RESEARCH ARTICLE OPEN ACCESS

Analysis Study of Routing Protocols Performance and RSU Attack for E-Call Service in VANET

Nour Hasan Agha [1], Majd Zhlat [2], Mothanna Alkubeily [3], Ahmad S. Ahmad [4]
Fourth Year Student [1], Assistant Professor [4]
Department of Medical Engineering
Al-Andalus University, Alkadmous - Tartous, Syria
Fifth Year Student [2], Assistant Professor [3]
Department of Mechanical and Electrical Engineering
Tishreen University, Lattakia, Syria

ABSTRACT
The aim of our paper is to study some protocols used in Vehicular ad-hoc networks (VANET) for medical applications, using the Network Simulator (NS2), by applying two scenarios. The first is applied in a crowded area such as city centers, and the second is applied to the less crowded areas such as the countryside. In addition, we study the types of attacks on these networks and their effects on the network, we will focus our study on the analysis of the RSU attack based on the VANETSIM simulator and discuss the results.
Keywords :— VANET, AODV, DSDV, e-call service, VANETsim.

I. INTRODUCTION

VANET (Vehicular Ad-hoc NETwork) is a self-regulated, decentralized network consisting of a range of mobile, transceiver and Global Position System vehicles, designed specifically to provide connectivity between vehicles or between them and Roadside Unit (RSU), which is located on the roadside [1]. The new vehicle technologies are evolving with new technologies such as electronic minds and communication devices to make road use more comfortable and secure. The vehicles communicate directly with each other without the need to go through the road infrastructure; the goal is to increase safety by sending the required information from one vehicle to another, for example, a vehicle that detects an ice road tells the vehicles traveling from the opposite side of the road. We use roadside units (RSUs), to gather, collect and analyse information transmitted in real time, and then generate traffic information, which include intermediate speed of vehicles, vehicle density and events such as traffic congestion. Then, this information is transmitted to vehicles at a relatively close distance, suitable for urban transport. Each car will be equipped with an 802.11 or 802.16 WiMAX wireless device to enable cars to communicate with each other, as well as RSU to connect remote cars to one another or to connect to the Internet, and even connect trains and aircraft to this network, making the volume of information exchange very large. However, these networks are not safe enough and are on the focus of the attackers who used their wireless communications to launch attacks on them to achieve their own goals [2]. The most important applications in VANET [3], which aim to reduce road traffic injuries and deaths, include: Avoid collisions and detect road obstacles, Driver Assisting Service, E-call service.

E-call service is a project initiated by the European Commission [4], which aims to provide rapid assistance to drivers by sharing a collision anywhere in the EU. In case of failure, the e-call vehicle calls the nearest emergency center, even if the passengers are unable to connect; due to injuries sustained during the incident. Medical services are one of the most important applications of the VANET Networks.

Due to the wireless connections in VANET, the security of these networks is one of the most important challenges. Due to the problems that can be caused by any security failure in these networks of human accidents in the first place, traffic congestion, and disruption of the interests of the population and passengers, and comfort in the second class. We will simulate two different scenarios using (VANETsim) to study, analyse one of the types of attacks on the network.

The reminder of this paper is organized as follows: In section II, we study the routing protocols and the attacks in VANET networks.. In section III, we compare two routing protocols for e-call service using ns-2 and we evaluate the RSU attack over VANET using VANETsim. Finally, conclusion and future work are presented in section IV.

II. RELATED WORKS

A. Routing Protocols in VANET Networks

Routing protocols in VANET are classified into two main categories [5-8] as shown in fig (1).

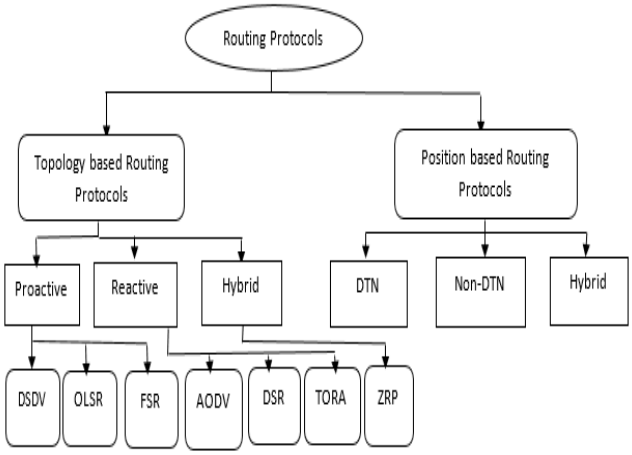

Fig. 1 Classification of VANET routing protocols

A.1 Position based routing protocols

The protocols of this category depend on location information to determine the next hop to reach the goal. However, our study relied on Topology based routing protocols.

