INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2020.14.122 Volume 14, 2020

Source Fabrication Detection Model based on Key-value Variables in Reactive Protocols of VANET

Fadlallah Chbib
ICD/ERA Lab
University of Technology of Troyes
Troyes, France
fadlallah.chbib@utt.fr

Walid Fahs
CCE Department
Islamic University of Lebanon
Wardanieh, Lebanon
walid.fahs@iul.edu.lb

Jamal Haydar
CCE Department,
Islamic University of Lebanon
Wardanieh, Lebanon
jamal.haydar@iul.edu.lb

Lyes Khoukhi
ENSICAEN, GREYC CNRS
Normandie University
Caen, France
lyes.khouki@ensicaen.fr

Rida Khatoun
INFRES Department
Telecom ParisTech
Paris, France
rida.khatoun@telecom-paris.fr

Abstract: The vehicular communication has been considered as the most promising wireless communication technology in the computer network scenario, the beginning of which has marked a great change for the passengers in the range of safety application. The development of vehicular communication increased security threats and weaknesses. Vehicular communication is exposed to several vulnerabilities such as Denial of Service attacks (DoS), Black hole and fabrication attacks. Fabrication attack consists of a malicious node that modifies information in the packet causing critical damage in the network like congestion and high delay. In this paper, we propose a novel fabrication model which consists of two algorithms one for source attack and another for anti-source attack. In such attack, the malicious node fabricates the source address of the route request message; this means that the malicious node selects randomly from the routing table a source address that is different from the input source address and the source address of the current node and forwards the message to its neighbors. In the anti-attack, our novel proposed algorithm has the role to identify the source attack during the communication. We create two variables at each node in order to check if the input source address in RREQ is equal to the output source address in RREQ; otherwise, the node is identified as a malicious node and an urgent message is broadcasted to all nodes to remove it from their routing table. The proposed algorithm targets to minimize the delay of packets. Our simulation is done using SUMO 0.22 simulator, NS-2.35 and awk scripts; the simulation was applied on Hamra area (Beirut, Lebanon). The results show good improvements in terms of packet delivery ratio and the end to end delay.

Keywords: -Vehicle Ad-hoc Networks, Source fabrication Attack, Reactive Routing Protocol, RREQ, DoD, SUMO, end to end delay, packet delivery ratio, Lebanon.

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) is a network that depends less on infrastructure. Enhancement in safety-related techniques and comfort while driving is the most significant services provided. It permits vehicles to exchange data concerning the safety and traffic analysis. The range of VANET application has increased with the new advances in technology and improvement of smart cities across the world. VANET provides a self-aware system that has the main effect on the enhancement of traffic services and in minimizing road accidents. Vehicular Ad Hoc Networks (VANET) has typically gained the attention of today's researchers, while the existing solutions still not sufficient to realize secure VANET and to protect the network from attacks, trying to reach an acceptable level for both the driver and the manufacturer to complete safety of life and infotainment [1], [2], [3].

The Federal Communications Commission (FCC) has assigned the frequency spectrum for vehicle communications under Dedicated short-range communications (DSRC). DSRC is divided into seven 10 MHz channels, which are currently distributed across the spectrum between 5.850 and 5.925 GHz in bands, numbered between 172 and 184. The channel numbered 178 is used only for safe communication, while there are four service channels numbered 174, 176,180 and 182 that are dedicated for reporting an insecure case. However, channels (172, 184) are used for specific purposes. DSRC forms the basis of IEEE 802.11p, also known as Wireless Vehicle Access (WAVE) [4].

These networks have major features including high mobility and large scalability, allowing them to deliver interesting communication services to both drivers and passengers. Services to the driver include

accident warnings and traffic conditions. Services to the passengers comprise reliable Internet connection. Indeed, drivers can prevent accidents if they get an urgent message half a second before the accident [5]. However, confirming the security of these networks is necessary to guarantee the expected services. Different attacks could expose the VANET's performance from a security point of view [6]. These attacks can be classified into the following types (Fig.1):

(1) Fabrication Attack: in this attack, the attacker sends incorrect information into the network for instance changing the destination address, source address, hop count. The information could be incorrect or the transmitter could assert that it is another node. This attack includes deleting messages, warnings, declarations, personalities.

