RESEARCH ARTICLE OPEN ACCESS

Fabrication Attack Effect on Medical Applications based on VANETs

Aleen Sliman [1], Karam Madi [2], Aws Khadour [3]
Boushra Maala [4], Ahmad S. Ahmad [5]

Fourth Year Student [1], Assistant Professor [5]
Department of Medical Engineering
Al-Andalus University, Alkadmous - Tartous, Syria

Fifth Year Student [2] & [3], Associate Professor [4]
Department of Mechanical and Electrical Engineering
Tishreen University, Lattakia, Syria

ABSTRACT
In the context of expansion of using Vehicular Ad-hoc Networks-VANETs in the medical field around the world, studying the attacks on these networks becomes an urgent need to overcome these attacks and to serve a safe use in medical applications. In this paper, we will focus on a fabrication attack scenario which is one of the most dangerous attacks on VANETs' reliability. Our simulations are built using VANET-SIM simulator, in which we study the fabrication attack using three different scenarios that is taking place in Lattakia city.
Keywords :— MANET Networks, VANET Networks, security, Fabrication attack, VANET-Sim.

I. INTRODUCTION

VANETs provide many services to vehicles' users in order to save their lives in urgent cases such as notification of accident up ahead and decentralized 911 service [1]. In addition to that, VANETs might be used to provide monitoring services to several diseases and other medical conditions that require constant monitoring of physiological signals and vital signs on daily bases, such as diabetics, hypertension, etc.[1] So VANETs which provide these critical services cannot be tolerated with fabrication events that may happen because of attacks on the network, like fabrication attacks which menaces the reliability of these networks and makes it inefficient to serve medical applications.

The reminder of this paper is organized as follows: In section II, we study the VANET networks and the fabrication attack.. In section III, we evaluate the fabrication attack over VANET using three scenarios. Finally, conclusion and future work are presented in section IV.

II. RELATED WORKS

A. VANET Networks

Vehicular Ad-hoc Networks (VANETs) consist of a set of mobile vehicles fitted with transmitter / receiver and the Global Position System (GPS). These networks are designed to provide connectivity between vehicles to each other wirelessly without the need for infrastructure or between them and the units located on the side of the road (called RSU (Road Side Unit)), its goal is to provide efficient and safe transportation. However Infrastructure-to-vehicle (I2V), vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V) communication systems are enabled by VANET[3]. Also, it includes units which are located on road sides, providing vehicles connections with the Internet and other far vehicles, called RSU units [4]. IEEE 802.11p Wireless Access in the Vehicular Environment (WAVE) has been serving as the facto wireless protocol for a VANET with the explosive growth of vehicular applications [5]. Figure1 shows an example of a network VANET.

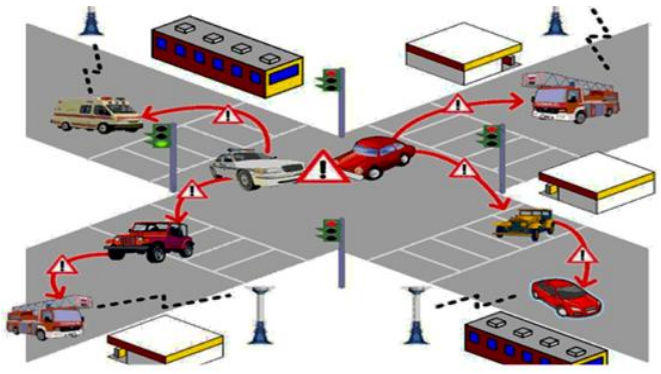

Fig. 1. Example of VANET .

One of the most important services of these networks is the safety application. VANET aims to reduce injuries and deaths from traffic accidents and improve public safety. Especially that the statistics conducted on the number of deaths from traffic accidents has given large numbers around the world. In Syria, for example, according to the statistics of the Ministry of Transport between 2000 and 2010 as shown in Figure 2, we note, for example, that the number of deaths in 2007 up to 2818 people.

