The Current Security Challenges of Vehicle Communication In The Future Transportation System

Huu Phuoc Dai Nguyen [1,2], Rajnai Zoltán[1]

[1]Doctoral School on Safety and Security Science, Budapest, Hungary
[2]CanTho Economics Technology College, Vietnam
phuoc.daitt@bgk.uni-obuda.hu, rajnai.zoltan@bgk.uni-obuda.hu

***Abstract*—In the near future, drivers will be supported with an intelligent traffic system everywhere by the early warning signals. Moreover, this system can help to minimize vehicle collisions; increase the safe road; decrease the fatal injury for the pedestrians, passengers, and drivers; and inter-vehicle communication. These are some benefits of vehicle to vehicle communication (V2V).With the development of this technology, these vehicles can communicate together and with infrastructure or Road Side Units (RSU). In this article, the authors explored the basic concepts and the benefits of vehicle to vehicle communication. Furthermore, this paper points out several security concerns toward Vehicular Ad hoc Network (VANET) system, vehicle to vehicle and vehicle to infrastructure communication.**

***Keywords*:** security challenges, VANET, vehicle communication, V2V security.

I. INTRODUCTION

Nowadays, transportation plays an essential role in our daily lives. Thus, car producers not only improve vehicle design and performance day by day but also enhance the vehicle safety on the road. However, according to the report from World Health Organization (WHO) in 2015, there were over 1.2 million deaths caused by traffic accidents every year [1],[2]. Traffic accidents can be a terrifying fear for passengers, drivers and pedestrians in the road; family sorrows and social burdens. Hence, the development of Vehicular Ad hoc Network (VANET) system is one of the potential solutions to reduce a large number of roadway crashes and fatal accidents. In VANET system, vehicles can share information together, known as vehicle to vehicle communication (V2V) and between vehicles and infrastructure (V2I). With the boosting of this technology, it allows vehicles to become new generation vehicles for a better transportation system. Besides, this technology can increase traffic safety, support efficient mobility services and diminish environmental impacts. However, the potential risks of cyber-attacks towards vehicle communication are increasing when vehicles can connect via the Internet and wireless network. In this article, the authors first described the general concepts of vehicle communication; then, the authors indicated several possible cyber-attacks towards vehicle communication in the future transportation system.

II. THEORETICAL BACKGROUND

A. Vehicular ad hoc networks (VANETs)

Vehicular ad hoc networks (VANETs) are related to mobile ad hoc networks (MANETs) communication for transferring data between the vehicles [3], [4]. Additionally, VANETs consist of vehicle to vehicle (V2V) and vehicle to road side units (RSU) or vehicle to infrastructure (V2I) communication [5],[6]. The most essential components in the VANETs architecture are RSU, Application Unit (AU) and On Board Unit (OBU). While the RSU keeps an application to give services, the AU is the device in the vehicle that the providers use to communicate with OBU via wireless or wired connection, and OBU is a wave device which is integrated with on-board vehicle in order to transfer information with RSUs or other OBUs [7]. In addition, VANETs is a foundation of the intelligent transportation system (ITS) and smart cities. In this network, vehicles are able to send and receive messages from other vehicles or RSU via wireless medium connection. The vehicles with suitable hardware can access and process the location data like global positioning system (GPS) or differential global positioning system (DGPS) receiver in VANET [8], [9]. Moreover, this network offers a lot of benefits such as emergency notifications (warning lights, highway construction or maintenance, weather broadcast's board, highway danger zone announcement, and stop or go traffic information), road vehicle communication, and inter-vehicle communication [10]. With this technology, it can give the promise for a better future scenario in transportation system in general, a safe life for pedestrians, passengers and the drivers in specific.

B. Vehicle to vehicle (V2V)

Vehicle to vehicle (V2V) is a technology which offers a network communication for vehicle to connect each other. This technology was first developed and demonstrated in 2005 by General Motors [11]. Besides, V2V is also a collision avoidance technology based on sharing information among the vehicles nearby to alert the drivers about the hazardous cases [12]. For instance, vehicles with an automated emergency braking system inside could help the drivers activate the brake system

automatically based on calculation in safe zone between two vehicles to prevent unexpected potential crashes. Moreover, V2V communication system supported a number of wireless-based features in the vehicles which could enhance the safety for traffic, roadway efficiency and driver convenience [13], [11]. In fact, Huang and Lin [14] suggested a system which could give the warning signal to drivers before collision happening by using an Early collision warning algorithm (ECWA) and global positioning system (GPS). This system calculated distance between vehicles and sent the alert messages to the drivers in order to reduce collision. In V2V environment, the vehicles communicated together via Dedicated Short Range Communication (DSRC) [15] to share vehicle information such as speed, braking status, location and the like to other vehicles or RSU. Regarding this technology, it could be used for early collision warning, reducing the fatal crashes, improving the safety in the road and applying various applications to make a better life.

C. Vehicle to infrastructure (V2I)

Similar to V2V technology, V2I communication based on wireless connection to exchange critical safety and operational data between vehicles and RSU or highway infrastructure in order to reduce vehicle crashes via DSRC protocol [16]. Moreover, V2I plays an essential role in collecting data from global or local information on traffic and road conditions, then it suggests vehicle behaviors on the street [17]. There were several potential safety applications which were deployed in V2I such as red light violation warning, curve speed warning, stop sign gap assist, reduced speed zone warning, spot weather information warning, stop sign violation warning, railroad crossing violation warning and oversize vehicle warning [16] to avoid vehicle crashes.

D. V2V's benefits

Nowadays, with the evolvement of VANET technology, vehicle can communicate together itself and the road side units (RSU) or road infrastructure by using DSRC, wireless, Bluetooth [18], ZigBee, Radio, Cellular, GPS, Wi-Fi and Ultra-Wide Band [19] to share location, speed, and acceleration with n eighbor vehicle; long distance communication. Regarding DSRC protocol (5.9 GHZ) with a 360 degree view, vehicle can detect the threats and give the warning signals to the drivers for reducing the collision because the drivers cannot recognize the potential dangers during the traveling behind the wheel in some cases [20]. For instance, V2V can alert the driver to decrease the speed because there is another car ahead suddenly brakes or another car is quickly entering the street. Moreover, V2V brings some safe technologies such as collision avoidance system, driver warning system, automated emergency braking assistance, and vehicle stability system [11]. The collision avoidance system as well as driver warning system and vehicle stability system play an essential role in decreasing the collision and enhancing safe conditions in the road. Indeed, one vehicle appears in the safe zone while another one is on the road, this technology will automatically send the alert to the driver in order to react in time. Besides, the automated emergency braking assistance is combined with the sensors to give real time information, the position, the speed and the emergency case. Therefore, it can help the drivers brake the vehicle in time, when he or she cannot handle it.

III. THE SECURITY CONCERNS TO VANET

According to Santosh et Rama [4], they demonstrated all possible cyber-attacks in VANET environment. These attacks targeted to three major groups like availability, authentication and confidentiality vulnerabilities in VANET [Table 1].

TABLE 1: TYPE OF ATTACKS IN VANET

	Type of attacks	Effect of attacks	Impact
Availability	DoS	Jamming the channel, users can't communicate in the network	High
	DDoS	Breaking down the network	High
	Spamming	Consuming the bandwidth of the network	Low
	Black hole	Making data lost, making first step for man in the middle attack	High
	Malware	Limiting VANET operation	High
Authentication	Sybil attack	Providing illusion of many vehicles to force the vehicles get off the road for attacker's goal	High
	Node Impersonation	Changing driver's identity and car's identity to deceive the police when accident happens	Mediu m
	Message suppression	Preventing the authorities and RSU to know about the collision	Mediu m
	Alteration	Changing or modifying exist data to deceive the users	Mediu m
	Relay	Capturing and replaying the packet to puzzle the authorities and prevent vehicle's identity in any accident	High
	GPS spoofing	Taking the identity and	High

		geographic location of vehicles on the network to fool them.	
	Tunneling	Conducting a traffic analysis or preparing for forwarding attack	High
Confidentiality	Timing attack	Modifying the actual content time to create delay time for message	High
	Home attack	Taking control of the user vehicle	High
	Man in the middle attack	Controlling all communication between the sender and receiver to inject or modify message between vehicles	Mediu m
	Traffic analysis	Using the packets to analyze the important information of vehicle like ID, location	High
	Social attack	Confusing the victim to make driver disturb	Low
	Brute force	Using this technique to break the cryptography key	High
	ID disclosure	Taking vehicle's ID and monitoring the victim s' vehicle route	High
	Bogus information	Broadcasting false information to affect the decision of other vehicles	Mediu m

IV. THE SECURITY CHALLENGES IN V2V

A. Controller Area Network (CAN)

In the past, car manufactures deployed point to point wiring systems for the electronic device inside link together [21]. Therefore, it led cars become heavier and expensive with a big wire in car's skeleton. However, in 1985, Bosch company invented CAN for connecting vehicle electronic device [21],[22]. This new technology brought some advantages such as reducing cost, the complexity and weight of wiring system; developing serial communication bus; and combining with in vehicle network's standard. The CAN communication protocol showed how the information moved between the devices in the system and integrated with the Open Systems Interconnection (OSI) at two layers as data link layer and physical layer [22], [Figure 1].

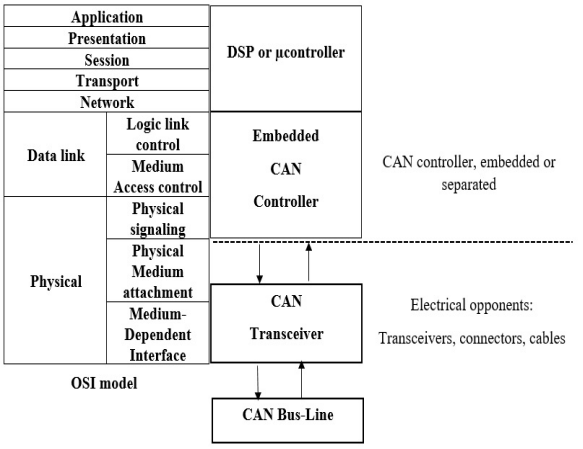

Figure 1: CAN model integrated with OSI model (ISO 11898 standard architecture)

Inside every vehicle, there are the electronic control units (ECUs) consisting of CAN interface in lieu of the analog and digital signal inputs to the system [Figure 2]. Nonetheless, CAN is easily targeted by the advisory because there is no such security mechanism to protect it. For instance, Hoppe et al. [23], [24], [25], demonstrated the attackers could exploit CAN vulnerabilities to control electric window lift, warning lights, brake, airbag control system, and so on in a car by using CarShark software.

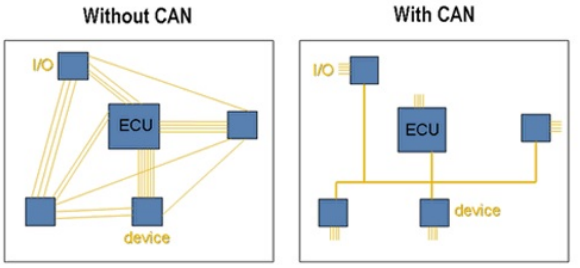

Figure 2: CAN network in reducing wiring system in vehicle [21]

B. In-car wireless network

To improve the safety of vehicles, car producers designed the first wireless network in new vehicle in USA - namely the tire pressure monitoring system (TPMS). TPMS can improve the road safety, braking distances, traction and tire rolling resistance because it can send the alert signal to the drivers to let them know about the tire pressure status. However, Rouf *et al.*[26], [24] described an attacker could use the eavesdropping and spoofing method to control TPMS via a passing vehicle in 40 meters distance. They found that TPMS did not have any cryptographic mechanisms and used a fixed ID in every packet during transmission, which increased the ability of tracking vehicle via these identifiers.

C. Electronic control units (ECUs)

Nowadays, many car manufactures produce the cars with the embedded electronic components inside. These

systems are interconnected, monitored, and controlled by ECUs through some gateways in the car's network [27]. Nevertheless, Koscher et al. [24], [25] showed that an attacker can take the control of an ECU to activate some functions like body control modules, engine control modules and electronic brake control modules.

V. THE SECURITY ISSUES IN V2I

Based on the vulnerabilities of confidentiality, integrity, and availability in V2I interface, there are several security attacks as shown [Table 2], [28].

TABLE 2: TYPE OF ATTACKS IN V2I INTERFACE

Type	Effects of attack	Feasibility
Distributed denial of service (DDoS)	Breaking down the network, services unavailable	High
Impersonation	Disrupting the network, hiding identity	High
Message alternation	Affecting to the safety service provided by RSUs	Moderate
Malware and spam	Leading potential dangerous interruption in service for an RSU	Low
Eavesdropping	Stealing the sensitive and private information of drivers or vehicles	Moderate

VI. CONCLUSION

V2V communication technology is becoming more popular, realistic and perhaps every vehicle will be provided by this technology in the near future. This technology can enhance travel safety and reduce the traffic jams or delays caused by vehicle crashes. In this paper, the authors introduced several possible cyber-attacks toward VANET, vehicle to vehicle communication, and vehicle to infrastructure communication. Although this technology offers several benefits for the users, the security issues of vehicle communication should be considered. Therefore, cybersecurity protection is crucial for the future. In the future research, the authors intend to figure out the solutions for detecting cyber threats from malicious attacks and implement some safety applications to make vehicle communication environment safer.

VII. ACKNOWLEDGEMENTS

The research presented in this paper was carried out as part of the EFOP-3.6.2-16-2017-00016 project in the framework of the New Széchenyi Plan. The completion of this project is funded by the European Union and co-financed by the European Social Fund.

VIII. REFERENCES

[1] World Health Organization, "WHO - Road Traffic Accidents," *None*, p. 2015, 2015.

[2] T. Toroyan, "Global status report on road safety," *World Heal. Orgainisation*, p. 318, 2015.

[3] P. I. Offor, "Vehicle Ad Hoc Network (VANET): Safety Benefits and Security Challenges," no. 2009, 2012.

[4] S. Santosh, Sharma; Rama, "Vanet: Security Attacks and Its Possible Solutions," *J. Inf. Oper. Manag.*, vol. 3, no. 1, pp. 301–304, 2014.

[5] E. Fonseca *et al.*, "Support of anonymity in VANETs-putting pseudonymity into practice," *Wirel. Commun. Netw. Conf. WCNC*, pp. 3402–3407, 2007.

[6] S. Kim and I. Lee, "A secure and Efficient vehicle to vehicle communication scheme using Bloom filter in VANETs," vol. 8, no. 2, pp. 9–24, 2014.

[7] R. Barskar and M. Chawla, "Vehicular Ad hoc Networks and its Applications in Diversified Fields," *Int. J. Comput. Appl.*, vol. 123, no. 10, pp. 7–11, 2015.

[8] E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward," *ICAC 2014 - Proc. 20th Int. Conf. Autom. Comput. Futur. Autom. Comput. Manuf.*, no. September 2014, pp. 176–181, 2014.

[9] J. Jakubiak and Y. Koucheryavy, "State of the Art and Research Challenges for VANETs," *2008 5th IEEE Consum. Commun. Netw. Conf.*, pp. 912–916, 2008.

[10] W. Enkelmann, "FleetNet - Applications for inter-vehicle communication," *IEEE Intell. Veh. Symp. Proc.*, pp. 162–167, 2003.

[11] K. Shah, E. M. Parentela, and D. Ph, "A Case Study on Potential Benefits of V2V Communication Technology on Freeway Safety."

[12] NHTSA, "What are the advantages of V2V?," pp. 1–4, 2014.

[13] Ronald K. Jurgen, *V2V / V2I Communications for Improved Road Safety and E ciency V2V / V2I Communications for Improved Road Safety and Efficiency*. 2012.

[14] S.-Y. L. Chung-Ming Huang, "An early collision warning algorithm for vehicles based on V2V," *Int. J. Commun. Syst.*, vol. 23, no. 5, pp. 633–652, 2010.

[15] N. H. T. S. Administration, "FMVSS No. 150 Vehicle-To-Vehicle Communication Technology For Light Vehicles," *Off. Regul. Anal. Eval. Natl. Cent. Stat. Anal.*, no. 150, 2016.

[16] J. Harding *et al.*, "Vehicle-to-Vehicle Communications : Readiness of V2V Technology for Application," no. August, p. 327, 2014.

[17] L. Glielmo, "Vehicle-to-Vehicle/Vehicle-to-Infrastructure Control," *Impact Control Technol.*, 2011.

[18] S. J. Mccormick and S. Mccormick, "Key Areas of Security Risk for Connected Vehicles," 2017.

[19] M. Khairnar, D. Vaishali, and D. Pradhan, "V2V communication survey wireless technology," *arXiv Prepr. arXiv1403.3993*, vol. 3, no. 1, pp. 370–373, 2014.

[20] A. L. Svenson, "NHTSA Update : Connected Vehicles V2V Communications for Safety V2V Overview," 2015.

[21] "Controller area network (CAN)." [Online]. Available: http://www.ni.com/white-paper/2732/en/.

[22] S. Corrigan, "Introduction to the Controller Area Network (CAN)," *Texas Instruments*, no. August 2002, pp. 1–17, 2016.

[23] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networksPractical examples and selected short-term countermeasures," *Reliab. Eng. Syst. Saf.*, vol. 96, no. 1, pp. 11–25, 2011.

[24] C. Lin and A. Sangiovanni-vincentelli, *Security-Aware Design for Cyber-Physical Systems*. 2017.

[25] G. Mastakar, "Experimental security analysis of a modern automobile," *IEEE Symp. Secur. Priv.*, pp. 1–16, 2012.

[26] I. Rouf *et al.*, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study.," *Proc. USENIX Secur. Symp.*, vol. 39, no. 4, pp. 11–13, 2010.

[27] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," *Proc. Int. Conf. Dependable Syst. Networks*, 2013.

[28] M. Islam, M. Chowdhury, F. Asce, H. Li Student, H. Hu, and A. Professor, "Cybersecurity Attacks in Vehicle-to-Infrastructure (V2I) Applications and their Prevention," vol. 7656, 2017.