Engineering Universe for scientific Research and management
ISSN (Online): 2319-3069
Vol. XIII Issue IX
September 2021

IMPROVEMENT SECURE INTELLIGENT AND EFFICIENT AGAINST DOS ATTACKS IN VEHICULAR AD-HOC NETWORK

Vivek Kumar[1], Prof. Chetan Agarwal[2],Prof. Priyanka Parihar[3]
[1,2,3] Department of Computer Science Engineering RITS, Bhopal, (MP), India
viveksrist@gmaill.com

ABSTRACT Vehicular Ad hoc Networks (VANETs) have emerged recently as one of the most attractive topics for researchers and automotive industries due to their tremendous potential to improve traffic safety, efficiency and other added services. However, VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives. This paper presents a survey of VANETs attacks and solutions in carefully considering other similar works as well as updating new attacks and categorizing them into different classes.

Keywords: *Vehicular Ad hoc Networks, enhanced navigation, growing number, remote keyless entry devices.*

1. INTRODUCTION

In the last few years, accompanying the massive deployment of wireless technologies and the growing number of wireless products on motorized vehicles including remote keyless entry devices, personal digital assistants (PDAs), laptops, and mobile telephones, automotive industries have opened a wide variety of possibilities for both drivers and their passengers. Vehicular Ad hoc Networks (VANETs) have attracted a lot of attention in research community because of their varied value added services, namely vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based service for finding the closest fuel station, travel lodge or restaurant and simply access to the Internet NETworks (MANETs) VANETs inherit all the discovered and undiscovered security and privacy vulnerabilities related to MANETs. Furthermore, VANETs have a number of distinctive properties [5] that could be also vulnerabilities for attackers to exploit. Those properties include the particular nature of communication in VANETs. Connections in a VANET in particular and in any Wireless Ad hoc Network in general are based on node-to-node communications: every node is able to act as either a host inquiring data or a router forwarding data. There are two types of nodes: (i) Road Side Units (RSUs) standing for fixed nodes provisioned along the route and (ii) On Board Unit (OBU) referring to mobile nodes (i.e., vehicles) equipped with some sort of radio interface that enables connecting to other nodes in wireless manner. Figure 1 depicts a general view of VANETs structure. It is worth mentioning that the speed of mobile nodes- vehicles in VANETs may be much higher than in MANETs. This reason makes VANETs very dynamic in nature. A number of nodes can communicate once as a group but can then rapidly change their own structure caused by leaving of a member or joining of another node. Therefore, it is expected that nodes are continuously "keeping in touch" with other nodes in the group to maintain the survival of the network. This aspect of VANETs seems to be very vulnerable and attacks can be unconsciously or intentionally performed to damage a part of or the total network. As mentioned above, VANETs provide many added applications that are safety, entertainment, or infotainment oriented. Attacks to VANETs may lead to catastrophic consequences such as the losses of lives in the case of traffic accident, losses of time (e.g., tampering traffic jam made by attacks) or financial losses (i.e., in payment services).