(2) Sybil Attack: in this attack, the attacker makes multiple identities to simulate multiple nodes. For example, a malicious node forges a large number of fake identities to interrupt the proper working of VANET applications. This attack is very dangerous because a bone node can give its various locations at the same time and this will create security risks.

(3) Denial-of-Service (DoS): in this attack, the attacker targets to shut down a node or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash [7].

(4) Black hole Attack: When a malicious user enters into the network and stops forwarding messages to the next nodes by dropping messages.

(5) Grey hole Attack: This attack occurs if some node drop 50% of the packets and the rest 50% is sent by altering the message. In this way, wrong information is broadcast [8, 9].

Our work focuses on the detection of the fabrication source attack at the routing layer in a vehicular environment in order to reduce the delay of packets and to increase the packet delivery ratio. In this paper, we consider a reactive routing protocol where a source node sends Route Request (RREQ) packets to his neighbors and waits for a Route Reply packet from a destination in order to discover the route between the source and the destination.

In particular, in the source attack algorithm, the source node aims to send a route request message to a destination during the route discovery process, an intermediate node which acts as a malicious node fabricates the source address of the message, it selects randomly from the routing table a source address that is different from the input source address and the current node address and forwards the message to its neighbors. The anti- source attack algorithm aims to discover this fabrication attack by creating two variables at each node, to check if the input source address in RREQ is equal or not to the output destination address in RREQ.

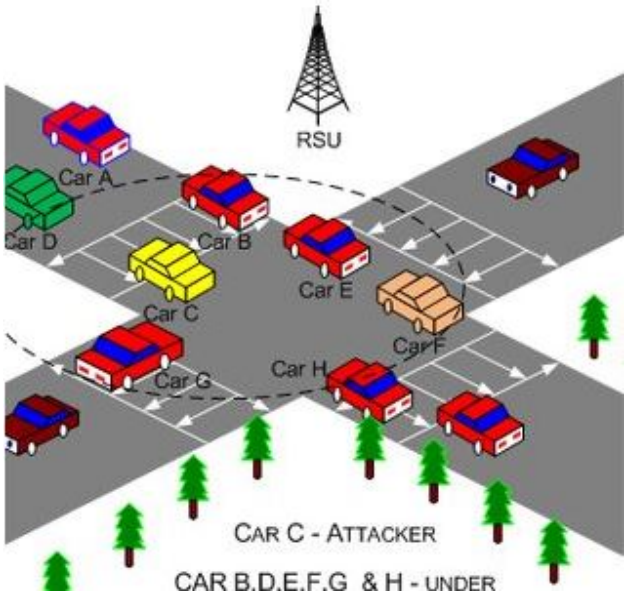

Figure 1: Attack in VANET

The remaining of the paper is organized as follows. A literature review is provided in Section II. Section III presents the two proposed algorithms: the source attack and the anti-source attack. In Section IV, the performance of our proposal is studied, where we compare the results of the two proposed algorithms. Lastly, Section V concludes the paper.

II. RELATED WORKS

In this section, we introduce related work that targets Vehicular network attack, several papers pointed to a different type of attacks, the most significant was fabrication, Denial of service (DOS), black hole and grey hole etc. In [10], the performance model focused to detect the fabrication attacks using statistical analysis of link latencies. A novel solution has been designed requiring a new link to undergo a vetting period during which its latency is evaluated. In [11], the authors explored the impact of different PAI species, fabricated with different materials, on several local-based descriptors combined with the Fisher Vector feature encoding, in order to increase the robustness to unknown attacks. In [12], a different Message Fabrication Detection mechanism, called MEFAD scheme were proposed. This scheme is designed to recognize vehicle-fabricating information in VANETs. The target of the approach is to avoid malicious nodes or vehicles from intercepting packets in transmission. In [13], two methods were presented to diminish the MPR execution number in a way to minimize control message congestion in OLSR. Results revealed the accuracy of the proposed method

