WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Security Issues in Connected Autonomous Vehicle

P B Savitha[1], Madhu S[2]

[1]Dayananda Sagar College of Engineering, Bengaluru
[2] BNM Institute of Technology, Bengaluru

ABSTRACT

The growth in autonomous vehicles and its adoptability in the today's society is not a nightmare. The journey of intelligent and autonomous vehicles has come far away with the recent advancement in its control, driving and especially in communication and connectivity related aspects. The cyber security is a major issue in all web connected devices. Hence the connected vehicles are not an exception. The cyber attacks on connected vehicles are classified broadly based on the three important parts of the system namely control system, driving system components and V2X communications. In this paper a review of various cyber security attacks on connected vehicles, importance of cyber security and its side effects are discussed.

Keywords: connected autonomous vehicle, cyber security issues

The journey of intelligent and autonomous vehicles popularly known as connected autonomous vehicles (CAV) has come far away with the recent advancement in its control, driving and especially in communication and connectivity related areas. The CAV's are able to connect to various external devices and vehicle to everything. The advance technologies like artificial intelligence, cloud computing, vehicle to everything changed the conventional security concept and susceptible to various cyber issues.[1,2] . As the communication technologies mature, the vehicles are capable to connect to an external devices and vehicle-to-everything (V2X), the necessity to secure communications becomes evident. Meanwhile, the established computer security policies are not followed by the industry standards for in-vehicle and vehicular communications because of constraints of hardware and differences in configurations of network [3,4]. Hence the cyber security is a major issue in all network connected devices. In addition to this, the increased connectivity in vehicles and complexity of the system would provide the wider opportunities for malicious attacks and resulting in exploiting the devices [5].Hence the risk of cyber attack is a growing concern. The cyber attack may become national public security problem due to personal privacy disclosure and economic loss, endangers people's life safety. The predicted statistics of connected vehicles vulnerable to cyber security is shown in table 1.The expected rise of connected autonomous vehicles in 2030 is about 370 million with partially automated feature 13 million with highly automated and the amount of globally sold automated vehicle in the year 2040 is about 33 Million[6].

Table 1. A predicted data of automated vehicles [6]

Year	**Number of vehicles estimated**
2015	1.4 Million number of vehicle recalls (1.4 Million number of Vehicle was recalled in the USA for cyber security vulnerabilities for the first time in history)
2018	Approximately 100 Million ECU's is exist modern vehicle
2030	370 Million number of Vehicles will have various automated features.
	13 Million number of vehicles will be highly automated
2040	33 illion number of autonomous vehicles will be sold globally

Material and Methods:

The overview of communication in connected autonomous vehicles.

The CAV's major zones are broadly categorized and are shown in Figure 1.1. The In-vehicle, the Communications and Back end systems are the three major categories. The In-vehicle contains protocols such as Local Interconnect network (LIN), Computer Area Network (CAN), FlexRay [3]. The second category is communication between in-vehicle and back end system, this also contains navigation systems, telematics modules etc., .The third category is about back end system or server cluster which is used by service provider.

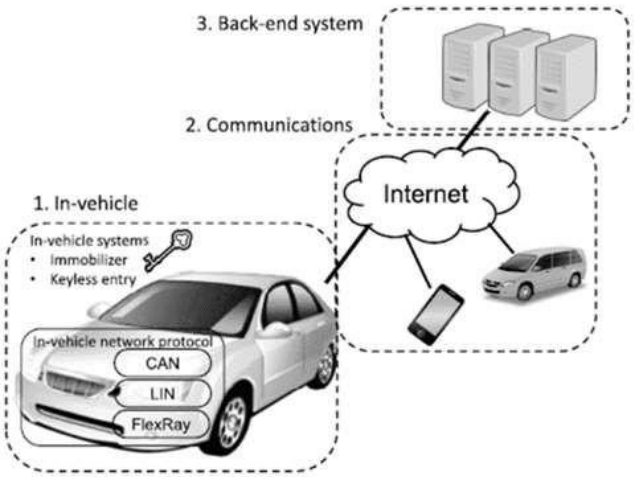

Figure 1.1: The environment surrounding connected vehicles [7]

The control, communication and sensors are the three areas of CAV which are directly prone to cyber attacks. The associated parts or the system responsible are categorized under three headings namely control, driving system components and V2X communications. The cyber issues arise in CAV are directly linked to these three headings. The figure 1.2 shows the type of control with the vehicle, the communicating devices/ connecting systems and the basic sensors used which are responsible to communicate via sensing the relevant signal.

Figure 1.2 The Connected Autonomous Vehicle system.[8]

The type of communications in CAV are (i) within the vehicle - which is interaction between different vehicular sub systems, (ii) with infrastructure (V2I) - it is bi directional information exchange with external road systems such as traffic lights and street lights and cameras, (iii) with devices (V2D) - in this type the interaction with other road users mobile devices such as pedestrians, cyclists, drivers or passengers, (iv) with each other (V2V) - wireless data transmission between vehicles about real time positions and speeds and (v) with other networks (V2N) - wireless data exchange between vehicles and networks to access cloud-based infrastructure[9,10] The most common in-vehicle network architecture and the major control parts of the vehicle under each protocol is listed [11,12,13].

1. Gate way:
2. Local Interconnect Network (Body Control)

Instrument

Door/Seat

Light/Climate

Remote Keyless entry (RKE)

3. Controller Area Network (CAN)(Power Train)

Power Train sensors

Hybrid Drive

Transmission

Engine Controller

4. Media Oriented System Transport (Ethernet)-Infotainment

   Phone

   Audio/Video

   Navigation

   Display

5. Flex Ray –(Safety and Chassis Control)

   Air Bag

   Chassis Control

   Steering Control

   Braking Control.

The Engine control unit (ECU) is used in all connected autonomous vehicles. The role of ECU is to control the vehicle through signal acquisition, signal processing and control of electronic component associated to it. The ECU's are connected through

(i) Controller Area Network (CAN) which is serial communication protocol which supports distributed real time control.

(ii) FlexRay which is an automotive network communication protocol and it is faster and more reliable compared to CAN

The number of key ECU's in CAV is, Navigation control module (NCM), Engine control module (ECM), Transmission control module (TCM), Electronic brake control module (EBCM),Telematics module with remote commanding, Inflatable restraint module (IRM), Body control module (BCM), Vehicle vision system (VVS), , Radio and entertainment centre, Remote door lock receiver, Heating, ventilation, and air conditioning (HVAC), Instrument panel module.

The Table .1.1 shows the type of communication network, topology, and maximum data rate in inter-vehicle wired interconnection

Table 1.1 Inter-vehicle wired interconnection communication technologies [14]

Network	**CAN**	**LIN**	**Domestic Digital Bus**	**Flex Ray**	**Ethernet**	**Media oriented systems transport**	**Interface description block**	**Low Voltage differential Signaling**
Maximum data rate	1Mb/s	19.2kb/s	11.2Mb/s	20 Mb/s	100 Mb/s	150 Mb/s	400 Mb/s	655Mb/s
Topology	Linear bus, Star,ring	Linear bus	Ring	Linear bus,star, or hybrid-high	Linear bus star	ring	Linear bus,Star,ring	Point-Point

a. Cyber security attacks faced by connected autonomous vehicles.

In connected autonomous vehicle the components are controlled by various electrical control units (ECU's) which are connected together with internal and external communicating devices in tern by networks. In whole it is a Cyber Physical system which contains hundreds of lines of codes. The attacks are listed under network and protocol attacks, phishing attacks, password and key attacks. The CAV attacks are also classified as passive attacks and active attacks. In passive attack, hackers cannot alter the data during the transmission and also not able to interact with the transmitted data. The passive attacks are eaves dropping, release of the information and traffic analysis.

The type of advanced persistent threats is, Spoofing Attacks, Denial of Service Attacks (DOS), Malware Attacks, Malicious Mobile Apps and Hacker Attacks. Due to these attacks the system in the vehicle get attacked are Infotainment system, Smart/Remote keys, In-vehicle and loud based networks, Software updates /downloads, In-Vehicle sensors, Vehicle data server, Wireless communication functions, Smart phone connections, Onboard diagnosis, ECU (Electronic Control units).

The parts such as automotive control system which consists of Electronic control unit (ECU) , Controller area network(CAN), Local inter connect network (LIN),Radio Frequency (RF), FlexRay and the autonomous driving system components like LIDAR, Video Camera, GPS, radar sensor, central

computer, ultrasonic sensor and vehicle to everything (V2X) provides traffic efficiency, traffic safety, infotainment. The major system components and sensors of CAV are shown in the Figure 1.3 .

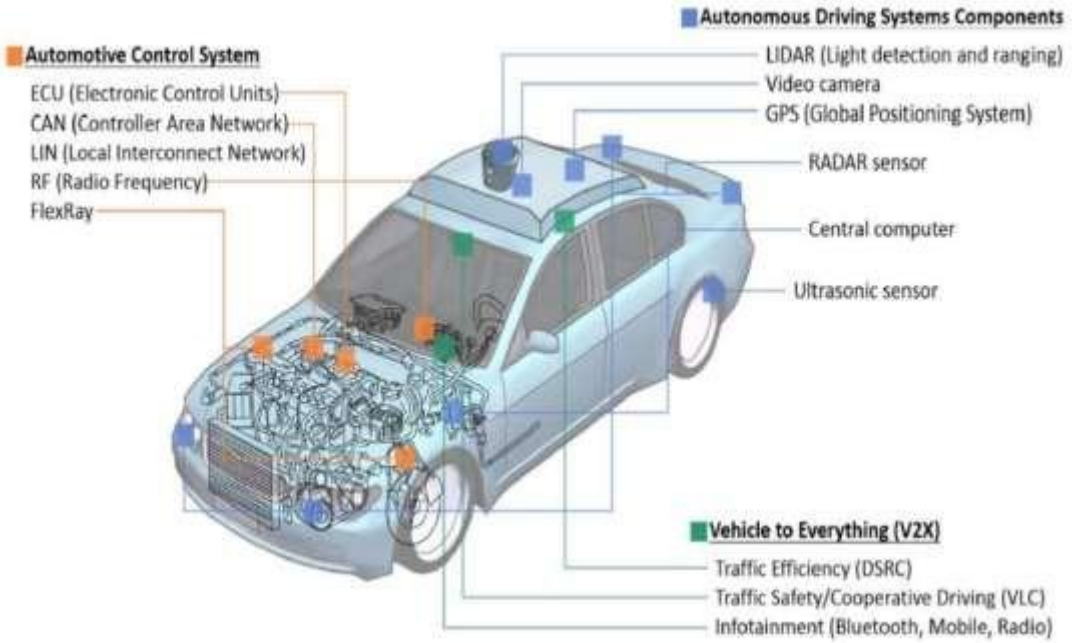

Figure 1.3 Surface /systems/components of CAV [14]

Figure 1.4 Surface /systems/components prone to Cyber attacks in CAV [8]

The consequence of cyber attack may affect the various parts of the autonomous vehicles. Some major attacks and its consequences are listed.[1]

- Driving function fail
  - Loss of brake control,
  - Loss of engine control
  - Loss of Steering Control.
- Vehicle system fail

- Dysfunctional door locks
- Inoperative lights
- Disrupted passenger safety systems

➢ Vehicle theft

Track vehicle GPS Co-ordinates

Take over Control

Vehicle sold or hold to ransom

➢ Data theft

Infrastructure data

Personal data

Vehicle data

➢ Collision

- Liability questions
- Driver injuries or deaths
- Pedestrian inquiries or deaths

➢ Commercial loss

Brand damage

Reduced buyer confidence

Revenue loss

➢ Other system fail

➢ Faulty diagnostics

- Disrupted entertainments
- Manipulated navigation
- Telematics

The analysis of network attacks against vehicles in the recent 10 years is presented in Table 1.2 and the categories of sever attacks are listed in Table 1.3.

Table 1.2: The network attacks against vehicles in the recent 10 years [15]

Attack Mode	**Attack Entrance**	**Attack Model**	**CIA Threat**
Direct physics	CAN illegal access OBD port	Frame sniffing, message playback, etc.	Integrity and confidentiality
	OBD port	Frame sniffing, message playback, and camouflage, DOS attack, etc.	Integrity and confidentiality
A little distance Wireless attack	Bluetooth	Frame sniffing, message playback, and camouflage	Integrity and confidentiality
	TMPS, tire pressure monitoring system	Sniffing, message replay, and camouflage	Integrity and confidentiality
Integrity and confidentiality	Remote wireless /Wi-Fi, etc	Message replay and camouflage, etc	Integrity and confidentiality

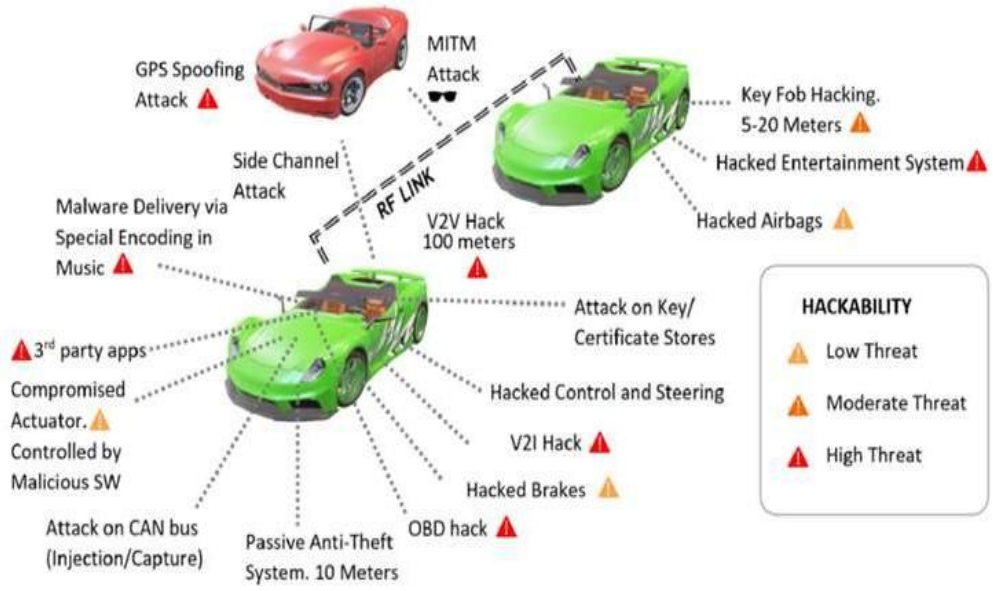

Figure 1.5 Possible Cyber Vulnerabilities in Connected Autonomous Vehicles [8]

The Figure 1.5 shows the cyber vulnerabilities in CAV's.

Table 1.3: Categories of severity of attacks [16]

Level	Type of Threat	Attack types
1	Critical	mislead cameras/fake vision (cameras ,Remote control (audio/video devices);); hidden objects (LiDAR); fake identity (cloud authority),hidden objects(radar); spoofing (GNSS);
2	High Threat	Fake objects (LiDAR); DoS attack (battery system); injection (in-vehicle system);); fake objects (radar);modification(in-vehicle system); modification (V2V communication); change infrastructure sign (V2I communication); injection (cloud dataset); fake/ghost message (V2V communication); modification (cloud dataset)
3	Moderate Threat	DoS attack (V2V communication); Blind vision (cameras); jamming (LiDAR); jamming (radar); jamming (GNSS); eavesdropping (in-vehicle system);traffic analysis (in-vehicle system); block/remove sign (infrastructure sign); road line changing (road)
4	Lower Threat	Loud volume (audio/video devices); fake sound (audio/video devices)

b. The cyber security challenges and mitigation approaches:

Cyber secure implementation of connected autonomous vehicle system involves designing and developing of secured network. In order to implement it, the prerequisites of the system is to have authentication, integrity privacy and availability of the data or information is important [3,17]. However, due to the continuing progression in communication, vehicle infrastructure, and operating systems, the proposed methods may not provide security throughout the life span of vehicle

The mitigation can be categorized from the point of hardware such as sensors, control units, software's and various protocols used and its connected external /internal devices. The modes of mitigation are prevention, reduction, transference, acceptance and contingency.

Prevention: The prevention is for passive attacks like eves dropping, by encrypting the messages in communication channel. If the messages are encrypted, it is more difficult for attackers to hack the information. , For example, a blind vision attack to the camera, the other sensors may be used after abnormal attack detection. [18]

Reduction: The reduction is to reduce the possibility of cyber attacks. It is achieved by having redundant sensors in the system. If one sensor is attacked by hackers the redundant sensor will provide the data to the system.

Transference: It is sharing possible risks with others such as third party organizations including insurance companies and government organizations. . This mitigation method is applicable when a single supplier or manufacturer could not manage all the information safely.

Acceptance: Accepting the risks on effect of cyber attacks with minimal impact on CAV's. For example a traffic analysis is a signal which is attacked but it is not causing any physical damage to the system.

Contingency: It takes care of the possible reactions if the attacks happen. In brief ,a provision for a possible after attack plan to recover the system. For example a battery loss due to denial of service (DoS) attack, it could pull up the CAV to a safe place.

Another method of mitigation is achieved by a multi layered approach. This helps in industry to adopt best practices and improves the security to the vehicle.