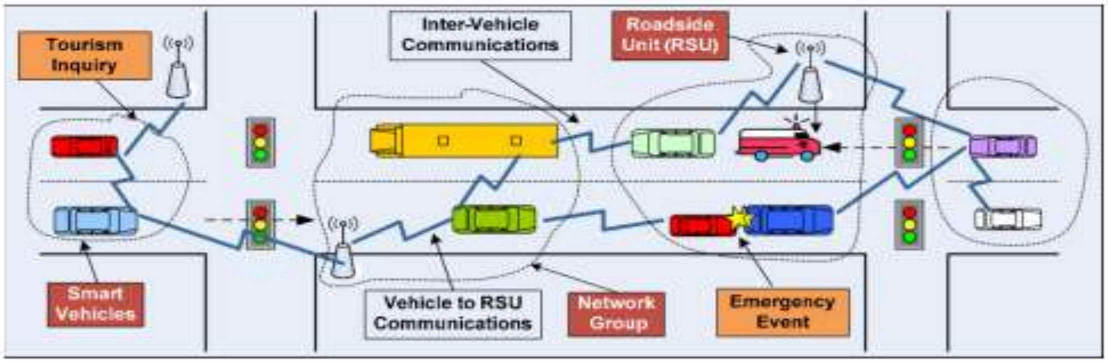

Fig. 1: A basic structure of VANETs

The researches on VANETs security were triggered in the middle of and genuinely bloomed since 2007. In order to provide a thorough survey covering a big number of publications related to VANETs attacks, we searched for and collected papers approaching this topic from that had made a significant contribution to the improvement of VANETs security. indicated the numbers However, there is a few survey works in the literature on VANETs attacks. In the existing surveys [2], [3], [6], some of attacks were not enough illustrated in detail and some were missed. Our paper aims to introduce more concisely the possible attacks, their mechanisms and influences as well as their corresponding solutions to thwart those attacks. We characterize the attacks (e.g., type of attacker, security aspects that are damaged) for a further classification. For each attack, we try to perform a concise scenario to better identify this attack. We equally point out the properties that can be collected to detect the attacks. These properties could be the input for an intrusion detector that we consider as future work of our research. Our purpose in this study is to not only depict a detailed list containing up-to-date attacks but also a global view of security threats in VANETs, in order to provide a useful starting point for researchers interested in the subject and to help VANETs designers to develop and deploy secure VANETs infrastructures. The causes that motivated this research are fleetingly discussed in this section. World Health Organization open that, nearly 3,400 persons die on the world’s infrastructures every day. Tens of millions of persons are battered or inactivated every year. Over 130,000 deaths are caused yearly 3 by road accidents in India. Every hour, 40 persons under the age of 25 die in road accidents everywhere the world. In India unaided, the death toll design to 14 per hour in 2009. According to Reservoir of Top Lists India is ranked no.1 for maximum number of expiries in road accidents or traffic associated deaths in 2012. The intense social and economic deportments of road accidents have inspired the research towards Vehicular Ad-hoc Networks (VANETs). VANETs will augment driver protection and diminish traffic deaths and grievances through employing collision circumvention and threatening systems. Researchers say that, by approving VANET for our transportations and cars, the driver community will be intelligent to become the following information:

- Traffic related information: Traffic Jams, Road Conditions, Bridges, etc.,
- Safety related information: Emergency braking, accidents warning, collisions ahead, etc.,
- Infotainment related information: Neighboring petrol stations, hotels, restaurants, shortest routes and tollgates.

The safety driven requests of vehicular communication have inflexible consistency and interruption necessities, which are not fulfilled by existing wireless standards. As a outcome, to empower statement in the vehicular environment, the Steadfast Short Range Communication Standard (DSRC) [10], with set of communication protocols and standards detailed for automotive use, was fashioned. They available an examination of wireless entrance standards for VANETs, and pronounce particular of the recent VANET trials and dispositions. Yet, there are numerous other challenges in employing vehicular communication in practice. Among which, security and concealment are the double major issues to be touched judiciously in VANET. Accomplishing scalability deprived of compromising these two parameters (security and privacy) is decidedly challenging with huge integer of nodes and their high-mobility nature. Although many earlier studies have vexed to solve scalability issues to dissimilar extends, none of them either provisions both Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications or affords a very fast verification algorithm such that virtually all the incoming messages could be administered with a noticeably lower message loss, straight when the traffic density grows. Investigation of the prevailing VANET protocols established that greatest of them result in presentation bottleneck during high traffic circumstances. The main problem with these procedures is the large packet size, that results in bigger cryptographic and communication overheads.

