Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Topology base Routing Attacks in Vehicular Ad hoc Network – Survey

Sumit A. Khandelwal[1], Ashwini B Abhale[2]
Assistant Professor[1], Lecturer[2]
Department of Computer Engineering,
MIT Academy of Engineering, Alandi (D), Pune, India

Abstract - Vehicular ad-hoc networking is an emerging technology for future on-the-road communications. Due to the virtue of vehicle-to-vehicle and vehicle-to-infrastructure communications, vehicular ad hoc networks (VANETs) are expected to enable a plethora of communication-based automotive applications including diverse in-vehicle infotainment applications and road safety services. Even though vehicles are organized mostly in an ad hoc manner in the network topology, directly applying the existing communication approaches designed for traditional mobile ad hoc networks to large-scale VANETs with fast-moving vehicles can be ineffective and inefficient. To achieve success in a vehicular environment, VANET-specific communication solutions are imperative. Via inter-vehicle communications, drivers can be informed of crucial traffic information such as treacherous road conditions and accident sites by communicating with each other and/or with the roadside infrastructure. With better knowledge of traffic conditions, it is plausible that the problem of accidents can be alleviated. Traffic monitoring and management can also be facilitated by vehicular communications. This paper we focusing on the various attack in vehicular ad-hoc network. . The result of this work could guide a way to design a privacy preserve solution and present a trend of existing solutions.

Keywords— Vehicular networks, Security, Privacy, IVC, MANET, Attacks.

I. INTRODUCTION

Recently, Vehicular ad hoc network (VANET) [1] can offer various services and benefits to VANET users and thus deserves deployment effort. Vehicular networks are very likely to be deployed in the coming years and thus become the most relevant form of mobile ad hoc networks. In recent years, the number of motorists has been increasing drastically due to rapid urbanization. The number of automobiles has been increased on the road in the past few years. Due to high density of vehicles, the potential threats and road accident is increasing. Wireless technology is aiming to equip technology in vehicles to reduce these factors by sending messages to each other. Critical traffic problems such as accidents and traffic congestion require the development of new transportation systems [2]. Intelligent Transportation Systems (ITS) [3, 4] are aimed at addressing critical issues like passenger safety and traffic congestion, by integrating information and communication technologies into transportation infrastructure and vehicles. They are built on top of self-organizing networks, known as a Vehicular Ad hoc Networks (VANET), Vehicular communication systems facilitate communication devices for exchange of information among vehicles and between vehicles and roadside equipment. Working in tandem with the fielded Intelligent Transportation Systems (ITS) infrastructure, VANET is expected to enhance the awareness of the traveling public by aggregating, propagating and disseminating up - to - the minute information about existing or impending traffic-related events. Even though vehicles are organized mostly in an ad hoc manner in the network topology, directly applying the existing communication approaches designed for traditional mobile ad hoc networks to large -scale VANETs with fast-moving vehicles can be ineffective and inefficient. To achieve success in a vehicular environment, VANET-specific communication solutions are imperative. Via inter - vehicle communications, drivers can be informed of crucial traffic information such as treacherous road conditions and accident sites by communicating with each other and/or with the roadside infrastructure. With better knowledge of traffic conditions, it is plausible that the problem of accidents can be alleviated. Traffic monitoring and management can also be facilitated by vehicular communications. In support of their mission, VANET communications, employing a combination of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [4, 6] wireless communication are expected to integrate the driving experience into a ubiquitous and pervasive network that will enable novel traffic monitoring and incident detection paradigms[4]. It is widely known that, due to high-speed mobility[6], V2V and V2I communication links tend to be short lived. Thus, it is important to propagate traffic-related information toward a certain region of interest instead of sending to a particular vehicle; moreover, one of the best ways of propagating traffic-related advisories towards a particular region is some form of (controlled) broadcast transmission. Mobile nodes that are connected in a self-organized way without an underlying hierarchical infrastructure form mobile ad hoc network (MANET) [7]. The MANET is called a vehicular ad hoc network (VANET) in the special case where the mobile nodes are embedded in vehicles. The nodes of a VANET [1, 8] are commonly divided in two categories: On-Board Units (OBU), that are radio devices installed on

vehicles, and Road Side Units (RSU)[18], that constitute the network infrastructure. RSUs are placed along the roadside and are controlled by a network operator[2]. VANETs are expected to allow for transmission of information between vehicles or between vehicles and the roadside units (RSUs) [17] and, thus, to enhance the safety of both vehicle drivers and passengers [1].

Vehicular ad hoc networks (VANETs) are expected to enable a plethora of communication-based automotive applications including diverse in-vehicle infotainment applications and road safety services. Even though vehicles are organized mostly in an ad hoc manner in the network topology, directly applying the existing communication approaches designed for traditional mobile ad hoc networks to large-scale VANET with fast-moving vehicles can be ineffective and inefficient. To achieve success in a vehicular environment, VANET-specific communication solutions are imperative. Via inter-vehicle communications, drivers can be informed of crucial traffic information such as treacherous road conditions and accident sites by communicating with each other and/or with the roadside infrastructure. With better knowledge of traffic conditions, it is plausible that the problem of accidents can be alleviated. Traffic monitoring and management can also be facilitated by vehicular communications (e.g., vehicle platooning [1,5]) to elevate traffic flow capacity and improve vehicle fuel economy.

However, most of VANET researches focus on message transmission. Vehicle is extremely personal device; therefore, personal information, so-called privacy has to be protected. In proposed work in which analyze attacks, problems, and solutions based on topological network model. The network model's transparency design goal and protect vehicle's real identity even revealing the vehicle's location. We survey the existing attack on VANET and find out the existing solution and limitation of these work. The result of this work could guide a way to design an attack preserve solution and present a trend of existing solutions in future.

II. LITERATURE REVIEW

A. Attacks on Privacy

Attacks on privacy [14, 19] over VANETs are mainly related to illegally getting sensitive information about vehicles. As there is a relation between a vehicle and its driver, getting some data about a given vehicle´s circumstances could affect its driver privacy. These attacks can then be classified attending to the data at risk:

1) Identity revealing.

Getting the owner´s identity of a given vehicle could put its privacy at risk. Usually, a vehicle´s owner is also its driver, so it would simplify getting personal data about that person.

2) Location tracking.

The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle´s profile and, therefore, that of its driver[16].

Mechanisms for facing both attacks are required in VANETs. They must satisfy the tradeoff between privacy and utility. In this way, security mechanisms should prevent unauthorized disclosures of information, but applications should have enough data to work properly.

Existing studies related to the security and authentication for VANETs is based on the use of an asymmetric algorithm (Dedicated Short Range Communications (DSRC); IEEE). The sender signs each message before sending it using the asymmetric algorithm and the receiver verifies the originality of each received message. For reasons related to achieving high safety levels of ground transportation, it is recommended that each vehicle broadcast at regular time intervals information disclosing location, speed and direction (IEEE) [15].VANET is developed to support Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) [2,4] communication. For many years, global researchers and projects have been investigating VANET research issues: routing, security, address allocation etc. Based on these researches, some project group built a test bed and implemented programs on the vehicle for communication. The field test results of message exchange and network connectivity are satisfied. For an additional research, they focused on security issues in VANET. The application of vehicular ad hoc network (VANET) improves driving safety and traffic management. Due to the above applications, security attacks on VANET can be serious threats all the time. VANET is a special form of mobile ad hoc network (MANET). Hence any attacks exist on MANET also can be arisen on VANET. Moreover, some special attacks can be raised on VANET, which do not exist on MANET. Nevertheless, some characteristics of VANET can be positive effects and some can be negative effects on security issues. Before designing the security mechanism to defend attacks, the authors should take the positive effects and avoid the negative effects on the security of VANET. Furthermore, all possible attacks of VANET from every network layer. They also introduce the reason of forming every attack and the possible effect on VANET in detail.

Gilles Guette at el proposed [10] the influence of different assumptions on the success of Sybil attacks has been studied.It is a critical attack. In this type of attack an attacker transmits multiple messages with different ids to the other vehicles. In this way other vehicles feels that these messages are coming from different vehicles, so there is a jam further and they are enforced to take alternate route [5]. In other words, it say that the main task of the attacker is to provide an illusion of multiple vehicles to other vehicles and to enforce them to choose alternate route and leave the rod for the benefits of the attacker. This task is done by sending multiple messages with different ids.

Halabi Hasbullah at el proposed [11], Denial of service (DOS) attack in VANET. In DOS the main objective is to prevent the legitimate user from accessing the network services and from network resources. DOS attack can occur by jamming the channel system so that no authentic vehicle can access it . In VANET it is most serious problem as the user cannot communicate in the network and pass information to other vehicle which could result in more devastation in life critical

application. there are three ways the attackers may achieve DOS attacks, namely communication channel jamming, network overloading, and packets dropping Three different ways through attacker can achieve it.

1) In basic level the attacker overwhelm the node resource so that it cannot perform other necessary tasks which results in becoming the node continuously busy and not able to do anything else.

2) In extended level the attacker jam the channel by generating the high frequency in the channel so no vehicle is able to communicate to other vehicle in the network.

3) Drop the packets.

Halabi Hasbullah at el proposed [11], Distributed DOS (DDOS) attack is more severe than DOS attack as it is distributed in manner. In this attacker uses different location to launch the attack. They may user different time slot for sending the message. The time slot and the nature of the message may be different varied from vehicle to vehicle of the attackers. The main objective is to down the network so the network will not be available to the uses [11]. The two possibilities of DDOS attacks are:

1) Vehicle to Vehicle (V2V)
2) Vehicle to Infrastructure (V2I)

DDOS attacks directly affect the trust in a VANET network. When the attacks have successfully caused the network to break down, the trust for accessing and using the network services will no longer exist. Furthermore, the nodes may no longer believe on any received messages, thus leading to mistrust of the network and its services by the VANET nodes.

Vimal Bibhu el at [12] proposed, black hole attacks in VANET. In this problem, present the performance analysis of the black hole attack in Vehicular Ad Hoc Network and elaborate the different types of attacks and their depth in ad hoc network. The performance metric is taken for the evaluation of attack which depends on a packet end to end delay, network throughput and network load. a node refuses to participate in the network or when an established node drops out to form a black hole. In this all the traffic of the network get redirected towards a specific node which is actually doesn't exists which results in data lost. The malicious code chooses whether to drop a packet to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.

III. LIMITATION AND SCOPE OF RESEARCH

Paper [10] Proposed the results presented in this paper consider only the signal strength and direction analysis. As future work, we plan to study how node collaboration can reduce the success area of Sybil attacks. This technique is applicable to tuning the transmission power and using a bi-directional antenna instead of an omni-directional one. The basic goals of the attacker are to provide an illusion to other nodes by sending wrong messages and to enforce other nodes on the road to leave the road for the benefits of the attacker Paper [11] Proposed The network may be re-established in an attempt to provide continuous services, but it will be only available for short period before it breaks down and leads to unavailability of network and its services. Trust in the network may not be developed if attackers alter the life critical information before the intended recipient is really receiving it. Therefore, it is important to maintain network availability and to develop thrust in the VANET network, in order for the safety applications to be useful and beneficial to road users Paper [12] Proposed, black hole for AODV and OLSR protocol only. This protocol is the network protocols, these attacks are not supported to geographical protocol architecture.

Form the above limitations discussed; there is a scope for further research to address various issues in the design and implementation of secure system and its application for the VANET outdoor environment, in general, and more specifically to the attack and solution scheme for VANET

IV. CHALLENGES IN VEHICULAR AD-HOC NETWORK

The motivation for future network will need to manipulate precious information, with a possible impact on driver behavior and even on human life. Therefore, any solution needs to be thoroughly tested before integration in a real system. Field tests require not only implementation of the solution on real hardware, but also dedicated road infrastructure and equipped vehicles. These high costs have, until now, limited the size of these experiments at no more than 10–20 cars. Even the large-scale deployment scenarios that are currently prepared will only have the capacity to test a minor proportion from the proposals made by the vehicular ad-hoc networks (VANET) research community. On the other hand, the vehicular environment is highly complex and analytical models need to take into consideration not only the network, but also the properties of the vehicles and the behavior of the drivers simple traffic models are inappropriate for road traffic simulation, the impact of IVC on road traffic can be directly evaluated. The proposed research fulfill the requirement of privacy technique for location based and working for RSU unit. However, these solutions still require precise topological information, like building location. VANET simulation is the large number of nodes that need to be modeled. This is because in a wireless simulation, the receivers need to be searched among all the other entities. In the case of V2V networks, every node is also a source, therefore the number of communications is not constant and the resource consumption grows in this case with the square of the number of cars. proposed protocol is not only provides conditional privacy, a critical requirement in VANETs, but also able to improve efficiency in terms of the number of

keys stored at each vehicle, and identity tracking in case of a dispute. Meanwhile, our proposed solution can be deployed easily: does not require support from the roadside infrastructure or the OBUs is secure against adversary.

V. CONCLUSION

Vehicular Ad-hoc Networks (VANETs) will start becoming deployed within the next decade. Among other benefits, it is expected that VANETs will support applications and services targeting the increase of safety on the road, and assist in improving the efficiency of the road transportation network. However, several serious challenges remain to be solved before efficient and secure VANET technology becomes available, one of them been efficient authentication of messages in a VANET. There is a significant body of research work addressing this issue, however, while progress has been made, the challenge is still far from having been resolved and reliable and secure systems ready for deployment becoming available. Form the above limitations discussed; there is a scope for further research to address various issues in the design and implementation of privacy system and its application for the VANET outdoor environment, in general, and more specifically to the efficient and multi-level privacy-preserving communication protocol scheme for VANET.

REFERENCES

[1] Ho Ting Cheng, Hangguan Shan, Weihua Zhuang, Infotainment and road safety service support in vehicular networking: From a communication perspective, Mechanical Systems and Signal Processing 25 (2011) 2020–2038, journal homepage: www.elsevier.com/locate/jnlabr/ymssp.

[2] Josiane Nzouonta, Neeraj Rajgure, Guiling (Grace) Wang, "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 7, SEPTEMBER 2009.

[3] Razvan Stanica , Emmanuel Chaput, André-Luc Beylot, ―Simulation of vehicular ad-hoc networks: Challenges, review of tools and recommendations Computer Networks, journal homepage: www.elsevier.com/ locate/comnet2011.

[4] C. Sommer, Z. Yao, R. German, and F. Dressler, "Simulating the Influence of IVC on Road Traffic Using Bidirectionally Coupled Simulators," Proc. IEEE INFOCOM: Mobile Networking for Vehicular Environments (MOVE '08), Apr. 2008.

[5] M. Bakhouya , J.Gaber , P.Lorenz, "An adaptive approach for information dissemination in Vehicular Ad hoc Networks" Journal of Network and Computer Applications, journal homepage: www.elsevier.com/locate/jnca

[6] Razvan Stanica , Emmanuel Chaput, André-Luc Beylot," Simulation of vehicular ad-hoc networks: Challenges, review of tools and recommendations", Contents lists available at ScienceDirect Computer Networks journal homepage: www.elsevier.com/ locate/comnet

[7] A. Shastri, R. Dadhich, Ramesh C. Poonia, "Performance Analysis Of On-Demand Routing Protocols For Vehicular Ad-Hoc Networks" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011 DOI : 10.5121/ijwmn.2011.3407.

[8] Yasser Toor And Paul Mühlethaler, Inria " Vehicle Ad Hoc Networks: Applications And Related Technical Issues" IEEE Communications Survey, 3rd Quarter 2008, Volume 10, No. 3 www.comsoc.org/pubs/surveys

[9] Hannes Hartenstein, University of Karlsruhe Kenneth P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks" Toyota Technical Center.

[10] Paolo Cencioni , Roberto Di Pietro, " A mechanism to enforce privacy in vehicle-to-infrastructure communication" Computer Communications 31 (2008)2790–2802 www.elsevier.com/locate/ comcom

[11] Irshad Ahmed Soomro, Jamalul-lail Ab Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", World Academy of Science, Engineering and Technology, 65 2010, page no. 411 to 415. Online Available http://www.academia.edu/927299

[12] Vimal Bibhu,Kumar Roshan,Kumar Balwant Singh,Dhirendra Kumar Singh, "Performance Analysis of Black Hole Attack in Vanet" International Journal of Computer Network and Information Security(IJCNIS) ISSN: 2074-9090 (Print), ISSN: 2074-9104 (Online), IJCNIS Vol.4, No.11, October 2012.

[13] Bidi Ying , DimitriosMakrakis , Hussein T. Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs" , Contents lists available at SciVerse ScienceDirect journal homepage: www.elsevier.com/locate/jnca

[14] Ahren Studer, Elaine Shi, Fan Bai§, & Adrian Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs" CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office.

[15] Paolo Cencioni , Roberto Di Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication" Computer Communications 31 (2008) 2790–2802, Available on www.elsevier.com/locate/comcom

[16] Jinyuan Sun, Xiaoyan Zhu, Chi Zhang, Yuguang Fang, "RescueMe: Location-Based Secure and Dependable VANETs for Disaster Rescue" IEEE Journal On Selected Areas In Communications, Vol. 29, No. 3, March 2011.

[17] Ahren Studer, Elaine Shi, Fan Bai§, & Adrian Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs" CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office.

[18] Levente Butty´an, Tam´as Holczer, and Istv´an Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs" F. Stajano et al. (Eds.): ESAS 2007, LNCS 4572, pp. 129–141, 2007. c_Springer-Verlag Berlin Heidelberg 2007.

[19] Dandan Ren and Suguo Du, Haojin Zhu, "A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs", IEEE ICC 2011 proceedings, 978-1-61284-231-8/11/$26.00 ©2011 IEEE.