in rising both packet delivery and throughput while decreasing the communication overhead. In [14], the authors proposed a novel scheme for recognition of malicious node in Black Hole attack in CR-VANET. In this model, the authors used a Trusty Dynamic Software Agent (TDSA) which are active for each node in VANETs and shares databases in the memory spaces of the neighboring nodes. Moreover, they matched the communication range(R) and the distance between two adjacency nodes. In [15], an active Sybil attack detection algorithm was proposed in order to locate Sybil nodes using short detection packets without adding special hardware or exchanging pieces of information. Different than the previous detection approaches, this algorithm was capable of Sybil detection even in dynamic power environments. The authors of [16] present an intelligent Intrusion Detection System (IDS) which depends on anomaly detection to protect external communications from the grey hole and rushing attacks. These attacks try to avoid transmission between vehicles and roadside units (RSU) and have a straight and bad impact on the extensive approval of this novel class of vehicles. They used two classes of machine learning which are neural network and a support vector machine for the design of the intelligent IDS.

III. PROPOSED MODEL

In this section, we present a new source fabrication model that consists of two algorithms source attack and anti-source attack, it is very significant and novel since it focuses on a sensitive message fabrication that will affect the entire network and cause a lot of damage. The main ideas we are going to focus on in our proposed work are listed below:

1) The RREQ message which contains the sequence number, the source and destination addresses and the hop count.
2) The malicious node selects randomly from the routing table a source address that is different from the input source address and the current node address.
3) Creation of two variables that contain the input source address and the output source address.
4) Check variable 1 and variable 2, and accordingly we identify the node as malicious or not.
5) Update the routing table at each node.

A. Reactive Routing Protocol

Reactive routing protocols are called on-demand routing protocols because the routing process starts by discovering paths when a source node needs to communicate with the destination node [17, 18]. These protocols don't maintain routing information or routing activity at the network nodes if there is no communication. Concerning the route discovery process, it occurs by flooding the route request packets to the neighbors. This process starts once the source sends a Route Request (RREQ) packet and waits subsequently for a Route Reply packet from the destination. The RREQ packet contains the source address, a destination address, hop count, broadcast id and sequence number. While, the RREP packet contains the source address, a destination address, destination sequence, hop count and lifetime.Vehicular Reactive Protocol (VRR), and Stable CDS-Based Routing Protocol (SCRP) is examples of Reactive Routing Protocols [13], [17], [18].

B. Source Fabrication Attack

We consider a reactive routing alternative which relies on the route discovery process by flooding a specific request message (i.e., RREQ) to neighbors in order to find a route from source to destination. This message contains the source address and destination address when the node reaches the destination then sends a reply message (i.e., RREP) that determines the optimal path between the source and the destination according to bandwidth or traffic load [19].

In this section, we propose a new source attack algorithm that fabricates the source address of the input route request at the intermediate node. Our proposed algorithm starts by broadcasting a route request message from the source to the destination to find the different possible paths. Then, the destination node sends, in the reverse path, a route reply message.

In the source attack algorithm, the process starts when an intermediate node receives a packet. Then, we check the type of input packet, if it is not RREQ, the source attack process will end here, otherwise, the malicious node selects distinct random source address from the routing table. Following the context before, we check the input source address and the random source address at each node, if they are the same, we move to the next node, if not, the node switches between the source of the RREQ packet with the selected random source address. After that, the malicious node forwards the RREQ packet to the destination address. The source attack process has a great bad impact on the network, it increases the congestion by sending unneeded packets, besides it decreases the packet delivery ratio because of replying the packets to the fabricated source.

Fig.2 shows an example about the source fabrication attack, node A needs to send data to node G, for that node A needs to discover the route to node G, upon that it sends a route request message to its neighbors. In this case node B will receive a route request from node A, after that node B broadcasts the RREQ packet to all its neighbors with source address A and destination address H. In that context, node C, D and E will broadcast the route request message to their neighbors, while the malicious nodes (C, D) will also

Algorithm 1: Source Fabrication Attack Algorithm

```
Require: String src;
do
packet = receivePacket();
if packet.type == RREQ then
    src = inputpacket.src;
    srcAddress = selectRandomAddress();
    if src =!srcAddress then
        packet.src = srcAddress;
        forwardPacket(packet);
    end if
end if
While packets>0
```

broadcast the message, but by changing the source address from A to E and B respectively (select random source address from the routing table), only node E send the RREQ without changing the source address. The source fabrication allows the destination node G to receive multiple route request packets with different source addresses, from the nodes C, D and F. After that the node G will send many RREP each one according to source built in the RREQ. This process has a great impact on the network, it increases the congestion by sending unneeded packets, besides, and it increases the end-to-end delay through the sending of the data packets to the right destination through the longest path (A-C-E-F-G instead of A-B-C-G and A-B-D-G).

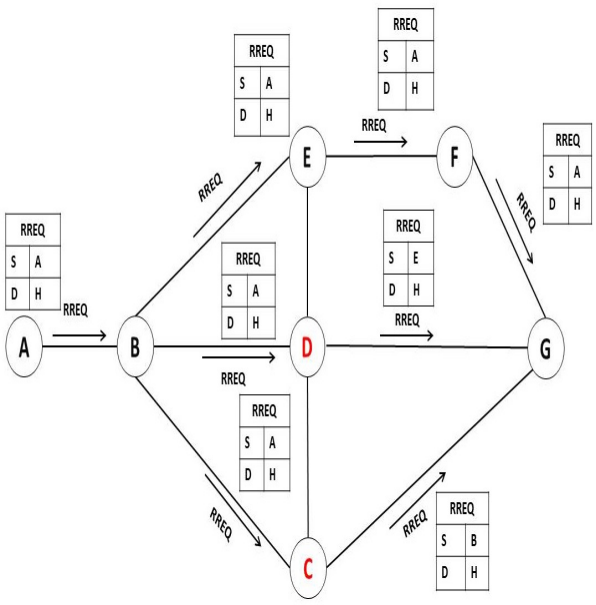

Figure 2: Source Fabrication Attack

C. Source Anti Fabrication Attack

In the source anti fabrication attack algorithm, the process starts by creating two variables and cleaning them at each node. Then, the algorithm checks the type of the input packet, if it is not RREQ, the process ends here, else, we put the input source address in variable 1 and the output source address in variable 2. Following the context before, we check the input source address (variable 1) and the output source address (variable 2) at each node, if they are the same, we move to the next node, if not we detect the current node as a malicious vehicle. After that, we drive a broadcast change message to the neighbor that inform all nodes to remove the malicious vehicle from their routing tables.

Algorithm 2: Source Anti-Attack Algorithm

```
Require: String src1;
Require: String src2;
Require: packet = receivePacket();
if packet.type == RREP then
    src1 = inputPacket.src;;
    src2 = outputPacket.src;
    if src1 != src2 then
        sendChangeMessage(vehicle);
        removeVehicleFromTable(vehicle);
    end if
end if=0
```

IV. SIMULATION

A. Simulation Scenario

In our simulation, we download Hamra file from OpenStreetMap (OSM), then we used this map file in SUMO 0.22 simulator to create a real-time scenario as shown in Fig.3, The mobility of traffic data is generated in SUMO trace exporter [20], [21], [22], [23] [24], [25], [26]; then it is exported to NS2 simulator to study the performance evaluation of our proposed algorithms as depicted in Fig.4. Table I shows a summary of the parameters that have been adopted in this simulation.

The evaluation of our algorithms is analyzed according to different performance metrics.These quantities measurements is useful for assessing the performance of vehicular communication in the proposed attacking and anti-attacking algorithms.

These fabrication algorithms are developed on the reactive routing protocol, where a source sends a RREQ packets to its neighbors and waits for a Route Reply packet from a destination.

The following performance metrics are employed in this study:

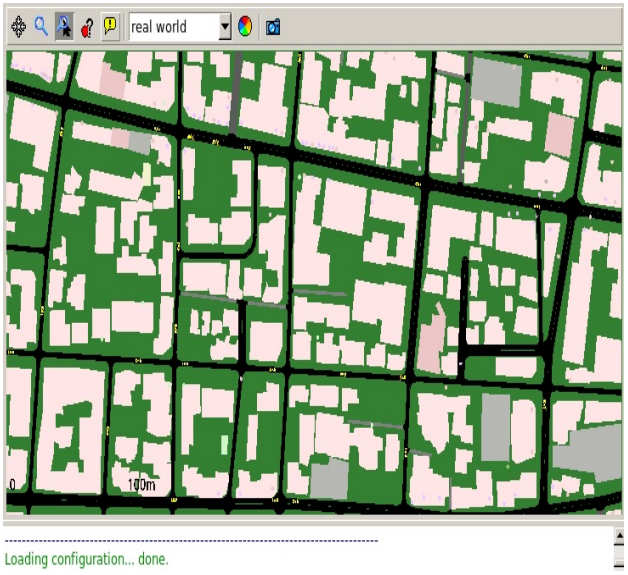

Figure 3: Hamra-Beirut Region Map

1) Packet delivery ratio: the total number of received packets over the number of sent packets.
2) End to end delay: is the time taken by a packet to be routed throughout the network from a source to its destination.
Fig.5 shows an improvement in packet delivery ratio of our proposed source anti-attack reactive routing algorithm (SAAR) with respect to the source attack reactive routing algorithm (SAR). We detect that with 60 vehicles, the packet delivery ratio of the anti-attack algorithm SAAR touched 95%, while in the attacked SAR it touched around 42%. When the number of vehicles increases, the packet delivery ratio decreases; this is typical because the number of route request messages and event messages increases. Although, the SAAR algorithm still achieves better than the SAR in all other cases 80, 100, 120, 140 and 160 vehicles.This improvement is achieved as a result of the early detecting of the malicious node.

Fig.6 specifies an enhancement in the end-to-end delay of our proposed source anti-attack algorithm (SAAR) concerning the source attack algorithm (SAR). We observe that with 60 vehicles, the end-to-end delay value of the anti-attack algorithm SAAR is equal to 5.3 ms, however, in the attack SAR it is equal to 3 ms. However, when the number of vehicles increases to 160, the end to end delay increases in both protocols to 5 ms and 7.5 ms in the SAAR algorithm and attack SAR algorithm respectively, due to the congestion. This specifies that the end to end delay in the source anti-attack algorithm SAAR achieves better than the source attack SAR in all cases.

Table 1: Simulation parameters

Parameters	Value
Simulator	NS-2.35
Traffic Simulator	SUMO
Wireless communication	IEEE 802.11 p
Propagation model	Nakagami
Frequency band	5.9 GHz
Channel width	10 MHz
Number of vehicles	[60,80,100,120,140,160]
Simulation duration	[200 sec]
Communication range	100 m
Network dimension	2500 m * 1500 m

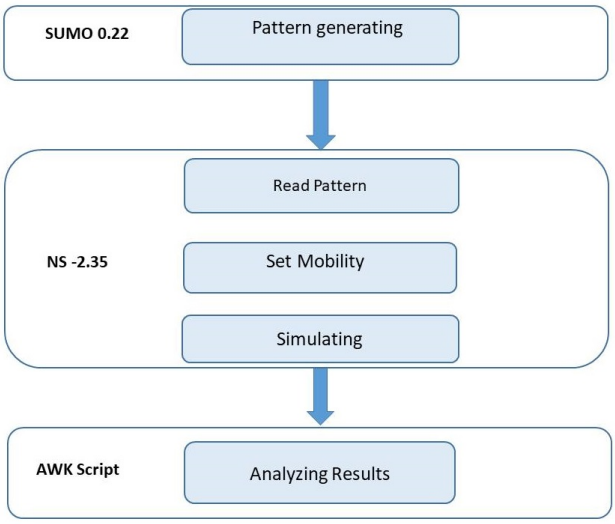

Figure 4: Simulation Process

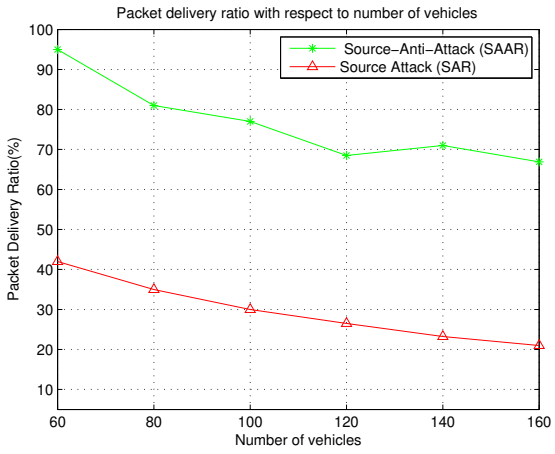

Figure 5: Packet delivery ratio with respect to the number of vehicles

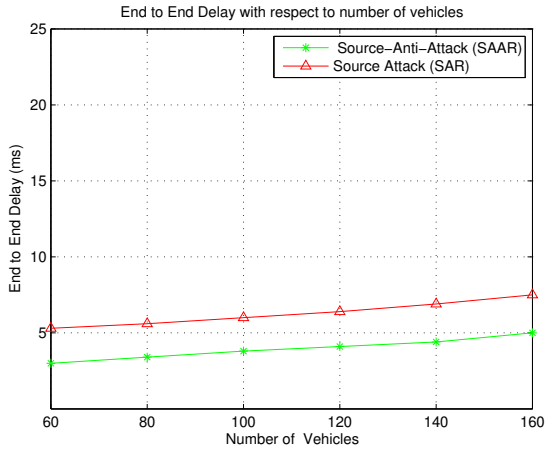

Figure 6: End to end delay with respect to the number of vehicles

V. CONCLUSION

Vehicular communications have become an active area of research and standardization. The communication between vehicles will lead to more efficient and secured roads by providing information about traffic and road conditions to vehicle drivers. In this paper, we proposed two new algorithms, the source attack and the source anti-attack, that are classified as fabrication attacks. In the source attacker algorithm, the malicious node selects a distinct random source address from the routing table. Consequently, the malicious node switches the source of the RREQ packet with the selected source address. Therefore, it forwards the RREQ packet to the destination address. In the anti-attack algorithm, we created two variables and cleaning them at each node. Following the context before, we check the input source address (variable 1) and the output source address (variable 2) at each node, if they are the same, we move to the next node, if not, we detect the current node as a malicious node. Hereafter, we drove a change message to the neighbor that inform all nodes to remove the malicious node from their routing table. The results indicated that an improvement in terms of end to end delay and packet delivery ratio is achieved. For future work, we plan to explore a predictive algorithm that captures the malicious node in the first period of the attack.

References

[1] R. Mishra and A. Singh and R. Kumar, "VANET security: Issues, challenges and solutions," *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 1050-1055.

[2] N. Mathew and V. Uma, "VANET security -Analysis and survey," *International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT)*, 2018, pp. 100-106.

[3] G. Samara and W. A. H. Al-Salihy and R. Sures, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)," *Second International Conference on Network Applications, Protocols and Services*,2010, pp. 55-60.

[4] H. Noun and W. Fahs and A. Kalakech and J. Haydar, "Performance of Revocation Protocols for Vehicular Ad-Hoc Network. Review of State-of-Art Techniques and Proposition of New Enhancement Revocation Method," *2018 2nd Cyber Security in Networking Conference (CSNet)*, 2018, pp.6.

[5] A. Ghandour and H. Hammoud and M. Dimassi and H. Krayem and A. Issa and J. Haydar, "Allometric scaling of road accidents using social media crowd-sourced data," *Physica A: Statistical Mechanics and its Applications*, Vol. 545, 2020.

[6] Sheikh, Liang and Wang, "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)," *Sensors*, Vol.19, 2019, pp. 380-389.

[7] M. Rmayti and Y. Begriche and R. Khatoun and L. Khoukhi and D. Gaiti, "Denial of service (DoS) attacks detection in MANETs using Bayesian classifiers," *2014 IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, 2014, pp. 7-12.

[8] P. Gu and R. Khatoun and Y. Begriche and A. Serhrouchni, "Support Vector Machine (SVM) Based Sybil Attack Detection in Vehicular Networks," *IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1-6.

[9] P. Gu and R. Khatoun and Y. Begriche and A. Serhrouchni, "Vehicle Driving Pattern Based Sybil Attack Detection," *IEEE 18th International Conference on High Performance Computing and Communications*, 2016, pp.1282-1288.

[10] D. Smyth and S. McSweeney and D. O'Shea and V. Cionca, "Detecting Link Fabrication Attacks in Software-Defined Networks," *26th International Conference on Computer Communication and Networks (ICCCN*, 2017, pp. 1-6.

[11] Tyagi, Parul and Dembla, Deepak, "A Taxonomy of Security Attacks and Issues in Vehicular Ad-Hoc Networks (VANETs)," *International Journal of Computer Applications)*,Vol.19, 2014.

[12] S. A. Chhoeun and K. S. N. Ayutaya and C. Charnsripinyo and K. Chamnongthai and P. Kumhom, "A Novel Message Fabrication Detection for Beaconless Routing in VANETs," *International Conference on Communication Software and Networks*, 2009, pp. 453-457.

[13] F. Chbib and A. Khalil and W. Fahs and R. Chbib and A. Raad, "Improvement of OLSR Protocol by Using Bacis Up MPR and Routing Table Mechanisms," *21st International Arab Conference on Information Technology (ACIT)*, 2018, pp.1-6.

[14] S. Mitra and B. Jana and J. Poray, "A novel scheme to detect and remove black hole attack in cognitive radio vehicular ad hoc networks(CR-VANETs)," *International Conference on Computer, Electrical Communication Engineering (ICCECE)*, 2016, pp.1-5.

[15] M.Mohamed and P. Dandekhya and A.Krings, "Beyond passive detection of sybil attacks in VANET," *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2017, pp.384-390.

[16] K. M. Ali Alheeti and A. Gruebler and K. D. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," *7th Computer Science and Electronic Engineering Conference (CEEC)*, 2015, pp. 231-236.

[17] S. I. Chowdhury and W. Lee and Y. Choi and G. Kee and J. Pyun, "Performance evaluation of reactive routing protocols in VANET,"*17th Asia Pacific Conference on Communications*, 2011, pp. 559-564.

[18] J. M. García-Campos and D. G. Reina and S. L. Toral and N. Bessis and F. Barrero and E. Asimakopoulou and R. Hill, "Performance Evaluation of Reactive Routing Protocols for VANETs in Urban Scenarios Following Good Simulation Practices," *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2015, pp. 1-8.

[19] F. Chbib and W. Fahs and J. Haydar and L. Khoukhi, and R.Khatoun , "Message Fabrication Detection Model based on Reactive Protocols in VANET," *2020 4th Cyber Security in Networking Conference (CSNet)*, 2020, pp.5.

[20] F. Chbib and L. Khoukhi and W. Fahs and R. Khatoun and J. Haydar, "Wave Performance Analysis and Enhancement for Safety Applications in Vehicular Networks," *10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2019, pp. 1-7.

[21] Pattnaik, O. and Pattanayak, Binod, "Performance analysis of MANET and VANET based on throughput parameter," *International Journal of Applied Engineering Research*, Vol.19, 2017, pp.7435-7441.

[22] R. Bala and C. R.Krishna, "Performance analysis of topology based routing in a VANET," *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2014, pp.2180-2184.

[23] A. Ghandour and J. Haydar and A. Hariri and J. Chahine , "Aparecium Wi-Fi Planner using Enhanced Indoor Propagation Model," *2020 International Wireless Communications and Mobile Computing (IWCMC)* , 2020, pp. 1106-1111.

[24] J. Haydar and A. Ibrahim and A. Samhat and G. Pujolle, "ABCDecision: A Simulation Platform for Access Selection Algorithms in Heterogeneous Wireless Networks," *EURASIP Journal on Wireless Communications and Networking* , Vol.5,No 3, 2010, pp.12.

[25] Felice, Marco and Ghandour, Ali and Artail, Hassan and Bononi, Luciano, "Enhancing the performance of safety applications in IEEE 802.11p/WAVE Vehicular Networks," 2012, pp.1-9.

[26] D. Krajzewicz and N. Bershad and M. Behrisch and L. Bieker, "Recent Development and Applications of SUMO – Simulation of Urban MObility," *International Journal on Advances in Systems and Measurements*, 2012, pp.128-138.

This project has been funded with the support of the National Council for Scientific Research in Lebanon CNRS-L.