A.2 Topology based routing protocols

These protocols use link status information in the network to route packets and in turn divide them into three basic types: Proactive, Reactive and Hybrid Routing Protocol.

Proactive routing protocol depends on the control packets transmitted regularly by all the nodes in the network. Next, the routing table that contains the nodes and the input that the data packet must follow is constructed to access the next node to reach the specified target. The basic feature of these protocols is that there is no need to discover the path as long as the path to the destination is pre-existing and permanently provided. They are also called table driven routing protocols.

The main idea of **Reactive routing protocol** is that the path is created only when a node need to communicate with another one. It stores only the path currently in use, thus reducing the load on the network compared to the proactive protocols. These protocols include a phase called discovery of the path where the source node must send discovery messages to the network in order to find the best path towards a specific target. This phase is completed when this path is found.

While the basic idea of **Hybrid routing protocol** is used to determine optimal network destination routes and report network topology data modifications. It divides the network into zones and use the proactive routing protocols intra-zone and the reactive one's inter-zones.

B. Attacks on VANET

The security of VANET is one of the most important issues because information flows through a wireless medium, which is vulnerable to hacking and this will negatively affect the performance of the network. Therefore, this network is vulnerable to many attacks, the most dangerous are: Network attack, Application attacks, Timing attack, Social attack, Monitoring attack…etc [2]. We will only discuss attacks that concern our search.

An attacker in this category can directly affect other vehicles, has the highest priority, and can affect the entire network. The main purpose of these attacks is to create a problem for legitimate users of the network. We will discuss the DoS and DDoS attacks.

B.1 Denial of Service (DoS)

The network availability is the basis of any network as all users rely on it, so DoS is one of the most serious attacks on the network level in which the attacker disables the main communication center, which leads to the lack of access to legitimate users and the denial of access to Network Services [9]. Figure (2) shows a scenario of DoS attack, Attacker A launches a DoS attack on the vehicle network and disables all communication between V2V and V2I, as a result, B-C-D legitimate users cannot communicate with each other or with the infrastructure.

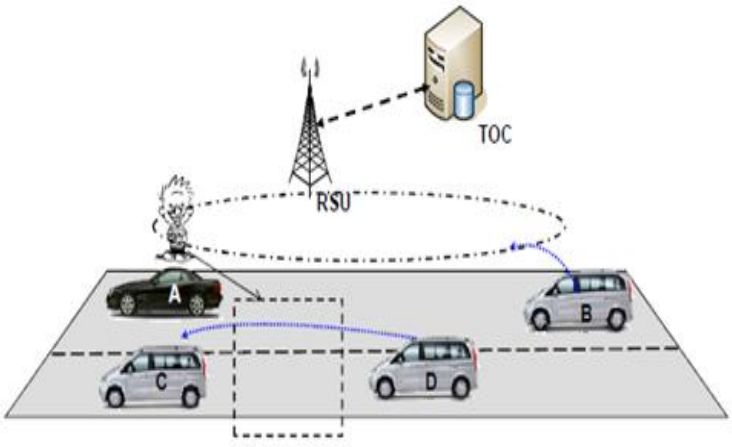

Fig. 2 DoS attack scenario

B.2 Distributed Denial of Service (DDoS)

This attack is the most severe attack in a vehicle environment because the attack mechanism lies in the way they are distributed. In this case, the attacker attacks from different locations and may use different periods to send messages [10]. The nature of the message and its period vary from one attack vehicle to another. Figure (3) illustrates the DDoS attack on a range of vehicles, with attack vehicles (B, C, D) attacking the vehicle (A).

This attack also aims at preventing legitimate users from accessing the services. Figure (4) illustrates the DDoS attack on infrastructure. B, C and D attackers launch an attack on infrastructure (RSU) from different locations, when other vehicles (A and E) want to access the network; the RSU is in an overload state.

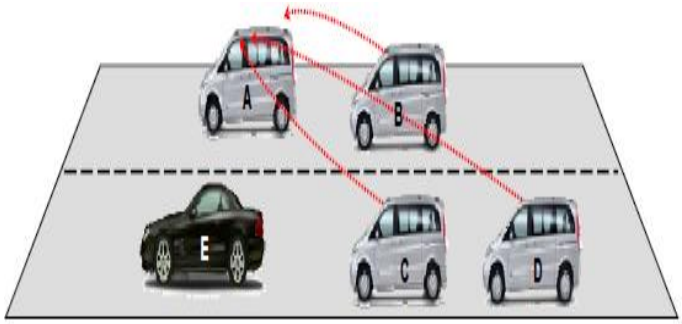

Fig. 3 DDoS attack on the V2V connection

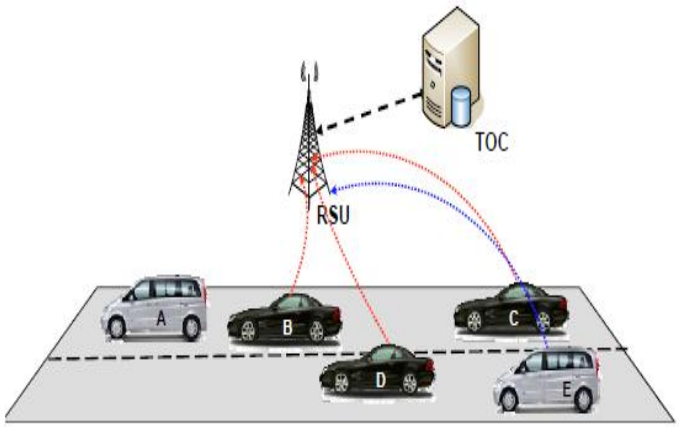

Fig. 4 DDoS attack on the V2I connection

III. SIMULATION RESULTS

A. *Part I:*

A.1System Model

Therefore, we will focus our project on the E-call service because it is important and it contributes to save human lives in the accident case because, as we mentioned earlier, it aims to provide rapid assistance to drivers by sharing the collision anywhere in the European Union. In case of failure, the e-call vehicle calls the nearest emergency center, even if the passengers are unable to connect, due to injuries sustained during the accident. Therefore, this service should be both quick and efficient. Based on this, our project aims to compare the performance of proactive and interactive protocols in VANET. We choose the AODV interactive protocol [11] and the DSDV proactive protocol [12] based on two different scenarios. Our simulation is based on NS2 simulator.

A.2 Performance parameters

We choose tow performance parameters:

Throughput: It is the number of packets received successfully over one time and estimated by bits per second (bps), or data packets per second or packets per time slot data, the higher the value, the better the network performance.

End-to-End Delay: The length of time the packet needs to move from the sender to the receiving node, it is measured by milliseconds.

A.3 Simulation Results

We used NS-2 to implement the desired network. A 50-node network was used to simulate the city's conditions and congestion, and the number of nodes was reduced to 10 to simulate the rural environment.

A.3.1 Scenario 1 (congested Environments):

A network of 50 nodes was randomly distributed. There were 15 mobile nodes as shown in Fig (5). The node $\mathbf{n_0}$ was chosen as a clustered node and 20 nodes were randomly selected to exchange information with the collected node using the UDP protocol. The CBR constant, the routing protocol is AODV in the first simulation and DSDV in the second simulation, the adopted mac protocol is 802.11, the simulation time is 70 seconds.

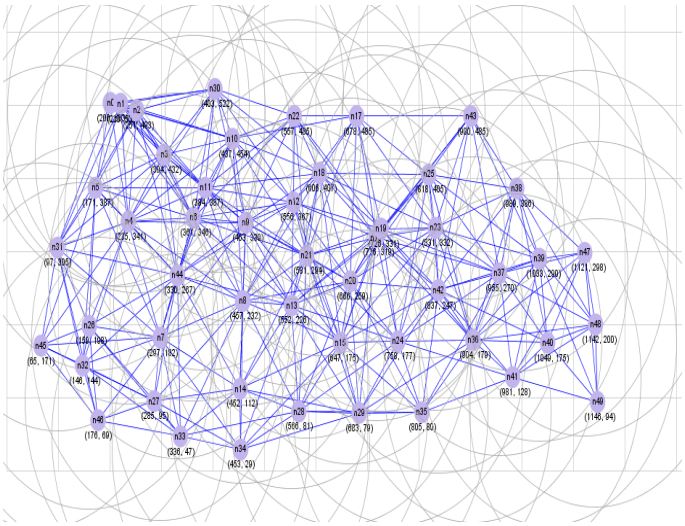

Fig. 5 Network topology of the first scenario

In the studied scenario, the number of messages sent using AODV protocol is 2765, while the number of received messages is 2535, and 230 messages failed. While in DSDV protocol, the number of sent messages is 1924 messages, while the number of received messages is 1877 messages, and 47 messages failed.

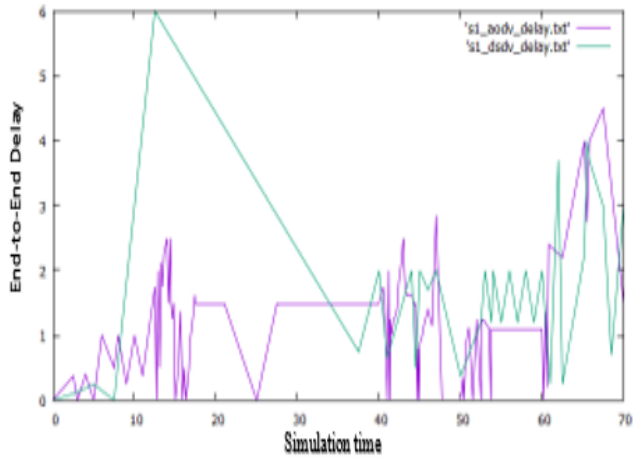

Fig. 6 End-to-End Delay of AODV & DSDV (first scenario)

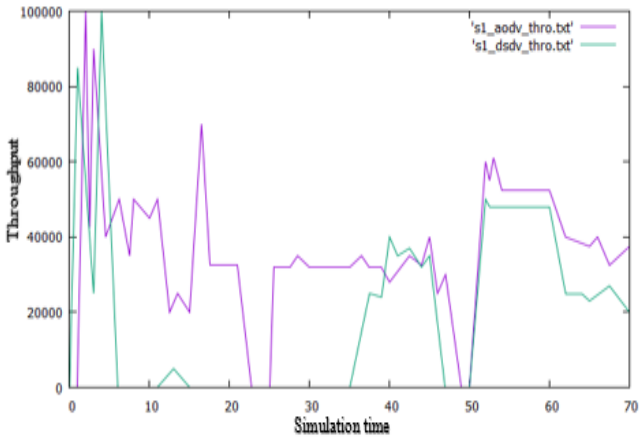

Fig. 7 Throughput of AODV & DSDV (first scenario)

We conclude as illustrated in fig.6 and fig.7 that the AODV protocol has a data delivery rate of 91.69% versus 8.31% of failed messages, while DSDV has a data delivery rate of 97.56% versus 2.44% of failed messages, and we noticed that end to end delay in DSDV is less than in AODV protocol, regardless of the primitive delay of the DSDV protocol because it is in the process of establishing the path according to its proactive nature. Thun, DSDV protocol is better for our study case.

A.3.2 Scenario 2 (non-congest Environment):

A network of 10 randomly distributed nodes was implemented. There were five mobile nodes as shown in Figure (8). The node **n0** was chosen as a clustered node. Three nodes were randomly selected to exchange information with the bundled node using the UDP protocol.

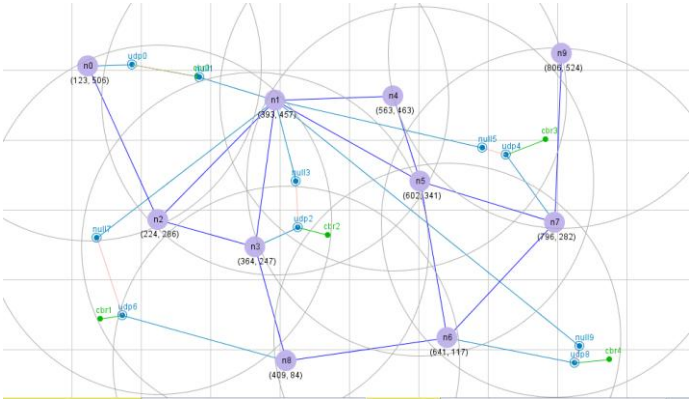

Fig. 8 The topology of the network studied in the second scenario

Using a grep instruction, in the studied scenario, the number of messages sent using AODV protocol was 625, while the received messages were 573 messages and 52 failed messages. While in DSDV protocol, the number of messages sent was 625, while the received messages were 520 messages and 105 failed messages.

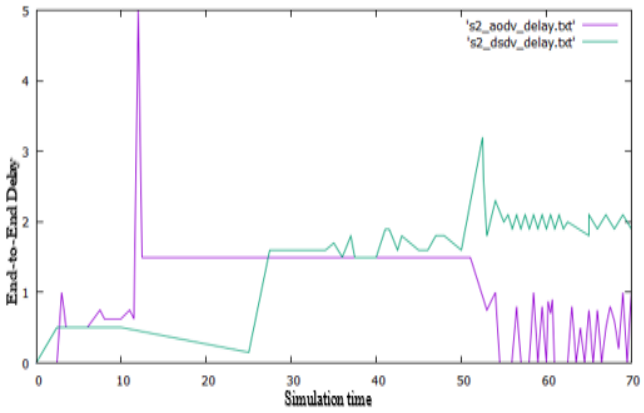

Fig. 9 End-to-End Delay of AODV & DSDV (second scenario)

We conclude that throughput is similar in both protocols, but DSDV suffers from a significant delay compared to AODV. Therefore, the interactive protocol is better in non-congested environments that contain a few nodes, especially in non-time-controlled applications.

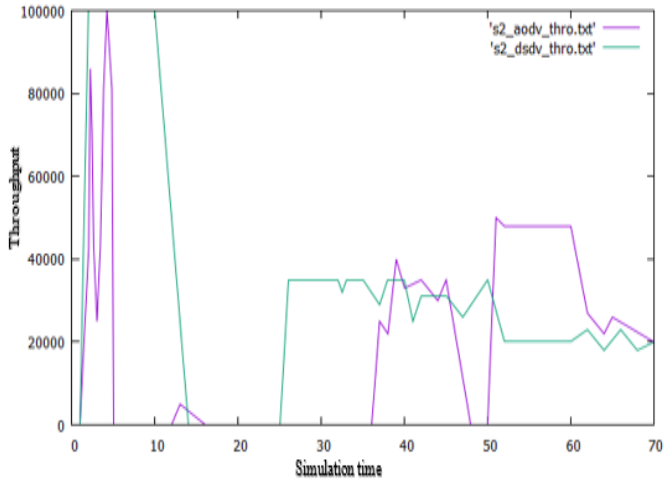

Fig. 10 Throughput of AODV & DSDV (second scenario)

B. Part II security using VANETsim:

We will study and analyse in this part the RSU attack, where we will examine the impact of its existence or not, that demonstrates the mechanism of the network without the presence of attackers, and a second scenario with the presence of attackers in the networks of mobile vehicles through practical simulation by VANETSim [13]. Our goal is to show the impact of the infrastructure in the hands of the attackers and what damage to the network is occurred.

B.1 Scenario 1 (without an attack on the network):

We import in our first scenario a map from the openstreetmap a site of Latakia as shown in Fig.11.

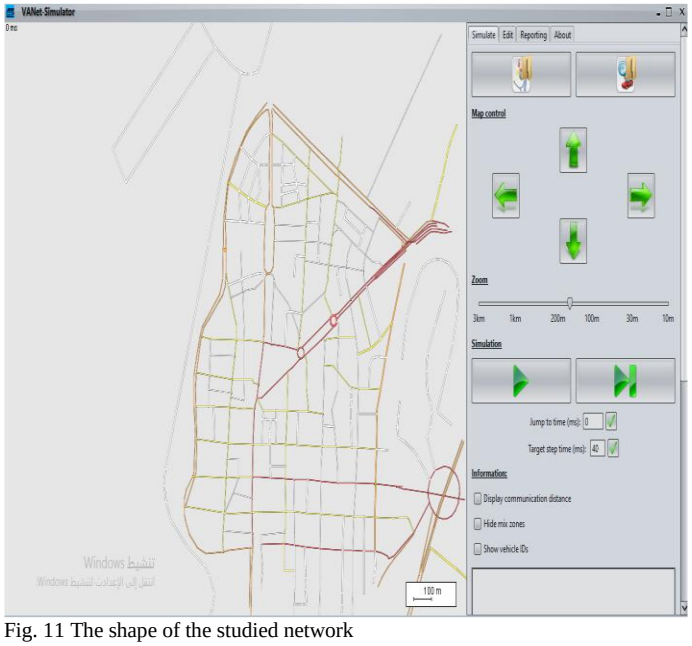

Fig. 11 The shape of the studied network

We add the nodes of the vehicles to the above network and RSU and run the simulation as illustrated in fig.12.

