Survey on Cyber Security of CAV

Qiyi He
Nottingham Geospatial Institute
University of Nottingham
United Kingdom
qiyi.he@nottingham.ac.uk

Xiaolin Meng
Nottingham Geospatial Institute
University of Nottingham
United Kingdom
xiaolin.meng@nottingham.ac.uk

Rong Qu
Department of Computer Science
University of Nottingham
United Kingdom
rong.qu@nottingham.ac.uk

***Abstract*—with the ever fast developments of technologies in science and engineering, it is believed that CAV (connected and autonomous vehicles) will come into our daily life soon. CAV could be used in many different aspects in our lives such as public transportation and agriculture, and so on. Although CAV will bring huge benefits to our lives and society, issues such as cyber security threats, which may reveal drivers' private information or even pose threat to driver's life, present significant challenges before CAV can be utilised in our society. In computer science, there is a clear category of cyber security attacks while there is no specific survey on cyber security of CAV. This paper overviews different passive and active cyber security attacks which may be faced by CAV. We also present solutions of each of these attacks based on the current state-of-the-art, and discuss future improvements in research on CAV cyber security.**

Keywords—Cyber Security; CAV; Autonomous Driving

I. Introduction

With the fast development of technology, autonomous driving is becoming to one of the mostly investigated issues around the whole world. According to the Boston Consulting Group Report [3], the market size of autonomous driving will reach 42 billion dollars by 2025. Different companies, from traditional car manufacturers such as BMW to emerging internet based companies such as Google [4], are investing enormous human efforts and money into the development of connected and autonomous vehicles (CAV) or driverless vehicles. These vehicles are all connected, have access to internet, and communicate with the surrounding environments via different sensors without drivers' involvement [5].

Public have also showed great interest in the realization of CAV. According to an observation report conducted by Cetelem in 2015 [1], 81% of the drivers said they wish to drive a 100% autonomous car in 10 years. Moreover, lots of countries also issue laws to support the legality of CAV and allocate space for the CAV developers to conduct field tests, including Detroit Motor City [6] and Silicon Valley [7] in the USA. In 2016, 20 states in USA introduced legislations of autonomous vehicles [8]. In Ibaraki, Japan, a 15km^2 test field will be put into use from 2017 [9]. In China, the first CAV test field, the National Intelligent Connected Vehicle (Shanghai) Pilot Zone, was set up in Shanghai [10]. The friendly development environment promotes the research and development of CAV around the world. It is believed that 2021 will be the beginning year of CAV's utilisation from technical perspective [11]. Though, there are still some concerns about the CAV such as morality and safety.

CAV could be used in a number of scenarios such as public transportation, surveying and mapping, etc. Along with the convenience it brings to our daily life, CAV are also faced with lots of safety issues. CAV usually use sensors to perceive the surrounding environments to model, and plan accordingly the following decisions and movements. In addition, the V2X (Vehicle to everything) communications allow CAV to communicate with other vehicles, pedestrians and infrastructure. One CAV could be equipped with various platforms to realize complex functions. After 2009, plenty of car manufacturers produced vehicles with internet access and entertainment devices, which are vulnerable to hacking regardless of their make or model. In 2015, two white hat hackers attacked a Jeep Grand Cherokee successfully [2], the results could be dangerous if such skills are used inappropriately.

The most effective way is to physically isolate the car with the outside environment, however, users need vehicles to communicate with the whole environment to get information, it is impossible to isolate the vehicles [12]. This paper concerns cyber security in CAV, and discusses problems faced and generated by CAV. Possible defence methods for cyber security attacks in CAV will also be discussed.

II. Cyber Security Attacks faced by CAV

In computer science field, the cyber security attacks are divided into 2 main parts and 6 more detailed parts [13]. However, in cyber security of CAV, there is no specific category.

Considering that CAV is kind of mobile computer, the communication theory is similar to the Internet communication, the cyber security in CAV could also be divided into 2 main parts, which are passive attacks and active attacks.

A. Passive Attacks

Passive attacks eavesdrop or monitor the transmissions between users, where the attackers cannot modify or change the content in the transmission, and would not interact with the data transmitted [14]. Passive attacks most probably faced by CAV include the follows:

- Eavesdropping and Release of the Information. During the usage of CAV, the attacker could eavesdrop the vehicle's situation and the communication message sent between the V2X communication channels. The messages include destination between the driver and the vehicle. In addition, in future CAV where the V2X communications play more important roles, attackers could eavesdrop communication messages between the vehicles or with the infrastructure and pedestrians, thus more private information could be monitored by attackers without permissions. Such information could be released to companies of a range of interests, or may lead to further physical damages to drivers.
- Traffic Analysis. To certain extend, CAV designers could address the eavesdropping problem and use cryptography to encrypt the messages thus only authenticated users or devices could decrypt the content. However, attackers could also use traffic analysis method to obtain the length and time of these messages, and with such information, could gather further information such as the time the car is used, and thus user's working time and time of their daily activities.

Normally, passive attacks are difficult to identify because the attackers do not modify the content in the message. The receiver and sender are not aware of that there is a 'man' between them. CAV manufacturers however could prevent the attacks while designing the vehicles to encrypt not only the messages but also the communication channels. In conclusion, to deal with passive attacks in CAV, defending and protecting is more important than fixing passive attacks.

B. *Active Attacks*

Despite passive attacks, attackers are more likely to take actions to modify or damage the messages and the data transmitted in active attacks [15]. These could cause much more damages than passive attacks especially in the CAV environment, and cause fatal injuries to drivers. In CAV, active attacks could be divided into four categories, which are listed below:

- Spoofing. Spoofing attack is conducted by faking identities or data. This happens when an unauthorised attacker pretends to be an authorised user. For example, the attacker pretends to be a nearby vehicle, and sends a wrong location to the driver. If the driver believes that there is no obstacle in front of the car, it may cause a serious accident. Moreover, attackers could also falsely report a fake car accident to the service platform. Other vehicles using the platform may be influenced to make wrong decisions based on the false information. It is crucial to authenticate the service provider and the drivers in this scenario. For example, it is more reliable to find a third party organization to store the authentication information. Such method is also widely taken by banks nowadays. In addition, new algorithms and frameworks also need to be established to filter false information and messages. For example, if there are 10 vehicles nearby, and 9 of them reported a traffic jam while only one said there is not, it is essential to check the authenticity of the messages of last one.
- Replay Attack. Attackers could intercept the message with authentication from sender to receiver, and resend the message to the receiver to obtain the authenticated access to the service. In CAV, this could also happen. Attackers do not need to know the content inside the package, so the encryption of data is useless in this attack. However, we could still use challenge response to deal with replay attacks, where after the sender sends a message, the receiver could send the challenge value and sender responds to it to get the authentication access.
- Modification. In this kind of attacks, attackers could modify the message such as GPS information between the communication channels. In 2016, a location-based reality game named Pokémon Go attracted millions of game players around the whole world. This game is based on GPS information. After installing the game on game players' phones, the players could track Pokémon in different locations worldwide. As not all types of Pokémon are available at all locations around the world, to get specific Pokémon they want, some game players modified the GPS positioning data of their phones. Some players also sell the modify equipment online [16]. The company Nintendo has developed some methods to detect players who modified the data by identifying those players who move too fast, or who have collected specific Pokémon that are not in players local areas. In the end, Nintendo banned all the accounts that falsely modified GPS data.

In CAV, the attackers could also easily modify their locations by using this method. Car manufacturers could design protocols or algorithms to detect the falsely modified data and punish the driver, for example, use the machine learning method to filter the data, like the technology now used in email account to tell spam. GPS data could also be used into the process because each car will generate huge amount of location data every day. The inspection method can also be combined with the GPS data processing procedure to clean useless data.

- Denial of Service (DoS). DoS attacks will block the access to the target server [17] by making use of flaws in the system or protocol to send huge amount of data, or request to interfere the receivers' network. This attack may cause delay and breakdown of the receivers' response. In some situations, delay may be not serious. However in CAV, the request of time is comparatively really high, and one second could cause or avoid an accident. If one vehicle could not process the data received, the vehicle could cause injuries to people. To avoid this kind of attacks, system need to be checked and updated frequently, and the protocols need to be improved continuously. It is also crucial to set up firewall to filter useless information and keep recording the security log and check if there is a security attack.

Compared with passive attacks, active attacks are much more difficult to defend but much easier to detect. It is crucial that, the CAV designers and car manufacturers always carefully consider all the possible flaws in the CAV systems and protocols.

According to the description above, based on the computer cyber security category, the main attack CAV may face are from 6 types, which range from the hardware part to software part.

III. The Attacks Caused by CAV

Despite of the attacks CAV may face, CAV could also be a security risk in our daily life. It has been reported that Tesla in USA caused fatality indirectly [19]. Except from the physical damage caused by CAV, there still are other risks.

First of such risks is the violation of privacy. CAV are equipped with many different sensors including cameras and LIDAR. Cameras are used to take pictures as a method of surveying and mapping. The pictures could contain someone's face incidentally, which may be a potential problem of privacy. If the pictures and their locations were uploaded to internet by someone, there could be an issue of a release of private information.

Moreover, with the increased tensions and conflicts around the world, CAV could also be used as a method to conduct criminal damage to innocent people. Especially in government, military area, the safe usage of CAV should also be enhanced. In high risk areas including government military areas, the CAV communication channels and frequency should be different, and public and commercial CAV should be prohibited.

IV. Methods To deal with Attacks

To avoid these attacks, CAV should follow these principles:

- Authentication. The CAV and service platform should be authenticated by each other or by a reliable third party company. Every time in the V2X communication and the usage of the vehicle, there should be a check procedure to verify both identities. The authentication process is also important in specific areas such as military and government area. Normal CAV should not be allowed to enter these areas or communication.

- Encryption. In message transmissions, all the messages should be encrypted to make sure that no one could monitor or modify their content. A good encryption should be strong enough to prevent decryption. In Europe, some tests on encryption in V2X communication use public keys [18]. Many encryption methods in computer security could be used in the V2X communications because we could regard CAV as a mobile computer.

- Standard and Regulation. Despite computer technologies which can be used to defend attacks, appropriate standards and regulations should also adapted to reduce CAV attacks such as the data content in V2X communications and the confidentiality of information in CAV. For example, when an accident happens and causes injuries such as the latest Tesla one [19], the responsibility need to properly defined and regulated in legislation.

V. Conclusion

Along with the fast development of technologies and research in science and engineering, the realization of CAV is not far away from being in our daily life. Despite the lots of benefits to our daily life, CAV is faced with plenty of cyber security threats. This paper discusses different categories of cyber security attacks based on existing computer securities issues. These include passive attacks and active attacks. Possible solutions to deal with these attacks have also been proposed.

Despite the existing research and development of CAV technologies, there still are lots of work to do. Extensive research to defend CAV cyber security attacks need to be conducted on authentication, encryption, standards and regulations.

References

[1] L'OBSERVATOIRE CETELEM, 2015. Consommation en Europe: 2009-2014, Les Annees Qui Ont Tout Change. Available on http://observatoirecetelem.com. Retrived at 10/03/2017

[2] Andy G. (2015, July 15). Hackers Remotely Kill a Jeep on the Highway - With Me in It. The wired website. Retrieved March 10, 2017, from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[3] BCG: Autonomous car market to hit 42 billion by 2025. (2015, June 01). Retrieved March 10, 2017, from http://www.consultancy.uk/news/2065/bcg-autonomous-car-market-to-hit-42-billion-by-2025

[4] Behere S, Torngren M. A functional architecture for autonomous driving[C]//Automotive Software Architecture (WASA), 2015 First International Workshop on. IEEE, 2015: 3-10.

[5] Gehrig, Stefan K.; Stein, Fridtjof J. (1999). *Dead reckoning and cartography using stereo vision for an autonomous car*. IEEE/RSJ International Conference on Intelligent Robots and Systems. **3**. Kyongju. pp. 1507–1512. doi:10.1109/IROS.1999.811692. ISBN 0-7803-5184-3.

[6] Mcity. *University of Michigan*. 9 December 2016. Retrieved 13 March 2017. from: http://www.mtc.umich.edu/test-facility

[7] Melanie Z. (2016, April 22). Silicon Valley startup to test self-driving cars in California. The Hill Website. Retrieved 13 March, 2017. from: http://thehill.com/policy/transportation/277274-silicon-valley-startup-to-test-self-driving-cars-in-california

[8] Autonomous Vehicles/ self-driving Vehicles Enacted Legislation. (2017, Feburary 21). Retrieved March 13, 2017. from: http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[9] Japan plans test site for self-driving cars. (March 24, 2016). Retrieved March 13, 2017. from: http://asia.nikkei.com/Tech-Science/Tech/Japan-plans-test-site-for-self-driving-cars

[10] Where in the World are Self-Driving Cars? (January 10th, 2017). Retrieved March 10, 2017. from: http://insuranceblog.accenture.com/where-in-the-world-are-self-driving-cars/

[11] Alitimeter, 2017. The Race to 2021: The state of Autonomous Vehicles and a “Who’s who” of Industry Drivers. Available on: https://www.slideshare.net/Altimeter/the-race-to-2021-the-state-of-autonomous-vehicles-and-a-whos-who-of-industry-drivers

[12] Navigant, 2016. Autonomous Automotive Cybersecurity: The Need to Protect Automated and Connected Vehicles. Available on: https://www.karambasecurity.com/pdf/Autonomous-Automotive-Cybersecurity-Report.pdf

[13] Stallings W. Cryptography and network security: principles and practices[M]. Pearson Education India, 2006.

[14] Gagandeep A, Kumar P. Analysis of different security attacks in MANETs on protocol stack A-review[J]. International Journal of Engineering and Advanced Technology (IJEAT), 2012, 1(5): 269-75.

[15] Sahadevaiah K, PVGD P R. Impact of security attacks on a new security protocol for mobile ad hoc networks[J]. Network Protocols and Algorithms, 2011, 3(4): 122-140.

[16] Guy Buesnel. One of the Keys to defeating spoofing is to detect it in devices[J]. Coordinates, 2017, 1(1): 11-12

[17] Hasbullah H, Soomro I A. Denial of service (DOS) attack and its possible solutions in VANET[J]. World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 2010, 4(5): 813-817.

[18] Weiß, C. (2011). V2X communication in Europe – From research projects towards standardization and field testing of vehicle communication technology. *Computer Networks*, *55*(14), 3103–3119. https://doi.org/10.1016/j.comnet.2011.03.016

[19] Boudette, N. E. (2017, January 19). Tesla’s Self-Driving System Cleared in Deadly Crash. *The New York Times*. Retrieved from https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html