Developing layered approach cyber security protections for vehicles reduces the risk of a successful vehicle cyber-attack and mitigate the potential cyber attacks. A systematic approach is followed by,

- For critical vehicle system, a risk-based prioritized identification and protection process for critical vehicle systems.
- Timely detection and rapid response to potential vehicle cyber security incidents, architectures, methods, and measures that design-in cyber security and cyber resiliency, facilitating rapid recovery from incidents when they occur.
- Methods for effective intelligence and information sharing across the industry to facilitate quick adoption of industry-wide lessons learned.
- Creation of standards that articulate best practices.

Conclusion:

In this paper a brief concept of connected autonomous vehicles and various parts which are vulnerable to cyber security issues are discussed. Cyber security attacks faced by connected autonomous vehicles and proposed solutions to mitigate the issues are presented in a systematic way.

References:

[1] Steve Bell, "The Connected car taxonomy Decoded: An Overview of connected autonomous vehicles and intelligent transportation systems", White Paper Heavy Reading Reports: The Connected Car Taxonomy Decoded, July 17.

[2] Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller. "Cyber threats facing autonomous and connected vehicles: Future challenges." IEEE transactions on intelligent transportation systems 18, No. 11 (2017): pp. 2898-2915.

[3] Dibaei, Mahdi, Xi Zheng, Kun Jiang, Robert Abbas, Shigang Liu, Yuexin Zhang, Yang Xiang, and Shui Yu. "Attacks and defences on intelligent connected vehicles: A survey." Digital Communications and Networks 6, No. 4 (2020): pp. 399-421.

[4] Roscoe, Jonathan Francis, Oliver Baxandall, and Robert Hercock. "Simulation of malware propagation and effects in connected and autonomous vehicles." 2020 International conference on Computing, Electronics & Communications Engineering (ICCECE), 17-18 August 2020, Southend, UK

[5] McCall, Sophia, CagatayYucel, and Vasilios Katos. "Education in Cyber Physical Systems Security: The Case of Connected Autonomous Vehicles." In 2021 IEEE Global Engineering Education Conference (EDUCON), pp. 1379-1385.IEEE, 2021.

[6] TUV SUD Report, "Potential Cyber Security Threats of Anomalous and Connected Vehicles: Consequences and Safety Solutions". 2018, www.tuvsud.com/autonomous-driving

[7] Junko Takshi,"An Overview of Cyber Security for Connected Vehicles"IEICE TRANS. INF. & SYST., VOL.E101–D, NO.11 , November 2018,pp-2561-2575.

[8] Barry Sheehan, Finbarr Murphy, Martin Mullins, and Cian Ryan. "Connected and autonomous vehicles: A cyber-risk classification framework." Transportation research part A: policy and practice 124 (2019): 523-536.

[9] M.H. Eiza, Q. Ni, Driving with sharks: rethinking connected vehicles with vehicle cybersecurity, IEEE Vehicle. Technology. Magzine (2017).

[10] P. Carsten, M. Yampolskiy, T.R. Andel, J.T. Mcdonald, In-vehicle networks: at-tacks, vulnerabilities, and proposed solutions, in: Proceedings of the 10th Annual Cyber and Information Security Research Conference, 2015.

[11] J. Deng, L. Yu, L. Fu, H. Oluwakemi, R.R. Brooks, Security and data privacy of modern automobiles, in: Data Analytics for Intelligent Transport Systems, Elsevier Inc., 2017, pp.131–163.

[12] J. Petit, S.E. Shladover, Potential cyberattacks on automated vehicles, IEEE Trans. Intell. Transp. Syst. 16 (2015) 546–556.

[13] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, B. Weyl, Security requirements for automotive on-board networks, in: 9th International Con-ference on Intelligent Transport Systems Telecommunications, 2009.

[14] Kim, Kyounggon, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. "Cyber security for autonomous vehicles: Review of attacks and defence." Computers & Security 103 (2021): 102150.

[15] Guan, T.; Han, Y.; Kang, N.;Tang, N.; Chen, X.;Wang, S. "An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles",Sustainability **2022**, 14, 5211.

[16] He, Qiyi, XiaolinMeng, and Rong Qu. "Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles." Journal of advanced transportation 2020 (2020).

[17] G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities, "Future Generation Computer Systems, 2018.

[18] Makowitz Rainer ,Temple Christopher . FlexRay-A communication network for automotive control systems. 2006 ,IEEE International Workshop on Factory Communication Systems.