The above condition motivated this research to expression for a reliable explanation to sustenance both V2I and V2V communications, yet by dipping the above said overheads that are not properly addressed through other studies. The main apprehension of this research is, to recommend an efficient protocol so that can gratify the scalability necessities and lower the message loss. The impartial of VANETs is to distribute safety and coziness, thus, in vehicular communications; the information bartered among vehicles plays an essential role. Identifying the agenda in which information might be important is an appropriate aspect to be painstaking. In particular, for safety-related applications, the information communicated among vehicles is well-thought-out critical, thus, timely and correct exchange of this evidence could avert a great numeral of fatal road accidents. Nevertheless, if an attacker deploys the information could hypothetically cause harm; consequently, in directive to prevent budding attacks, executing security procedures is of the extreme reputation. To speechless this, the implementation of Public Key Infrastructure (PKI) technology, which has been demonstrated to be an opposite solution in other disseminated environments, has been measured. The employment of PKI will enable the creation of secure communication channels, by providing services desirable to sidestep a wide choice of security attacks. Current PKI systems entail of a Central Authority (CA) answerable for recording users and issuing credentials (containing the corresponding private and public key-pair). In VANETs, it is planned that vehicles will be enumerated with their personal regional CA, and consequently, a common construction will require a widespread range of CAs. Interoperability among CAs, to deliver inter-domain confirmation when vehicles foldaway to dissimilar domains within regional scopes. Though, by following the employment of several CAs, how will confirmation and authorization be achieved when vehicles interchange between two changed geographical regions? It is presumed that when a vehicle travels to a diverse topographical region or domain, a mutual confirmation and trusted announcement will be accomplished thanks to former cross-certification agreements (mostly manual). Nonetheless, since certificate withdrawal is also the charge of the distributing CA, a shortcoming of cross-certification is that, it is not probable to obtain up-to-date cancelation information resulting in a defenselessness window for the trusting party, which raises the enquiry on how to mechanically perform cross-certification and i) authorize trust among unknown CAs and ii) validate in near-real time a VANET s node certificate status. Apart from the revocation problems just mentioned, and notwithstanding the assistances of empowering the procedure of PKI technologies in VANETs, the sole use of PKI.

2. OVERVIEW

There are quite a few attacks, which can distress the performance of operation in VANETs. Certain of these attacks are insider (occurred from central authorized vehicles, which are malevolent or cooperated vehicles) and further ones are external attacks (happened from outsider vehicles, which do not belong to an explicit VANET). Likewise, these attacks can be categorized as passive attacks (that eavesdropper does not intermingle openly with authorized vehicles or affect deliberately the channel among them; however he can apprehension transferred information among those vehicles to analysis or to take an exploit) and dynamic attacks (here eavesdropper tries to deception himself as a genuine vehicle to redirect the path of communicated data; and a breakdown in the transmission channel among authorized vehicles can be done). For improving the network security or efficiency various researchers presented various techniques and algorithm which helps in the protected communication amongst the nodes of vehicular ad hoc networks.

NS2 is associate ASCII text file event-driven machine designed explicitly for analysis in pc communication networks. The machine we've got accustomed simulate the ad-hoc routing protocols in is that the Network machine two (ns) [19] from Berkeley. To simulate the mobile wireless radio setting we've got used a quality extension to ns that's established by the CMU Monarch project at Carnegie Mellon University. Since its establishment in 1989, NS2 has endlessly gained tremendous interest from trade, academia, and government. Having been below constant investigation and improvement for years, NS2 currently contains modules for various network elements like routing, transport layer protocol, application, etc. to research network presentation, researchers will merely use associate easy-to-use scripting linguistic to assemble a network, and perceive results generated by NS2. Undoubtedly, NS2 has developed the foremost wide used uncluttered source network machine, and one in all the foremost wide used network simulators. Unfortunately, most analysis wants simulation modules that are on the distant side the scope of the constitutional NS2 modules. Including these modules into NS2 requires reflective considerate of NS2 architecture. Presently, most NS2 apprentices rely on online tutorials. Most of the on the market data chiefly explains the way to assemble a network and assemble results, however doesn't embrace enough data for building further modules in NS2.

NS is associate entity directed machine, written in C++, with associate OTcl interpreter as a frontend. The machine supports a classification hierarchy in C++ (also denoted to as the assembled hierarchy through this document), and an undistinguishable category hierarchy among the OTcl interpreter (also mentioned to as the reserved hierarchy through this document).
The two hierarchy's are faithfully associated with every further; from the user's perception, there's a complemented correspondence between a classification inside the reserved hierarchy and one within the assembled order. The foundation of this grading is that the grouping Tcl Object. Users produce innovative machine substances concluded the explainer; these matters are instantiated amongst the interpreter, and are meticulously replicated by a conforming object within the accumulated hierarchy.