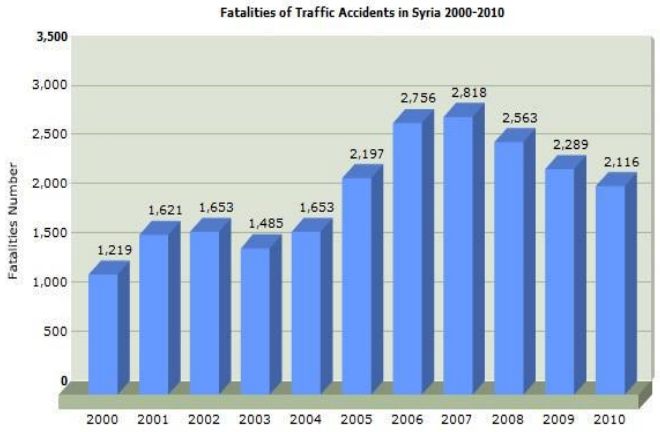

Fig. 2. Statistical of Department of Transportation in Syria for the deaths resulting from traffic accidents between 2000-2010.

B. Fabrication attack and its effect in VANETs

One of the most dangerous attacks in the vehicular environment is the fabrication attack because the aggressor can make the assault by sending wrong information into the system, these information could be wrong or the transmitter could assert that it is another person [6]. This assault incorporates create messages, warnings, declarations and personalities. Our paper focuses on studying the distributed case, which is the worst case of its cases, and studying its effect on the reliability of the VANETs.

III. RESULTS AND ANALYSIS

A. *Simulation Environment and Setup*

We simulated three scenarios A, B and C, to study Fabrication attacks effects on VANET that are applied in Lattakia city, as shows in figure-3.

Fig. 3. Lattakia city, the place where our scenarios is applied.

In addition, we study how IDS which is applied in VANET simulator can be able to detect the fake messages, which are generated by fabricated vehicles.

To do this simulation we used VANET-Sim simulator, which has been designed for studying attacks effects purposes in VANETs, VANET Simulator is an event-driven simulation platform, specifically designed to investigate application-level privacy and security implications in vehicular communications [7]. It focuses on realistic vehicular movement on real roads networks and communications between the moving nodes [7].

B. *VANET Simulator*

VANET Simulator can simulate scenarios with specific events and detects the messages which are sent as a react of these events such as "Stopped/Slow Vehicle Advisor", "Road Hazard Condition Notification", "Emergency Electronic Brake Lights" and "Emergency Vehicle Approaching" (EVA) [7]. Based on the type of these messages, this Simulator supports various forwarding protocols [8]. It also uses IDS to detect fake massages which are generated by attacked vehicular. In our scenarios, we used "HUANG_EVA" messages as fake messages which are sent from malicious vehicles.

C. *Intrusion Detection System-IDS:*

In general, IDS consists of three phases, a data collection phase followed by an analyzing phase and finally a response phase to prevent or minimize the impact of the attack on the system.

IDS can be classified according to the used detection techniques used into three categories:

- **Signature based system**: The system has a database behavior of certain attacks, which are compared with the data collected. An attack is detected if the data coincide with malicious behavior already registered.

- **Anomaly detection system**: The system detects any behavior which deviates the standard pre-established behavior and triggers a response (notification).

- **Specifications based system**: The system defined a set of conditions that a program or protocol must satisfy. An attack is detected if the program or protocol does not meet the conditions set of proper operation. [9] To detect false data in VANETs, IDS often uses application layer data such as position, time and application-specific information to conduct a form of context verification [10]. Then IDS in VANET Simulator works according to the last category.

Our paper will shows the benefits of using the IDS in VANET-Sim, in order to detect the fake messages that is

generated by the fabrication attack, thereby improvement the reliability.

D. ***Simulation scenarios:***

D.1. Scenario A

A VANET scenario includes 1000 vehicles, 50% of them send fabricated messages about medical Events did not occur, where the IDS didn't run and no events existed. So, the result shows an EVA detected messages as shows in figure-4, although no real events occurred, and the number of these message is large. In some cases up to 90 messages in one second are sent, which reflects the existence of 90 Events at the same second neither of it occurred in reality. As a result, this leads to dissipate the network and making it unable to serve the medical applications.

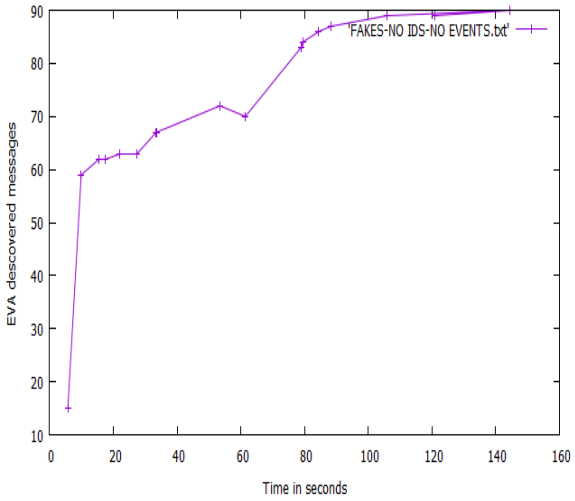

Fig. 4. results of simulated 'A' scenario.

D.2. Scenario B

It is similar to the previous scenario, VANET Simulator IDS is running. So , the results show that no EVA detected messages as shown in figure- 5, because the IDS has detected the fake messages and deleted them, this scenario explains how the IDS guarantees the reliability of the network, subsequently making it able to serve the medical applications safely despite the presence of the fabrication attack.

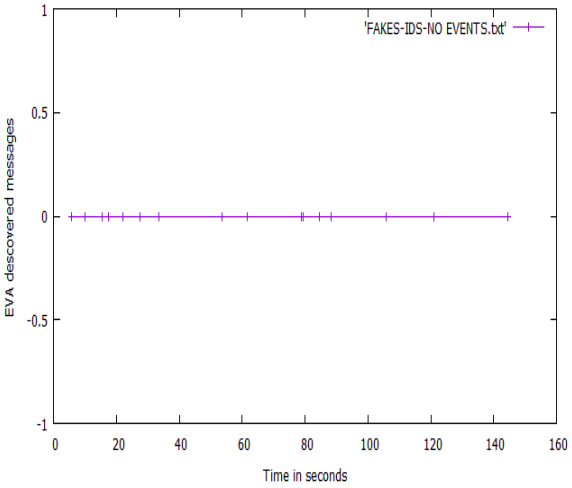

Fig. 5. results of simulated 'B' scenario, no EVA messages detected

D.3. Scenario C

This scenario includes 1000 vehicles, 50% of them send fabrication messages (EVA messages) about Events did not occur, the IDS is running and three realistic events existed as shown in figure-6. So when vehicles reach the events, they will send a realistic EVA messages.

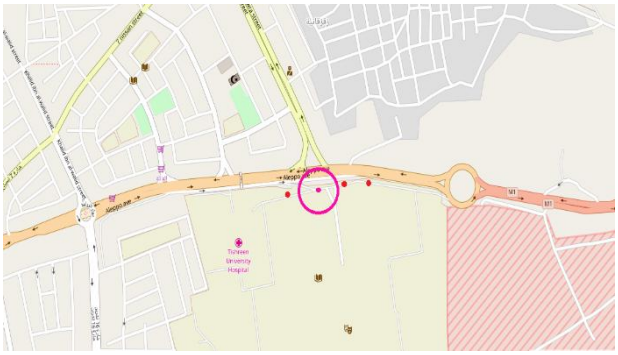

Fig. 6. scenario 'C' with three events (in red color).

As shown in figure-7 the number of EVA detected messages is considered as normal average. This is because of the IDS has detected the fake messages and deleted it, while it allowed to the realistic EVA messages to be sent. This result shows that up to 21 EVA messages sent in one second, this number is logical as a result of existed one thousand vehicle with three events in the network.

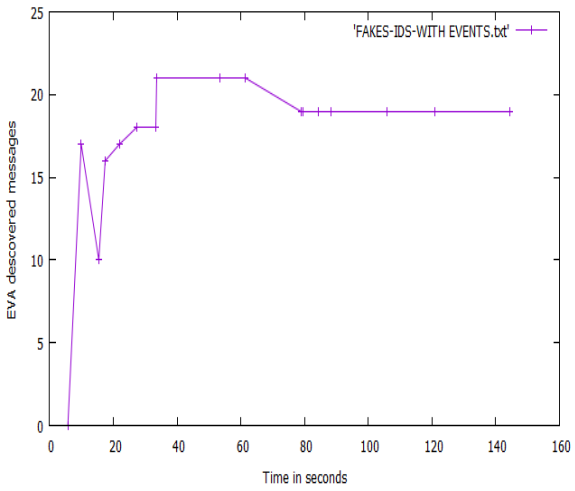

Fig. 7. results of simulated 'C' scenario, realistic EVA messages detected.