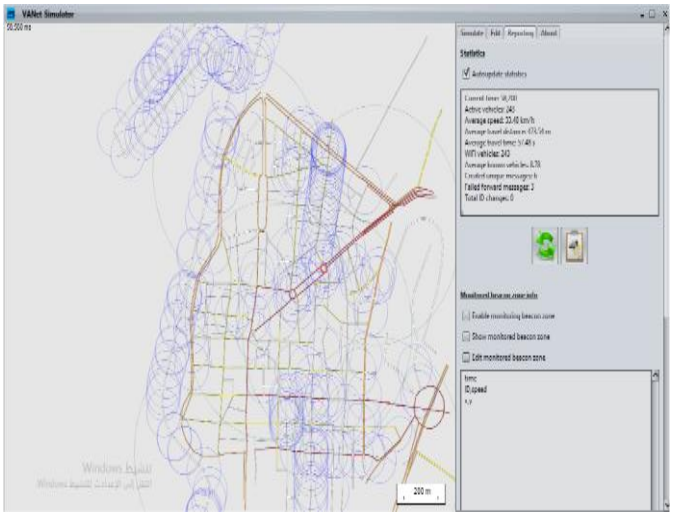

Fig. 12 The shape of the grid during simulation

The added vehicles were clarified with the coverage area of each node, in addition to the RSU and its coverage area. About 250 vehicles were added to the network with a coverage area of 300 m per vehicle and 5 RSUs were added (one RSU each 500 m). Note that after a period of time from the start of the simulation there is a loss of some messages, which is normal in wireless networks due to the congestion.

B.2 Scenario 2 (with attack on the net):

In this scenario, the attack on the RSU network infrastructure was simulated by adding a number of them as attackers.

Fig.13 illustrates the second studied scenario in which vehicles appear in blue, the RSU is green, and the attacked RSU in red.