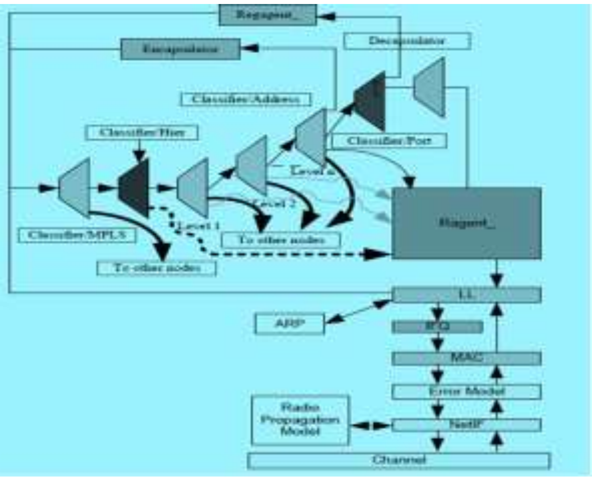

Fig.2: Radio propagation system

3. SIMULATION SCENARIO

Many visualization features are available in NAM. These features are for example animating colored packet flows, dragging and dropping nodes (positioning), labeling nodes at a specified instant, shaping the nodes, coloring a specific link, and monitoring a queue as shown in the Figure .

