards Magazine, vol. 3, no. 1, pp. 19-25, March 2019, doi: 10.1109/MCOMSTD.2019.1800050.

[10] M. A. Hossain, R. M. Noor, K. -L. A. Yau, S. R. Azzuhri, M. R. Z'aba and I. Ahmedy, "Comprehensive Survey of Machine Learning Approaches in Cognitive Radio-Based Vehicular Ad Hoc Networks," in IEEE Access, vol. 8, pp. 78054-78108, 2020, doi: 10.1109/ACCESS.2020.2989870.

[11] R. Kaur, T. P. Singh and V. Khajuria, "Security Issues in Vehicular Ad-Hoc Network(VANET)," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, pp. 884-889, doi: 10.1109/ICOEI.2018.8553852.

[12] I. A. Sumra, H. B. Hasbullah and J.-L. B. AbManan, "Attacks on security goals (confidentiality integrity availability) in VANET: A survey" in Vehicular Ad-Hoc Networks for Smart Cities, Berlin, Germany:Springer, pp. 51-61, 2015.

[13] Sindhu G, Mittal P., "A novel model based on group controlled observation for DDOS attack detection and prevention in VANET". Indian J Sci Technol 9(36):1–6, 2016.

[14] BiswasS J, Misic M, Misic M. DDoS attack on WAVEenabled VANET through synchronization. IEEE 2nd Global Communications Conference (GLOBECOM); Anaheim, CA. p. 1079–84, 2012.

[15] A. Pathre, C. Agrawal and A. Jain, "A novel defense scheme against DDOS attack in VANET," 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), 2013, pp. 1-5, doi: 10.1109/WOCN.2013.6616194.

[16] 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.

[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] 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.