These results assure the role of IDS in improving reliability in VANET. So the network will be able to serve the medical applications safely despite the presence of a fabrication attack.

E. *Simulation results comparison*

Based on comparison of the A, B and C scenarios results, we can notice how the fabrication attack can be very dangerous attacks on the medical applications that worked on VANETs, and how the IDS that is running in VANET Simulator contributes in guarantee the safety working of the medical applications on VANETs.

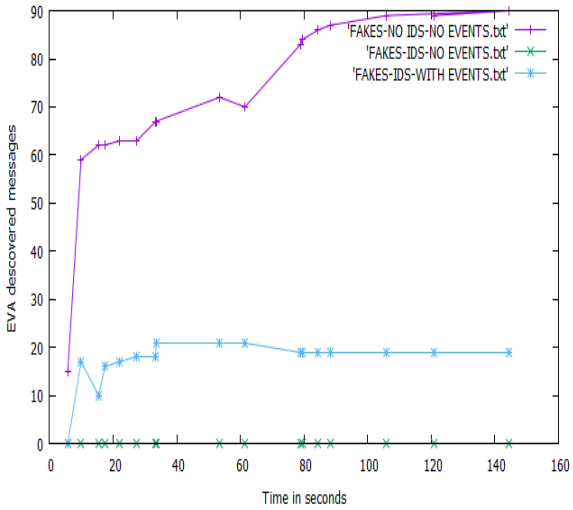

Fig. 8. comparison of the A, B and C scenarios.

IV. CONCLUSION AND FUTURE WORK

In this paper we studied the VANET networks that aims to provide efficient and safe transportation, and we will focused on a fabrication attack scenario which is one of the most dangerous attacks on VANETs' reliability. We evaluated our study using VANET-SIM simulator, in which we used three different scenarios that is taking place in Lattakia city.

As a future work, we will try to study more effective methods to protect the medical application from the fabrication attacks on VANETs.

REFERENCES

[1] Hyduke Noshadi, Eugenio Giordano, Hagop Hagopian, Giovanni Pau, Mario Gerla, and Majid Sarrafzadeh: "Remote Medical Monitoring Through Vehicular Ad Hoc Network ". Proceedings of the 68th IEEE Vehicular Technology Conference, VTC Fall 2008, 21-24 September 2008, Calgary, Alberta, Canada, PP: 1-5.

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

[3] Dhyey Patel, Mohd. Faisal Khan, Priyanka Batavia, Sidharth Makhija and M. Mani Roja," Overview of Routing Protocols in VANET ", International Journal of Computer Applications (0975 – 8887) , Shahni Engineering College, Mumbai 2016.

[4] Nirbhay Kumar Chaubey, " Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study ", International Journal of Security and Its Applications 2016.

[5] Che-Yu Chang , Hsu-Chun Yen , and Der-Jiunn Deng, "V2V QoS Guaranteed Channel Access in IEEE 802.11p VANETs ". In: IEEE Transactions on Dependable and Secure Computing .Volume: 13, Issue: 1, Jan.-Feb. 1 2016.

[6] Priyanka Soni , and Abhilash Sharma," A Review of Impact of Sybil Attack in VANET's ". International Journal of Advanced Research in Computer Science and Software Engineering, may 2015.

[7] 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.

[8] C. Maihofer, R. Eberhardt, and E. Schoch, "CGGC: Cached Greedy ¨ Geocast," in Wired/Wireless Internet Communications. Springer Berlin / Heidelberg, 2004, vol. 2957, pp. 171–182

[9] Mohammed Erritali, and Bouabid El Ouahidi," A Survey on VANET Intrusion Detection Systems ", International Journal of Engineering and Technology (IJET), Vol.5, No. 2, PP: 1985-1989, 2013.

[10] T. Leinmuller, E. Schoch, and C. Maih ¨ ofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks," Fourth Annual Conference on Wireless on Demand Network Systems and Services, 2009.