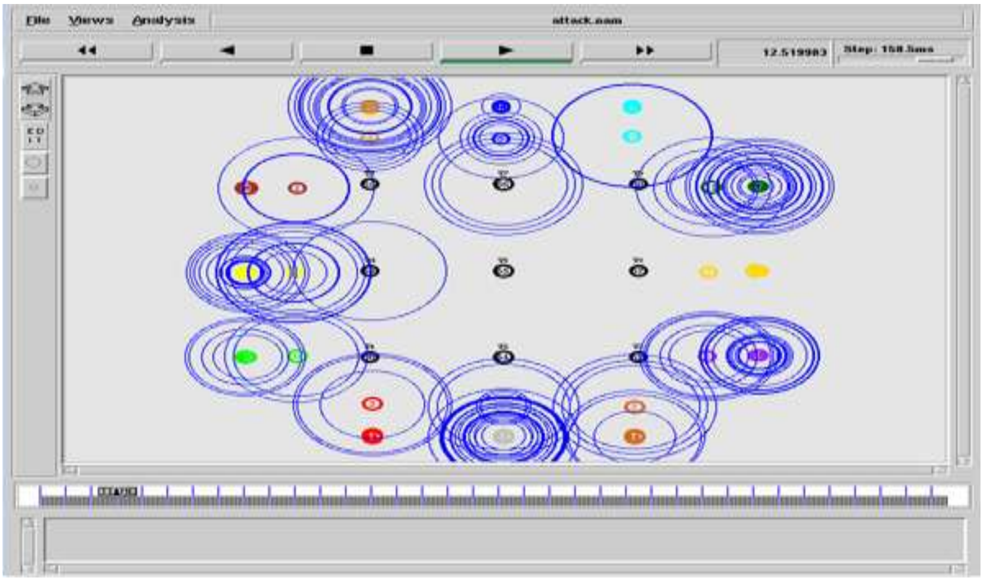

Fig. 3: DOS Attack Scenario

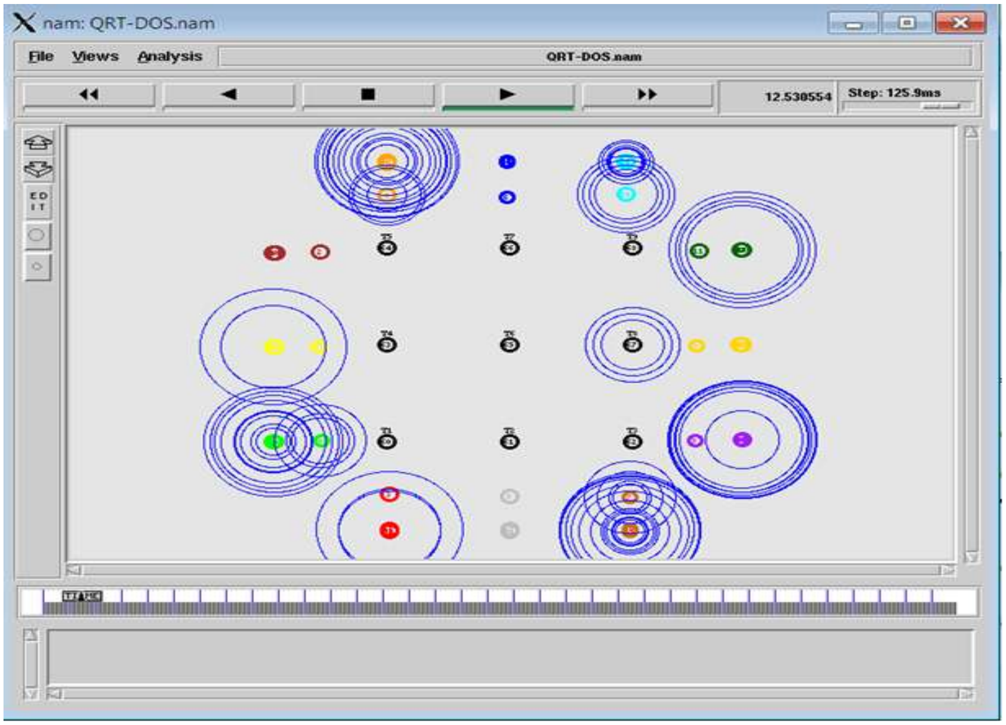

Fig.4: QRT-DOS Prevention Scenario

The packet dropping in wireless network is the major issue and the major reason is limited bandwidth utilization of vehicles in VANET. In this graph, the performance of proposed SE-DOS scheme is to provide the better performance by stop the flooding of attacker in VANET. The number of packets is sends at by sender is measures in three different scenario but proposed SE-DOS is provides better sending data in VANET. The RSU is able to handle the quantity of the data packets efficiently and this shows the reliability of proposed scheme as compare to previous.

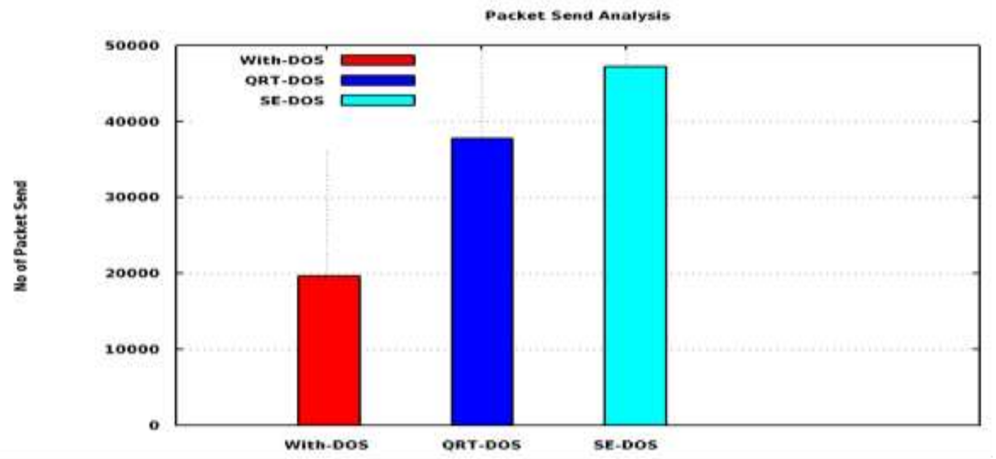

Fig.5: Comparison graph of packet send analysis between proposed and existing techniques

The DoS attacker is very harmful for the network because those vehicles that are in range of attacker then attacker are directly or indirectly flooded fake message to all nearby nodes in network. The fake packets are actually flooded by attacker node/s and attacker is actually flooded unwanted packets and drops the whole data packets. The performance of DOS receives, QTR-DOS and proposed SE-DOS is mentioned in this graph and proposed SE-DoS is receiving is highest. The data receiving is minimum in only DOS attack scenario because of flooding huge amount of fake information. That means the attacker drop data in network but proposed SE-DOS is stop its malicious activities. The vehicles is not receive any response in network and the reason is creating a situation that vehicles are not decided and follow destination path very slowly. At the time of attack number of routing packets flooding is high and data packets dropping is also high by that negligible packets in unit is measured. The proposed SE-DOS the performance is better as compare to existing QTR-DOS scheme because of more flexible routing security approach that secures the network and improves routing performance. In the graph the throughput, performance is measured and observes that the due to unwanted flooding data receiving is minimizes. Their effect is throughput is degraded. These packets receiving is very less as compare to existing (QRT-DOS) scheme. The proposed security scheme against malicious attack is secure the network performance and providing superior packets delivery.

4. CONCLUSION

The problematic of attacker is occur in any network because assaulter presence is affected the normal communication among the vehicles. if the vehicle network load is unbalanced or number of nodes in network is receives unwanted packets that means the DOS attacker is also yield portion in communication.. Vehicles have restricted computational capacities like bandwidth and buffer space. The popularity for eminence based routing has ensued in substantial attention by researchers in the region of security in VANET. The DOS, previous research QRT-DOS and the presentation of projected SE-DOS is comparing to measure performance. The presentation of projected SE-DOS scheme is proving efficient approach to protected routing procedure. The projected approach is using the concept of identifying flooding information with Identification.

REFERENCE

[1]Bako, B., & Weber, M. (2020). Efficient information dissemination in VANETs. INTECH Open Access Publisher.

[2]Ranjan, P., & Ahirwar, K. K. (2019, January). Comparative study of vanet and manet routing protocols. In Proceedings of the International Conference on Advanced computing and communication Technologies (ACCT).

[3]Kumar, R., & Dave, M. (2019). A review of various vanet data dissemination protocols. International Journal of u-and e-Service, Science and Technology,5(3), 27-44.

[4]Da Cunha, F. D., Boukerche, A., Villas, L., Viana, A. C., & Loureiro, A. A. (2014). Data communication in VANETs: a survey, challenges and applications (Doctoral dissertation, INRIA Saclay).

[5]Hartenstein, H., & Laberteaux, K. P. (2017). A tutorial survey on vehicular ad hoc networks. Communications Magazine, IEEE, 46(6), 164-171.

[6]Surmukh Singh, Sunil Agrawal, "VANET Routing Protocols: Issues and Challenges", Proceedings of 2018 RAECS UIET Punjab University Chandigarh, 06 – 08 March, 2014.

[7]Marshall Riley, Kemal Akkaya and Kenny Fong, "A Survey of Authentication Schemes for Vehicular Ad hoc Networks", Security and Communication Networks Published online 15 July 2016 in Wiley Online Library.

[8]Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)" National Advanced IPv6 Center, University Sains Malaysia Penang, Malaysia. June 28, 2019.

[9]Mohammed Saeed Al-kahtani, "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)",In proceeding of IEEE, 2012.

[10]Federal Communications Commission. Amendment of the commission's rules regarding dedicated short-range communication service in the 5.850-5.925 ghz band, fcc 02-302. Tech.rep., FCC, November 2002.

[11] Safi, S. M., Movaghar, A., & Mohammadizadeh, M. (2009). A novel approach for avoiding wormhole attacks in VANET. 2009 First Asian Himalayas International Conference on Internet. doi:10.1109/ahici.2009.5340317.

[12]Gaganpreet Kaur, Dr. Sandeep Singh Kang, "Study of various Data Dissemination types and its Protocols- A Review" International Journal of Information Management and Technology, ISSN NO. 2356-2600, Volume 1, Issue 1, Aug 2016.

[13]Harjit Kaur, Kamal Jeet Kaint, Rakesh Kumar, "A Review on Different Approaches of Safety Message Transmission in VANET" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 6, Issue 6, June 2016.

[14] Divya Chadha, Reena, "Vehicular Adhoc Network (VANETs): A Review" International Journal of Innovative Research in Computer and Communication Engineering, ISSN (online): 2320-9801, ISSN (print): 2320-9798, Vol. 3, Issue 3, March 2015.

[15]M. Raya, P. Papadimitratos, JP. Hubaux, Securing Vehicular Communications, IEEE Wireless Communications, Vol 13, 2006.

[16]B. Parno and A. Perrig, Challenges in Securing Vehicular Networks, Proc. Of HotNets-IV, 2005.

[17]I Aad, JP Hubaux, EW Knightly, Impact of Denial of Service attacks on Ad Hoc Networks, IEEE/ACM Transactions on Networking, Vol. 16, 2008.

[18]M Raya, J Pierre Hubaux, The security of VANETs, Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.

[19]S. A. Khayam, H. Radha, Analyzing the Spread of Active Worms over VANET, ACM Mobicom International Workshop on Vehicular Ad Hoc Networks, 2004.

[20]M. Raya, P. Papadimitratos, and J.-P. Hubaux, Securing vehicular communications, IEEE Wireless Communications Magazine, vol. 13, no. 5, pp. 8-15, 2006.