Analysis of Risks and Threats in Connected and Autonomous Vehicles

Jigyasa Bajpai
MBA TECH Comp. 2019-24
MPSTME, NMIMS
Mumbai, Maharashtra, India

Shiwansh Raj
MBA TECH Comp. 2019-24
MPSTME, NMIMS
Mumbai, Maharashtra, India

Pushpit Jain
MBA TECH Comp. 2019-24
MPSTME, NMIMS
Mumbai, Maharashtra, India

Abhinav Mathur
MBA TECH Comp. 2019-24
MPSTME, NMIMS
Mumbai, Maharashtra, Indi

Abstract— CAVs are connected and autonomous vehicles that do not require a driver to be attentive and controlling the vehicle all the time. These allow you to have a calm experience while travelling privately without even having the need of driving or knowing how to drive. CAVs are gaining popularity and require complex systems of various electronic, radio and satellite components. With this gaining popularity and usage of CAVs along with wide complex systems, there appear security risks and threats. Here in this paper, we are going to discuss various levels of the automations as defined as standardized with most common components of a CAV, then we will discuss what are the different types of attacks, several network and communication challenges used and faced by any CAV with the diverse defending and protection mechanisms for improving the security of the CAVs.

Keywords— CAVs, attacks, networks and communication.

I. Introduction

The autonomous vehicle has gained a lot of attention and momentum in the past decade. A fully autonomous vehicle is 'one in which a driver is not necessary'. Connected and Autonomous Vehicles (CAVs) incorporate many different technologies to enable driver-less, safe, and efficient transportation artificial intelligence systems, which employ machine learning techniques to collect, analyse and transfer data, in order to make decisions. Electric car companies, such as Tesla, embrace this trend to automate driving with their capabilities to push over-the-air software updates to all vehicles manufactured. For most of this time, it has only been viewed by the public to be a futuristic concept that is far from ready to fruition. Now that this concept is becoming a reality and we are getting closer to the actual deployment of such systems from all major car manufacturers, one critical concern remains unaccounted for, security.

According to the Boston Consulting Group Report, the market size of autonomous driving will reach 42 billion dollars by 2025. These vehicles are all connected, have access to the internet, and communicate with the surrounding environments without drivers' involvement via fitted out different sensors, antennas, including cameras, Radio Detection And Ranging (Radar), and other replacements of manual mirrors of the current cars. In addition, the V2X (Vehicle to everything) communications allow CAV to communicate with other vehicles, pedestrians and infrastructure. Autonomous cars and trucks use complex software, combined with physical feedback to change lanes, avoid collisions, and maintain routes. All these make CAVs prone and vulnerable to attacks.

An attacker may have many inspirations to hack the various aspects of the CAV including but not limiting to - To defame the manufacturing company, to take revenge against someone, trying to kill someone due to personal reasons or on a job given by someone, messing up the data or putting someone's life at risk for blackmailing for personal or other profits, for fun or as a challenge etc. Thus it is important for the users as well as manufacturers to know about the security risks on different layers and take appropriate measures accordingly, some of which are still topics currently under research or future potential risks.

II. Levels and Components

A. Levels of CAVs

SAE International (Society of Automotive Engineers) defines six levels of driving automation. The US Department of Transportation has also adopted these SAE levels. Below are brief descriptions of each level.

Level 0 – No automation; all major systems are human-controlled.

Level 1 – Includes automated systems, such as cruise control or automatic braking.

Level 2 - Partial driving automation, but human intervention is still needed.

Level 3 – Conditional automation and environmental detection; human override still necessary.

Level 4 – Officially driverless vehicles. Can operate in self-driving mode in limited areas and speeds, but legislative and infrastructure limitations restrict full adoption of these vehicles.

Level 5 – Full vehicle autonomy; no legislative or infrastructure restrictions limitations and no human interaction required. Testing of fully autonomous vehicles is currently ongoing in several markets globally; however, none are currently available for the public yet.

B. Components

There are various designs for autonomous vehicles, but the most common components normally include advanced software enabling artificial intelligence, navigation systems, advanced driver assistance system (ADAS) sensors, cameras, radar, and LIDAR (Light Detection and Ranging). Additional supporting infrastructure includes:

- Wi-Fi networks.
- Roadside computing units.
- Vehicular cloud services.
- Dedicated short-range communications (DSRC).
- Vehicle-to-vehicle (V2V).
- Vehicle-to-infrastructure (V2I).
- Other vehicle-to-everything (V2X) systems.

Without even going in-depth on the various technologies, the level of complexity of autonomous vehicles is clear. Unfortunately, a high level of complexity brings an increased level of risks. This makes autonomous vehicles very tempting targets for hackers.

Automobiles today are supervised by hundreds of computational units using Intra-Vehicle communication instead of simply connecting different mechanical devices. The Intra-Vehicle coordination of these units provides better driving experience to the driver while Vehicle-to-Cloud system provide car manufacturers the abilities to push hot patch over-the-air through their firmware upgrade system. These systems greatly improved the efficiency of modern automobiles, however, the added complexities also bring new security risks that need to be addressed. Besides Intra-Vehicle communication and Vehicle-to-Cloud, Vehicle-to-Vehicle and Vehicle-to-Roadside infrastructure communications are also trending industry topics.

Fig1: indicates the possible points of attack and their purpose and damages.

III. Types of Attacks

Types of attacks can be classified into three major groups as:

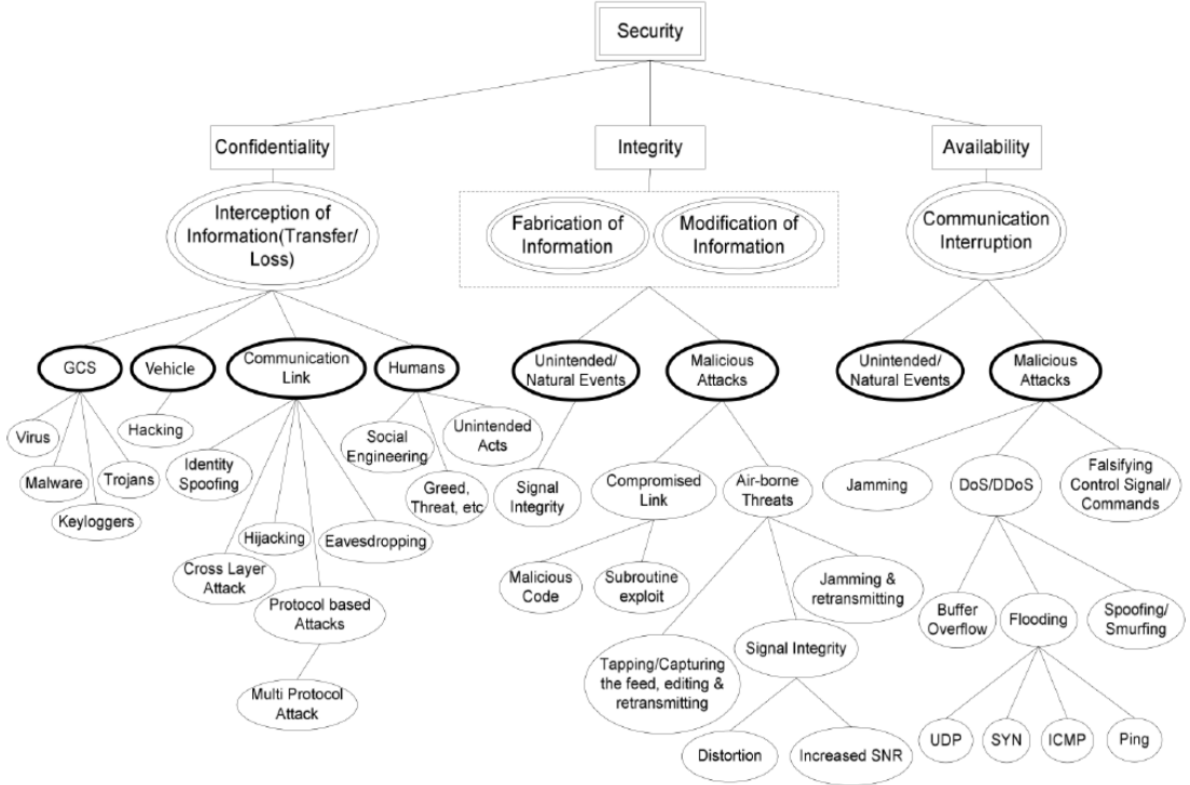

Fig. 1. Possible points of attack and their purpose and damages [3]

A. *Hardware Attack*

Many defence-critical applications such as unmanned aircraft, unmanned vehicles, robotics are using embedded systems and sensor devices at an increasing rate. It used to be the case that a vehicle is an isolated device with perhaps a simple ECU chip controlling the parameters of the vehicle. With the evolution of technologies, we're now in an era where hackers can gain access to millions of vehicles in the world remotely at the same time. However, these embedded systems aren't designed to handle the stream of information and attacks made available by the Internet and this weakness exposes them to the hardware attacks both when they are assembled and in usage. Embedded systems are more vulnerable to attacks because most embedded systems have minimal security measures, limited by the physical constraints of computing power and memory on board. Such system, when exposed to attacker, will allow the attacker to take complete control of the vehicle

B. *Firmware / OS Attack*

In most embedded systems, firmware that controls the functionalities are stored in the flash memory of the chip. The ability to update vehicles' on-board software over the air provides the convenience of obtaining security patches and new features without going to the service centre. However, such a channel, if controlled by an attacker, can be used to obtain control of the vehicles. OS are known to be vulnerable to the Denial of Service (DDoS) attacks. In September 2016, Keen Security Lab of Tencent, a tech giant in China, demonstrated a vulnerability to gain complete control of a brand-new Tesla Model S with the latest unmodified firmware and security patches.

C. *Services Attack*

With the advent of autonomous driving and modern vehicle technologies, our vehicles are more powerful and connected than ever. These functionalities rely on fundamental infrastructure services such as GPS, Cellular Network, Internet, Vehicle-to-Vehicle communication and so on. Just like some hackers are hijacking DNS servers to obtain their goals, cars might suffer from a hijacked infrastructure or services that lead to malfunction of its autonomous driving capability. Only this time, hackers and Artificial Intelligence might be able to assassinate someone from miles away by spoofing GPS of the vehicle's on-board navigation system. Although we currently don't have the complete standards of how vehicles will communicate in the future, the network currently used by Unmanned Aerial Vehicle (UAVs) could shed some light on how an attack targeting the infrastructure could severely damage the functionality of an autonomous car.

Just like UAVs today, vehicles will have the abilities to communicate with each other and with satellite and ground stations. The autonomous driving feature of the vehicle will rely highly on GPS and Vehicle-to-Vehicle communication, both can be manipulated by attack to achieve their goal to tamper with the vehicle and injure the passengers. By spoofing GPS, attackers can cause traffic jams so that police won't be able to catch up with their criminal activities such as robbing a bank. Or they might hijack a VIP to kidnap him. The image recognition technologies can be manipulated by changing the landscapes of the traffic signs or lanes so that the vehicle will be stopped or hijacked. The microphone installed on the vehicle's voice recognition system might be used to eavesdrop sensitive political / financial information. The on-board map data might be modified to fit the attacker's agenda. Security issues related to autonomous vehicles remain to be quite a challenge.

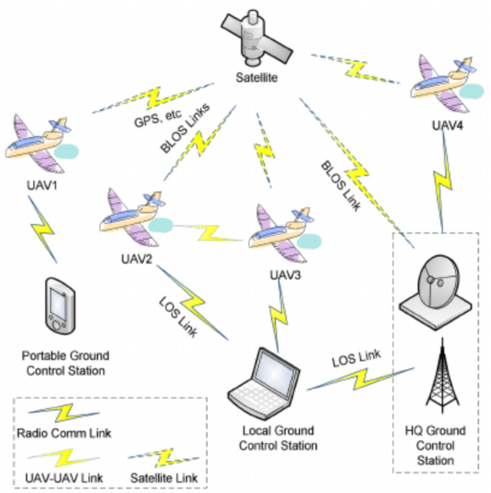

Fig. 2. Different satellite links and communications [3]

IV. Network and Communication Challenges

CAVs need to communicate with and detect the various components of the environment to function properly. These are required to detect traffic, changing lanes, secure from any obstacles in the way, and many more. These communications are classified in following types :

A. *Communication Networks:*

1) Intra-Vehicle Network : The intelligent intra-vehicle system can monitor the vehicle condition, and more importantly, it assesses the tiredness of the driver. This system, called onboard equipment (OBE), gathers drivers' data and

predicts the driver's tiredness using machine learning techniques. By gathering vehicle information (e.g., speed and GPS) and driver behaviour information (facial expression, head movements), the system can make valuable predictions that, if urgent, alerts the driver with a warning signal. The durability of the embedded chips should also be considered since the flawed data directly misleads machine learning techniques and the result leads to a potential risk to the driver. Fortunately, as the development of microprocessors such as Intel Atom evolves to be low-power and cost-efficient, the higher computational power can promote the usage of OBE

2) Vehicle-to-vehicle communication : Vehicle-to-vehicle communication (V2V) assists drivers by interacting with other vehicles and sharing warning messages wirelessly on the V2V communication platform [6]. The wireless LAN localization is the root for this service, the various signals (GSM, AM/FM radio, GPS) can be received and handled to the vehicle by these local LANs.

3) Vehicle-to-Cloud communication: The widespread use of mobile devices and the huge improvement in 3G/4G mobile broad-band technologies enables vehicles to use mobile networks for better services. Car companies such as Nissan, Ford, and Toyota have already been involved in vehicle-to-cloud connectivity. The high-speed service is particularly useful in providing driver assistance in real time. Besides that, the cloud service creates an ideal infotainment and entertainment environment for the drivers. The top challenge of the cloud service is the latency of the network. How to filter, process and send information is a complex task that will affect the efficiency of the overall real-time network.

4) Vehicle-to-Vehicle Communication : Vehicle-to-roadside infrastructure communication for environmental sensing and monitoring is another important function module for autonomous cars. When drivers provide the information of their cars to roadside sensors, this sensor will use the information that drivers provide and combine with weather conditions then automatically informing the drivers of real-time road conditions. Sensing data of road conditions can be transmitted to vehicles, and at the same time, these vehicles will transmit the information to other vehicles by vehicle- to-vehicle communication. Besides, the anti-collision detection system using adaptive cruise control will be also applied to the vehicle-to-roadside communication application. There is also a problem that should be worked out. Since the information will be from various nodes, prioritization, buffering, and queuing techniques should be designed to keep a very good order when tremendous data flock in. Radio-frequency identification (RFID) tags and receivers can be used to detect the situation of roads. This technology will help autonomous cars detect vulnerable road users (VRU) such as pedestrians or bicyclists, especially at road intersections and some hazardous sections. Every VRU would be recognized and road sensors would transmit their information to vehicles around.

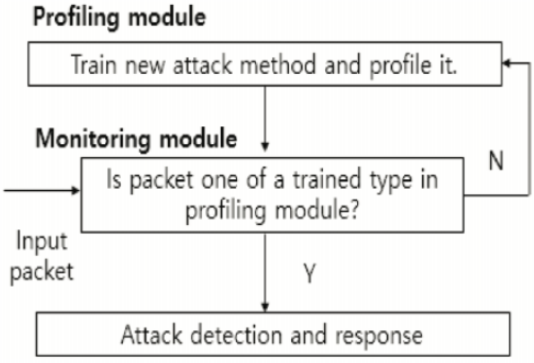
Profiling module
Train new attack method and profile it.
Monitoring module
Is packet one of a trained type in profiling module?
N
Input packet
Y
Attack detection and response

Fig3:Architecture of IDS based on ML techniques [3]

B. *Intrusion Detection using Deep Neural Network*

A common architecture of the IDS based on machine learning is like the Fig below. The IDS includes different modules for collecting and analysing a huge number of data packets which come from CAN. The monitoring module in IDS will extract the features or certain packets and detect the information about it. The profiling module includes various features which are trained off-line. When the monitoring module identifies a new attack which does not exist in the database, the profile module will update the database. Then the monitoring module will identify the same attack type. However, some research pointed the common way to train profiling module for intrusion detection is inefficient and very easy to occur error, especially in the issue of back- propagation (in each layer of neural network, the gradient of the error surface is computed while the gradient decreases with some layers, and it will probably cause a slow convergent speed). To improve IDS, Kang et. al proposed two main phases, the training phase and the detection phase, as shown in Fig below. In the training phase, the system will train every CAN packet and mark them with binary label information and extract features, then utilize DNN structure to train the features with weight parameters. In the detection phase, the same CAN features will be extracted, and the DNN structure computed with the trained parameters will help make the final decision. After introducing DNN structure which can provide the probability of intrusion, the IDS can help discriminate secure and in-secure packets and finally identify malicious attacks.

V. Defending and Protection Mechanisms

To better secure autonomous vehicles, three risk levels should be taken into account:

- Critical hardware and software components that receive over-the-air updates must have supply chains that are adequately understood and protected.
- The vehicle's operating system must use an interface that is secure and equipped to repel cyber security threats.
- Vehicle operating centers need to be secure.

While it is possible to use strong security measures and mechanisms in ordinary networks to protect it, the limited processing power of the In-vehicle network subsystems does not allow the same. Furthermore, CUs usually come from different vendors. Thus, it is not feasible to design one security solution for the whole system. One suggestion is to isolate the In-vehicle physical network to make sure that infecting one subsystem will not affect the entire network. However, this is not feasible with the increasing need for those subsystems to communicate among each other.
Recently, three main approaches have emerged to protect/defend connected vehicles against cyber security threats, and respond as quickly as possible to the reported hacks.

1) OTA Solution : One of the biggest challenges that the auto industry faces is to retrofit protection mechanisms in vehicles that were not secure or need to be secured against a recent threat/vulnerability. This may include software fixes, firmware upgrades, and security patches. To address this challenge and avoid costly recalls, more vehicles' manufacturers start using the OTA (Over-The-Air) updates. While OTA updates represent a reasonable solution to respond to cyber threats in connected vehicles, it suffers a major problem. Fixing vulnerabilities using OTA updates is a security risk. When OTA is delivered to the connected vehicle, it means that a remote code is allowed to execute. Thus, if security is not well implemented around the OTA updates, it can lead to serious consequences.
Some security mechanisms such as authenticating the OTA update, use a secure protocol to deliver it, and cryptographically verify the OTA update must be in place. This is also called Secure OTA (SOTA).

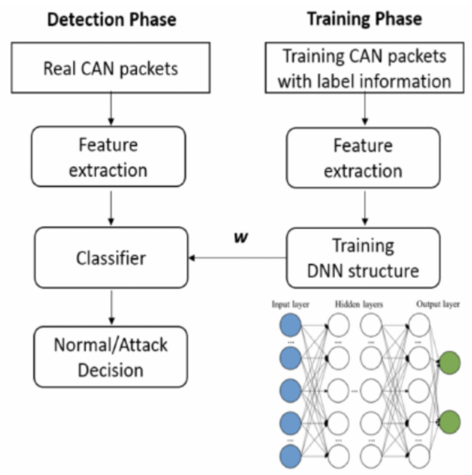

Fig. 4. Deep neural network structure [3]

2) Cloud-based Solutions : Since it is not feasible to protect each In-vehicle subsystem individually, centralised solutions have emerged to protect the In-vehicle network and consequently the connected vehicle.
For instance, Ericsson has developed a cloud-assisted solution called the Connected Vehicle Cloud (CVC) system. The CVC system establishes a new channel between the vehicle and a variety of services and support. The security layer provided in CVC ensures that the communication between the vehicle and the system is encrypted. It also contains an anomaly detection unit to detect any malicious attempt to hack into the vehicle. Finally, through a secure gateway, CVC filters the contents of the web surfing traffic to make sure that no viruses or malwares could infect the vehicle.
Some authors proposed a cloud-assisted vehicle malware defence framework, since it is impractical to rely on the vehicle itself to defend against malware. The authors present lightweight malware defence functions, in terms of processing power and storage, that operate in the vehicle. With the assistance of a security cloud, the on-board malware defence functions will have full access to a wide range of malware defence mechanisms and an up-to-date large malware information database. This eliminates the limited storage problem in the In-vehicle network. It is also suggested that the traffic can be routed through the security cloud to filter out any viruses or malware before reaching the connected vehicle.

While the cloud-based solutions to secure connected vehicles look very promising, there are three main issues to examine.

First, communications overhead and the delay incurred by routing the traffic through the cloud services need more investigation (e.g., routing V2V and V2I traffic to the cloud to defend against DSRC attacks is impractical).

Secondly, these solutions heavily depend on the fact that the cloud-based systems are secure. However, if the cloud-based system is infected with malware, it will spread to all its connected vehicles and could lead to severe damages.

Finally, these solutions assume that vehicles are connected to the cloud-based system all the time via the Internet. This may not be possible everywhere and would incur high costs for consumers.

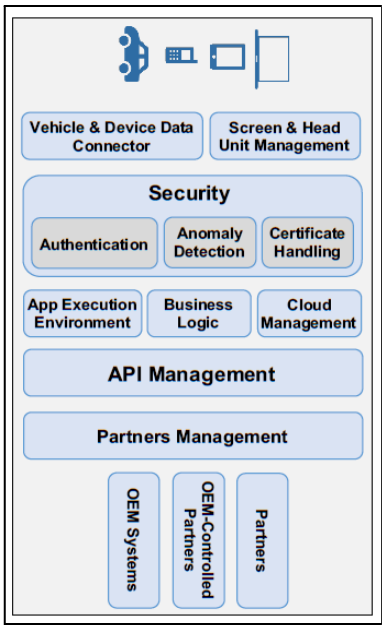

Fig. 5. Ericsson Connected Vehicle Cloud Overview [5]

3) Layer-based Solution : The National Highway Traffic Safety Administration (NHTSA) has launched a research programme that takes a layered approach to cyber security for motor vehicles. According to NHTSA, this layered approach reduces the probability of attacks and mitigates the potential ramifications of a successful one.

The programme focuses on four main areas at the vehicle level:

- preventive measures and techniques such as isolation of safety critical subsystems to mitigate the effects of a successful attack;
- real-time intrusion detection measures that include a continuous monitoring of potential intrusions in the system;
- Real-time response methods that aim to preserve the driver’s ability to control the vehicle when the attack is successful; and
- Assessment of solutions where information about successful hacks from partners can be collected and analysed to assess the effectiveness of the current protection mechanisms.

4) AI Security Solutions

- Security assessments of AI components are performed regularly throughout their lifecycle. This systematic validation of AI models and data is essential to ensure that the vehicle always behaves correctly when faced with unexpected situations or malicious attacks.
- Continuous risk assessment processes supported by threat intelligence could enable the identification of potential AI risks and emerging threats related to the uptake of AI in autonomous driving. Proper AI security policies and an AI security culture should govern the entire supply chain for automotive.
- The automotive industry should embrace a security by design approach for the development and deployment of AI functionalities, where cybersecurity becomes the central element of digital design from the beginning.

VI. Conclusion

Since the first solid-state circuit boards were installed into cars, the inevitable union/integration of automobiles and information technology was set into motion. From those early days of basic On-Board Diagnostics (OBD) systems, we have gradually evolved to the cusp of widespread autonomous vehicle adoption globally. Nevertheless, safety and security concerns are paramount. Research shows that AV-related safety risks may arise from the less cautious behaviour of vehicle occupants and road users, system errors, and the lack of regulation of crash algorithms that determine life or death situations during inevitable accidents.These concerns must be properly addressed and managed for autonomous vehicle adoption to be successful.

In short, the three key areas for enabling safe and secure autonomous vehicle adoption are:

- Fundamental – Basic cybersecurity techniques foundational to a cybersecurity program.
- Repeatable – Use of standards and frameworks to support consistent and repeatable deployments.

- Innovative – Develop new technologies and methodologies to address security needs in a dynamic AV ecosystem.

In the near future, we expect the market of autonomous vehicles will continue to grow. The cheaper computational power and the faster development of machine learning techniques will promote autonomous driving to be a more reliable technology that will finally improve the well-being of the society.

Acknowledgment

We are grateful for the support provided by the Mukesh Patel School of Technology Management and Engineering, NMIMS. We thank Professor Abhishek Vichare, MPSTME for his reviews, helpful comments and encouragement.

References

[1] Araz Taeihagh, “Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks”, December 2017.

[2] Jeremy Straub, John McMillan; