Extending OMNeT++ Simulator to Secure Vehicular Communication under Blackhole Attack

Gerardo Mario Marotta and Floriano De Rango[a]
Institute DIMES Dept., University of Calabria, Via P. Bucci, Rende (CS), Italy

Keywords: VANET, Security, OMNeT++, Black-hole Attack, Vehicular Communications.

Abstract: Vehicular Ad Hoc Networks (VANET) are gaining a lot of interest in these last years. Connected and autonomous vehicles are becoming a reality and security aspects need to be considered in the vehicle's communication and architecture in order to support critical services. In this paper, an additional security module has been proposed and added in OMNeT++ to support security features in vehicle communications. Cryptography and authentication services have been introduced to protect VANET by black-hole attacks. Some attack scenarios have been considered and security features have been proposed to mitigate or avoid these security attacks. Security features increase a little bit the protocol overhead, but they are able to maintain good performance under attack scenario. Performance evaluation has been led out considering as metrics the number of dropped packets, number of sent packets and the end-to-end delay.

1 INTRODUCTION

VANET (Vehicular Ad-Hoc Network) is a kind of Mobile Ad-Hoc Networks (MANETs) where the nodes involved in the communication are vehicles. The messages exchanged among the vehicles concern accidents on roads, roadblocks, speed control, unrestricted way for ambulances and concealed obstacles etc.

The importance of exchanged data makes VANET security a primary aspect in this scope.

VANET is prone to several vulnerabilities and attacks. These vulnerabilities deteriorate the functioning of the network, introducing severe problems in the network and pose potential security threats. The danger of attacks is linked to the purpose of the attack and its impact on the victim.

An attacker in vehicular network could steal, modify or drop the end-user personal information transmitted in the network, compromising confidentiality, integrity, authentication and availability. Security is a critical issues in many field such as emphasized in (Fazio et al., 2020)(De Rango et al., 2020)(M.Mehic, 2016),(De Rango et al., 2006)(F. Rezac, 2011). However, VANET and autonomous vehicles can increase the importance of the security considering the possible consequence that a security attack can determine. The vast vehicular set and the rapid change in the position increase the complexity for securing the vehicular networks. (Arif et al., 2019).

Routing protocols (Singh et al., 2020) are parts of VANET scenarios interested by security threats. Thus, vehicles in VANET work like routers for transmitting data between nodes. Malicious node could lead to various attacks, such as Black Hole.

Simulation frameworks do not offer features to implement security solutions to VANET's attacks.

The main contribution of this paper is to integrate OMNeT++ simulator with Crypto++ library to evaluate some security mitigations introduced to stem Black Hole attack in VANET context.

Sumo has been used to realize traffic simulation, whereas Veins allows the communication between the previous frameworks.

The paper is organized as follows: section 2 presents some works related to routing over VANET; section 3 presents the tools used to implement the attacks and the mitigations, and to evaluate them; section 4 describes mitigations' details; section 5 shows the results collected during the simulations and, finally, conclusions are summarized in the last section.

[a] https://orcid.org/0000-0002-3882-1678

Marotta, G. and De Rango, F.
Extending OMNeT++ Simulator to Secure Vehicular Communication under Blackhole Attack.
DOI: 10.5220/0010568703780385
In *Proceedings of the 11th International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2021)*, pages 378-385
ISBN: 978-989-758-528-9

2 RELATED WORK

In this section some works related to routing over VANET and security issues in the reference context are presented.

2.1 VANET Routing

Routing protocols applied in VANET gained a lot of interests in these last years, especially, considering the specific characteristics of VANET technologies such as high and constrained mobility, not energy limited nodes and partial infrastructure that is possible to use. A lot of work has been done in the MANET context regarding dynamic and efficient routing. Some protocols applied in MANET could be applied with some modifications and extensions also to the VANET. In particular, for the specific case, we have to consider that routing strategies need to quickly discover the path from source to destination considering the frequent route breakage that can happen in a highly dynamic scenario. Moreover, it is suitable to not maintain always updated the topology if there is not traffic between vehicles. Many routing strategies have been proposed for VANET and they are classified in two main macro-categories (Devangavi and Gupta, 2017):

- ***topology driven routing;***
- ***location-based routing***.

The first one uses the network state info and routing protocols build a table where IP addresses of nodes, next hop node and path metric are considered. The second category, instead, uses node location or geographic area to decide where to forward data packets and no network topology is maintained among nodes. The first category has been extensively applied in VANET because many of table-driven protocols have been standardized and are well-known in literature. Table-driven routing can be furtherly classified in two categories (Hayat et al., 2019):

- ***proactive:*** they maintain periodically the routing table through a continuous protocol packet exchange.
- ***reactive:*** they create a route only when there are data to transmit among vehicles. This approach tries to avoid to overload the network of control packets even in situation where there is no data traffic.
- ***hybrid:*** they use both techniques presented above combining in some part of the network a proactive approach and in other part pf the network the reactive strategy.

In our case we focused on a well know reactive protocol such as presented in (Santamaria et al, 2019). However, we considered some possible security threats that is present in the classical AODV version.

2.1.1 AODV Protocol

AODV (Perkins et al., 2003) is an on-demand table-driven routing protocol. It makes use of three routing protocol packets such as referred below:

- ***Route Request (RREQ)***
- ***Route Reply (RREP)***
- ***Route Error (RERR)***

The path is discovered only when the source has data to send. AODV is composed by two phases:

- ***Route Discovery:*** it is started when the source has data to send towards the destination;
- ***Route Maintenance:*** it is applied where there is a route breakage in order to remove broken link and start again the route discovery.

AODV uses the minimum hop count as path metric and it uses source and destination sequence number to avoid loop formation in the network. The RREQ is the message generated by source to discover the path toward the destination and it includes the source sequence number. Typically, this sequence number is incremented by one for each new RRE generated by the source. When the RREQ arrives at the destination, a RREP is generated and forwarded on the reverse path forwarding. The RREP carries the destination sequence number set as the maximum between the DSN (Destination Sequence Number) included in the RREQ and the value maintained in the node routing table. Every node associates a sequence number to each destination in order to maintain always updated the route. The higher destination value means a more recent info. Manipulating the DSN value can affect the network performance and it is possible to perform some network attacks.

2.2 Security Attacks over VANET

A VANET is a network where it is possible to apply attacks similar to those applied in MANET context. In the following some possible attacks are recalled and a focus on the blackhole considered in this work has been also presented.

2.2.1 Attacks Classification

It is possible to see different network attack types over VANET (Phull and Singh, 2019):

- ***Network Attack (NA):*** they have the target to limit or block the network resources such as bandwidth, transmission opportunity;
- ***Application Attack (AA):*** it has the objective to change the content of messages at application layer in order to create accidents or congestion.
- ***Timing Attack (TA):*** it consists in the time slot modification to produce a transmission delay.
- ***Monitoring Attack (MA):*** they make use of monitoring system to violate the secret of messages exchanged in V2I and V2V way.

On the basis of the attack classes it is possible to consider different kinds of attackers (Goyal et al., 2019):

1. ***Active:*** attacker is hided in the network with the objective to manipulate messages of legacy users;
2. ***Passive:*** it can act without modifying messages but sniffing or monitoring packets exchanged among legacy users;
3. ***Internal:*** attacker authenticated and authorized in the network that can change its behavior to produce damages knowing some specific network vulnerability;
4. ***External:*** it can act externally to the network performing attacks to limit network resources or discover secret keys;
5. ***Rational:*** external or internal entity that performs active attack to obtain specific benefits;
6. ***Malicious:*** external or internal entity performing attacks to produce damage on the network.

2.2.2 Black Hole Attack in VANET

AODV (Ad-hoc On-demand Distance Vector) is one of routing protocols that has been applied in the VANET context. It is proactive and on-demand and it can work under dynamic conditions such as vehicles moving in an urban or sub-urban context. However, AODV present in its basic version some vulnerability related to the route discovery procedure and protocol message exchange. Moreover, it does not guarantee integrity to messages. This means that an attacker can modify messages fields or it can generate false messages.

Among many possible security attacks that is possible to apply on AODV, the attention is focused on the Black Hole attack. This last one has the objective to act in the route discovery from source and destination to alter the legacy path (Fiade et al., 2020). Moreover, it can act on the RREP packet in the reverse path forwarding. The attack considers two phases:

- ***Route Discovery Alteration:*** after receiving the RREQ packet, the attacker performing the black-hole create a RREP where it sets to an high value the ***Destination Sequence Number*** and it sets the ***Hop Count*** to a zero value. This packet modification determines that the originator of the RREQ will include the attacker in the path because it considers this path the best;
- ***Packet Dropping:*** after performing successfully in the previous phase, the attacker can act internally dropping some packets forwarded on the legacy path from source to destination.

In brief, a malicious node cheats the routing protocol such as it presents itself for having a short route for forwarding the packet to the destination (Arif et al., 2019).

3 TOOLS

In order to analyze some security threats such as black hole attack, some well-known tools such as OMNeT++, INET, Veins e SUMO (Haidari and Yetgin, 2019) have been used. All these tools have been integrated with the Crypto++ library in order to integrate some security features applying cryptographic techniques, directly in the INET modules, like shown in Figure 1.

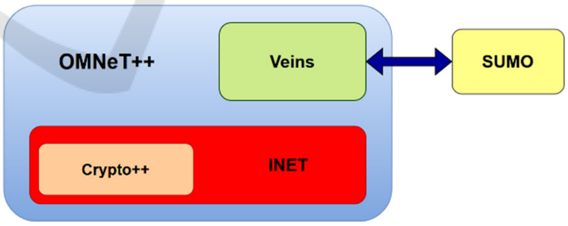

Figure 1: Tools integration.

3.1 OMNeT++

OMNeT++ is a well-known discrete time network simulator (OMNeT++, 2021). It is composed by the following components:

- A set of NED files useful to define the network scenario, simulation parameters, network interfaces and modules connections. It allows to define node types and to connect specific network protocol to nodes and interfaces;

- A file called omnetpp.ini to manage configurations and model parameters. It is possible also to plan more simulations with different parameters;
- A set of files .msg to model communications and packets. It is composed by attributes and data structure defined in C++ language;
- Source file compiled in C++; these files include all classes defined to characterize nodes, protocols and other network features.

3.1.1 INET

INET (INET, 2021) is an open-source library used in OMNeT++. It offers telecommunication protocols, agents and other models. INET is composed by modules communications between them through messages. These modules can be combined to realize new components. It is used to design and validate new protocols.

3.2 SUMO

SUMO (SUMO, 2021) is an open-source simulation suite to generate vehicular traffic. It has been released in 2001 and it allows the inter-modal traffic modeling considering vehicles, public transportation system and pedestrians. SUMO provides a broad set of tools to create, set and evaluate traffic simulations, path computation, CO2 emissions computation etc. SUMO can be extended with customized models and it provide API to control simulations. It offers plug-in able to generate vehicles path, to show vehicles and streets in a graphical interface and the possibility to import real maps using external program such as OpenStreetMap.
The environment can be defined and implemented through the filling of some specific files such as presented below:

- ***.node.xml*** and ***.edg.xml*** files that provide vehicles network info;
- ***.rou.xml*** file including traffic and vehicles route information;
- ***.con.xml*** and ***.typ.xml*** with additional information of rules defining vehicle movement on the streets;
- Optional additional file created by the ***polyConvert*** application, to describe with more details path in urban environment to model more realistic scenarios.

SUMO provides applications to create scenario in the *.xml* format to simplify the representation. ***NETCONVERT*** is an example of these applications able to convert files in specific SUMO formats.

3.3 Veins

Veins (Documentation Veins, 2021) is an open-source framework to simulate vehicles networks and VANET models. These models are executed by OMNeT++ that can interact also with SUMO. Some Veins components can also configure, execute and monitor the simulation.
Both simulators are connected through a TCP sockets. The protocol adopted for this communication is standardized and called ***Traffic Control Interface*** (*TraCI*). This connection allows a joint simulation between vehicular traffic and network traffic. Vehicles movement on the streets is reflected as nodes movement in OMNeT++. Nodes can interact with vehicle traffic at runtime.
Veins instantiates a network node for each vehicle instantiated in SUMO. Every instantiated node is related to an OMNeT++ module that can contain a mobility sub-module of TraCIMobility. At periodical interval the manager can use this module to let SUMO simulation time go on updating the node mobility info such as position, speed and direction in the basis of the vehicle behavior.

3.4 Crypto++

Crypto++ (Crypto++, 2021) is an C++ open-source library, that provides security API to create security policies. It provides cryptographic schemes such as AES, RSA, ECC etc. AES and RSA have been used in our proposal and simulations.
In particular, the use of AES as a symmetric cipher ensures the confidentiality of the communication between VANET nodes.
RSA, on the other hand, through the mechanism of digital signatures, guarantees the authenticity of the of specific fields of protocol’s packets exchanged among vehicles.
The choice of this library is linked to the program language used by OMNeT++ developers to implement simulator’s modules. So Crypto++ make easier to integrate security mechanism in OMNET++.

4 BLACK HOLE ATTACK MITIGATIONS

In this section some mitigation techniques to blackhole attack will be presented.

4.1 Mitigation 1: Solution

A first mitigation solution can make use of the cryptography applied to a known filed of the RREQ packet. This ciphered field can testify the node identity because it is based on a pre-shared key between source and destination. In this solution the destination node generating the RREP that is also the receiver of the RREQ can cipher the specific field using the key pre-shared with the source. Moreover, the Source Address included in the RREQ is included in the created RREP forwarded on the reverse path forwarding. In this way the attacker node performing the black hole attach, cannot easily create a false RREP at the destination because it should forge the crypted string included in the RREP packet. This cannot happen if the attacker does not know the pre-shared key between the source and the destination. Applying the mitigation explained, the source node can accept the RREP only if the decrypted test presents the same IP address. This proposed technique can be effective if the only node that can answer to a RREQ is the destination node and this means that under this mitigation technique it is not allowed a partial reply by intermediate node. The cryptographic operations adopted for this case are AES with 128 bits pre-shared keys.

4.1.1 Mitigation 1: Considerations and Issues

The mitigation 1 does not resolve completely the black hole attack. If the intermediate node answering wants to be activated to reduce the control overhead in the route discovery procedure, the Mitigation 1 can fail in protecting by black hole attack. Intermediate nodes do not have the capability to discriminate a legacy RREP by a forged RREP because they cannot access to the crypted field because they do not know the pre-shared keys. This means that they can process the RREP generated also by attackers and they can update their routing table on the basis of false information contained in forged RREP. In this case, forged RREP with some fields modified by the attacker can arrive at the source node that will forward the data towards the attacker that can apply DoS attack dropping data packet. In this case, the attacker will avoid to alter the RREQ but in a smarter way it will try to modify the RREP changing some important field such as the hop count and destination sequence number in order to let the source to believe that the best path can pass through the attacker node. In this case the attacker will be inside the legacy path and it can attack internally the network applying black-hole or gray-hole attacks.

4.2 Mitigation 2: Solution

The objective of this mitigation solution is to avoid that attacker can modify the Destination Sequence Number. To perform this task the RSA algorithm with the use of a private and public keys is considered. To guarantee the RREP DSN integrity, the node generating the RREP should cipher the field in the RREP using its private key including its cyphered text in a field. In this way the node receiving the RREP should verify the RREP DSN content applying a decryptography with the public key of node generating the RREP. This means that the attacker cannot simply change the value of a field inside the RREP, but it needs to cipher the text with a private key of the node generating the RREP. This is not a trivial job because it should know the private key of the RREP generator. The application of the asymmetric cryptography can face the problem of the alternation of the RREP at intermediate nodes.

In order to activate the answering by intermediate nodes to a RREQ, the intermediate node should be able to build correctly the cyphertext and it should know the private key of the destination. This is necessary because if it will try to forge the RREP it should sign the packet with a private key. In this case the source node, when receiver the false RREP is able to detect the forged packet because it cannot decrypt it. Moreover, it is not so easy for the intermediate node to know the private key of the destination considering the robustness of the applied cryptography. In order to integrate the proposed mitigation technique inside the AODV protocol some modifications should be performed:

- When a receiver node receives for the first time a RREP from a node X that it does not know, it updates its routing table and it maintain also the ciphered DSN inside the RREP packet.
- For the next RREQ towards X, that node does know yet, the intermediate node will generate RREP taking care to include in the ciphertext field of the RREP, the ciphered text stored in the previous point.

It is important to notice that the RREQ contributes to update the node routing table on the basis of the Source Sequence Number (SSN) fixed by the source generating the RREQ. An intermediate node receiving the RREQ compare the SSN with the DSN associated to the source and stored in its routing table and if it is higher an update is performed. To guarantee the SSN integrity, it is necessary to cypher it through its private key. Also, this ciphered SSN should be stored by intermediate node in the routing table and it can be used later when intermediate node has to answer to the RREQ.

5 ATTACKS MITIGATION ANALYSIS

The reference scenario adopted in our simulation is related to a square 1Km^2 area in the Cosenza city such as shown in Figure 2. A number of vehicles equals to 32 is considered where nodes can be source, destination, intermediate node and some of the, can be attackers. Two different attacks are performed. The first one where destination node try to alter the RREP (Attack 1) and the second one where intermediate node try to forge the RREP.

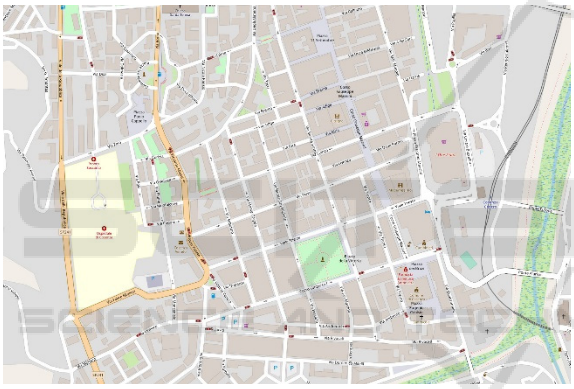

Figure 2: Simulated City Map Area.

5.1 Performance Evaluation Metrics

In order to evaluate the effects on the network under security attacks, some countermeasures have been implemented and tested. The following performance metrics have been considered:

1. ***RREQ Sent:*** RREQ number generated and forwarded by a node;
2. ***Sent RREP:*** RREP number generated and forwarded by a node;
3. ***Sent RERR:*** RERR number generated and forwarded by a node;
4. ***Received RREQ:*** RREQ number received by a node;
5. ***Received RREP:*** RREP number received by a node;
6. ***Mean Discovery Time (MDT):*** average time between RRRQ forwarding by source and the reception of the relative RREP;
7. ***Mean Hop Count:*** average hop count number related to the discovered paths;
8. ***RREQ E2E Delay:*** RREQ delay computed in the propagation from source to destination;
9. ***E2E RREP Delay:*** RREP delay computed in the propagation from destination to source;
10. ***AODV Encryption Time:*** total encryption time computed on every AODV packet;
11. ***AODV Decryption Time:*** total decryption time computed for each decryption operation applied on every packet.

Let us analyze now the performance evaluation of the network under different situations with and without blackhole attacks.

The following scenario have been studied:

- ***Scenario 1:*** a simple scenario where all nodes are legacy and no attack is performed;
- ***Scenario 2:*** scenario where the first type of attack is performed but no countermeasure is applied.
- ***Scenario 3:*** scenario with the first type of attack and where the fist mitigation is considered.
- ***Scenario 4:*** scenario where the second type of attack (Smart Black Hole) is applied and only the Mitigation 1 is applied.
- ***Scenario 5:*** scenario where some type 2 attack is performed and where the Mitigation 2 is considered.

5.2 Performance from Sender Perspective

In this sub-section it is analyzed the performance of nodes generating the RREQ for the route discovery and the nodes generating RERR and RREP to see what happens in the different scenario listed above. The MDT is evaluated in Figure 3 to see as it can change is an attack is performed. It is possible to see as in scenario 2 the MDT presents the lowest value. This could apparently seem to be a good result but it is only due to the collateral effect that intermediate nodes can forge the RREP reducing the MDT but creating unsuitable paths. On the contrary the scenario 5 that is the most secure the MDT increases because heavier cryptography approach (asymmetric crypto) is applied. In scenario 3 the MDT is lower because a lighter cryptography (symmetric) is applied. However, in scenario 3 there is the possible vulnerability to attack of type 2.

Obviously the E2E RREP Delay is observed to be lower in comparison with the MDT but it is expected because this metric in included in the MDT.

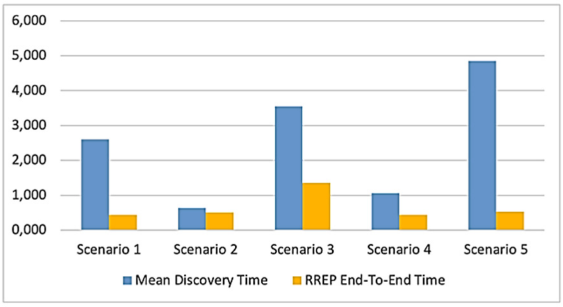

Figure 3: MDT sender.

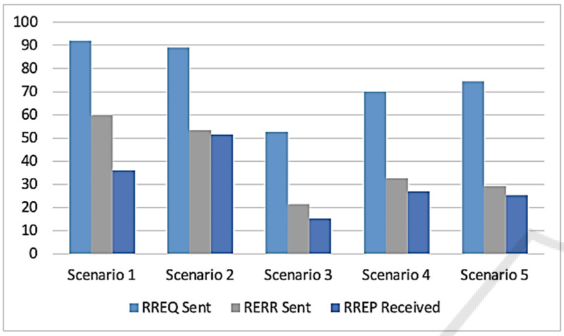

Figure 4: AODV sender packets.

Concerning the AODV protocol packets, as shown in Figure 4, in scenario 2 it is observed a high value of RREP received at the source, this is due to the attack of type 1 that is not mitigated. It is possible to see also as the number of RREQs is proportional to the number of RERRs and this is due to the route breakage related to the node mobility.

5.3 Performance from Receiver Perspective

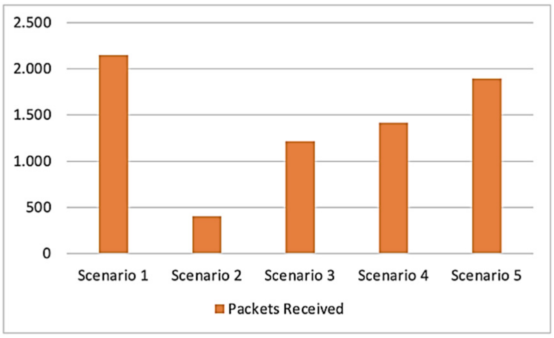

Figure 5: Receiver packets.

The number of packets received, as shown in Figure 5, by nodes change on the basis of the considered scenarios. It can have a value between 405 and 2148. The first value represents the lowest value obtained in the scenario under attack and without mitigation. The higher values such as 2148 and 1897 are obtained for scenario under attacks where the mitigation can reduce or block the attackers effect. The lowest value or received packets testify as the blackhole attack tries to drop packets reducing the number of received packets. Such as expected, the highest value is registered in the scenario 1 where without attacks a higher number of packets can be received without malicious dropping.

5.4 Black Hole Nodes

The number of sent and received packets generated by black hole nodes is zero such as expected because they do not generate new packets, but they will drop received packets. In scenarios without mitigation solutions the number of dropped packets is higher such as shown in Figure 6.

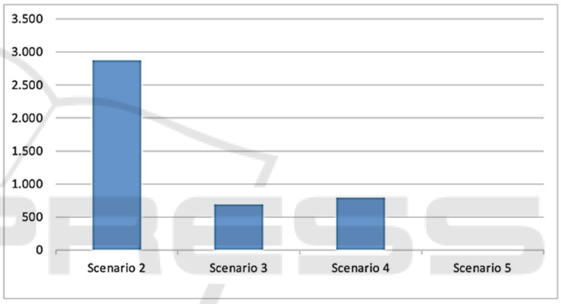

Figure 6: Black Hole packets.

Concerning the packets generated during black hole attack, as shown in Figure 7, it is possible to see as the most important packets to analyze are RREP packets because they are used and forged in the first part of the attack. The highest sent RREP packets are observed in scenario 2 and scenario 3 because RREPs are generated by malicious node whereas in scenario 4 and scenario 5 RREP are not generated by malicious nodes but they are only forwarded.

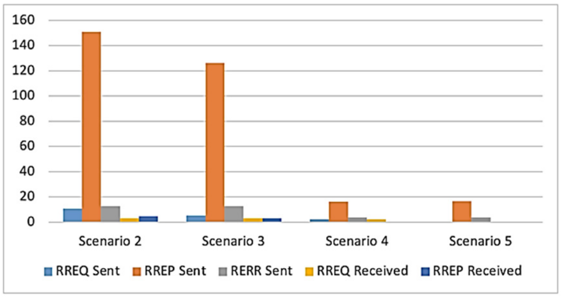

Figure 7: AODV Black Hole packets.

6 CONCLUSIONS

This work analyses some routing threats over VANET. The black hole attack has been evaluated proposing two possible attacks: one simple attack applied at the destination and another one that can be applied by intermediate nodes that can forge a RREP packet and then can perform an inside attack dropping data packets. To face these security issues, it is necessary to use cryptography to provide integrity to some field in the RREQ and RREP packets or to use a more complex asymmetric cryptography to authenticate the RREQ and RREP packets providing both authentication and integrity. Both security solutions have been evaluated considering different scenarios where attackers can perform the simplest attack or the smarter black hole attack. The second mitigation technique has been shown to be more effective increasing a little bit more the AODV protocol complexity.

REFERENCES

Arif, M., et al., J., 2019. *A survey on security attacks in VANETs: Communication, applications and challenges, Vehicular Communications*, Volume 19.

K. Singh, G. Mishra, A. Raheem and M. Kumar Sharma, *Survey Paper on Routing Protocols in VANET*, *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida, India.

A. D. Devangavi and R. Gupta, 2017. *Routing protocols in VANET — A survey*, *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Bengaluru, India.

S. Hayat, X. Liu, Y. Li and Y. Zhou, 2019. *Comparative Analysis of VANET's Routing Protocol Classes: An Overview of Existing Routing Protocol Classes and Futuristic Challenges*, *2019 IEEE 2nd Int. Con. on Electronics Technology (ICET)*, Chengdu, China, 2019.

A.F. Santamaria, P. Fazio, P. Raimondo, M. Tropea, F. De Rango, 2019. *A New Distributed Predictive Congestion Aware Re-Routing Algorithm for CO^2 Emissions Reduction,* in IEEE Trans. on Vehicular Technology, Vol. 68 (5), 2019, pp.4419-4433.

C. Perkins, E. Belding-Royer, and S. Das. *2003. RFC3561: Ad hoc On-Demand Distance Vector (AODV) Routing*, 2003. RFC Editor, USA.

N. Phull and P. Singh, 2019. *A Review on Security Issues in VANETs, in 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2019, pp. 1084-1088.

A. K. Goyal, A. Kumar Tripathi and G. Agarwal, 2019. *Security Attacks, Requirements and Authentication Schemes in VANET*, *2019 Int. Conf. on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Ghaziabad, India, 2019.

A. Fiade, A. et al. 2020. *Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad-Hoc Network)*, *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, Pangkal, Indonesia, 2020.

M. J. Haidari and Z. Yetgin, 2019. *Veins based studies for vehicular ad hoc networks*, *2019 Int.l Artificial Intelligence and Data Processing Symposium*, Malatya, Turkey, 2019.

OMNeT++ -Simulation Manual." [Online]. Available: https://doc.omnetpp.org/omnetpp/manual.

Inet Framework." [Online]. Available: https://inet.omnetpp.org/.

SUMO User Documentation -Sumo." [Online]. Available:https://sumo.dlr.de/wiki/SUMO_User_Documentation#Introduction.

Documentation -Veins. [Online]. Available: https://veins.car2x.org/documentation/.

Crypto++ Library: free C++ class library of cryptographic *schemes*[Online] https://github.com/weidai11/cryptopp.

P. Fazio, M.Tropea, M.Voznak, & F. De Rango, (2020). On packet marking and Markov modeling for IP Traceback: A deep probabilistic and stochastic analysis. Computer Networks, 182, 107464.

F. De Rango, M. Tropea, & P. Fazio, (2020, July). Mitigating DoS attacks in IoT EDGE Layer to preserve QoS topics and nodes' energy. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops.

F. De Rango, G. Potrino, M. Tropea, & P.Fazio, (2020). Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. Pervasive and Mobile Computing, 61, 101105.

F. Rezac, et al., Security analysis system to detect threats on a SIP VoIP infrasctructure elements. (2011) Advances in Electrical and Electronic Engineering, 9 (5), pp. 225-232.

M. Mehic, P. Fazio, M. Voznak, E. Chromy, Toward designing a quantum key distribution network simulation model, (2016) Advances in Electrical and Electronic Engineering, 14 (4), pp. 413-420.

F De Rango, DC Lentini, S Marano, (2006). Static and dynamic 4-way handshake solutions to avoid denial of service attack in Wi-Fi protected access and IEEE 802.11i, in EURASIP Journal on Wireless Communications and Networking 2006, pp.1-19.