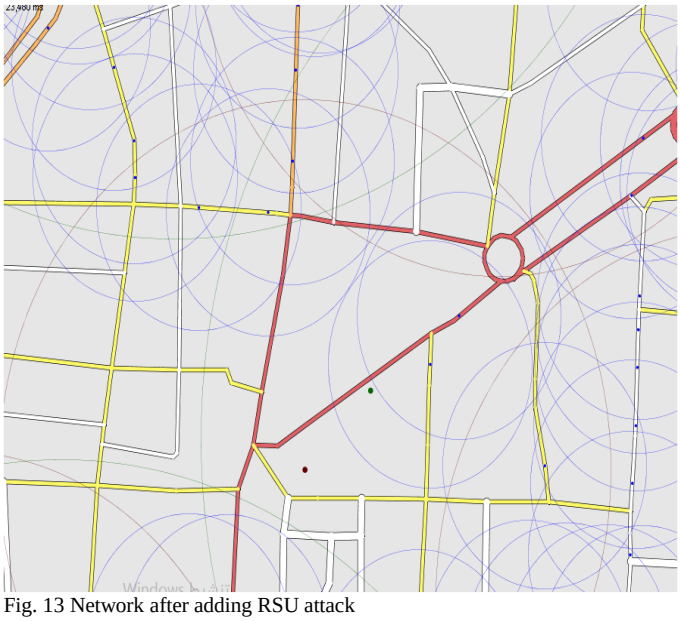

Fig. 13 Network after adding RSU attack

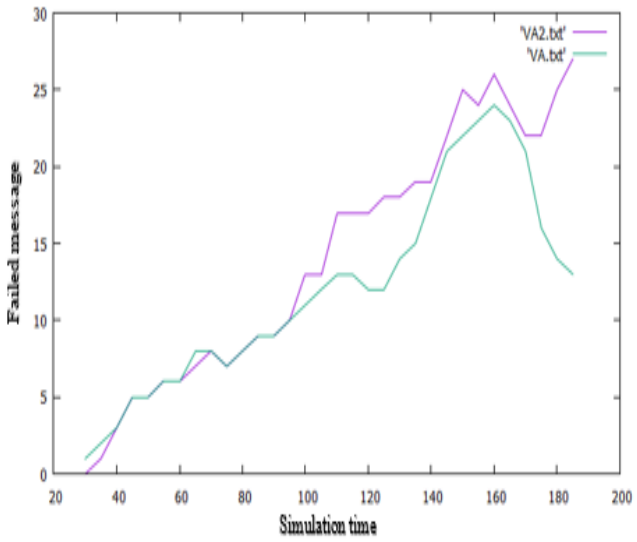

Fig. 14 Simulation results of the second part

The result of first scenario appears in green, while the second scenario appears in violet in fig.14. Note that in the second scenario, the rate of messages has increased with the increase of the number of failed messages, as the RSU has come under control and has been sending false messages towards the vehicles, resulting in depletion of the network's power and loss of information. Therefore, this type of attack is the most dangerous types of attacks at all because it leads to the network out of work.

IV. CONCLUSIONS

In this paper we studied the VANET networks that aims to provide efficient and safe transportation, and we focused on VANET routing protocols used for E-Call service by applying two scenarios. The first is applied in a crowded area and the second is applied to the less crowded areas. In addition, we study attacks on these networks, we focused our study on the analysis of the RSU attack (which is one of the most dangerous attacks on VANETs' reliability) based on the VANETSim simulator.

REFERENCES

[1] Divya Chadha and Reena, "Vehicular Ad hoc Network (VANETs): A Review ". International Journal of Innovative Research in Computer and Communication Engineering, 2015.

[2] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks,", Hot Topics in Networks (HotNets-IV), 2005.

[3] J. Tarng, B. Chuang, and F. Wu, "A novel stability-based routing protocol for mobile ad-hoc," IEICE Transactions on Communications, vol. E90-B, no. 4, pp. 876–884, April, 2007.

[4] Europe's Information Society Thematic Portal: http://ec.europa.eu/information_society/ activities/ esafety/ ecall /index en.htm.

[5] W. Sun, H. Yamaguchi, K. Yukimasa, and S. Kusumoto, "GVGrid: A QoS Routing Protocol for Vehicular Ad Hoc Networks," 14th IEEE International Workshop on Quality of Service, IWQoS'06., pp.130-139, 19-21 June 2006.

[6] Yan Gongjun, D.B. Rawat, and B.B. Bista, "Provisioning Vehicular Ad Hoc Networks with Quality of Service," International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), pp.102-107, 4-6 Nov. 2010.

[7] Li Xiaoyan, T.D. Nguyen, and R.P. Martin, "Using adaptive range control to maximize 1-hop broadcast coverage in dense wireless networks," First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON'04. pp. 397- 405, 4-7 Oct. 2004.

[8] W. Chen, and S. Cai, "Ad Hoc Peer-to-Peer Network Architecture for Vehicle Safety Communications", IEEE Communications Magazine, pp 100-107, April 2005.

[9] I. Ahmed Soomro, H.B. Hasbullah, and J.lb. Ab Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", WASET issue 65, april 2010 ISSN 2070-3724.

[10] Munazza Shabbir, Muazzam A. Khan, and Umair Shafiq Khan, "Detection and Prevention of Distributed Denial of Service Attacks in VANETs", International Conference on Computational Science and Computational Intelligence (CSCI), 15-17 DEC, 2016.

[11] H Perkins, et. al. "Ad-hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[12] Aditi.M.Khekale, Sampa.S.Jana, and Madhuri.K.Ninawe, "Design of Vehicular Ad Hoc Network using DSDV Protocol", International Journal of Recent Scientific Research Vol. 6, Issue, 3, pp.3213-3215,March, 2015

[13] Andreas Tomandl, Dominik Herrmann, Florian Scheuer, Karl-Peter Fuchs and Hannes Federrath," VANETsim: An open source simulator for security and privacy concepts in VANETs ", International Conference on High Performance Computing & Simulation, HPCS 2014, Bologna, Italy, 21-25 July, 2014.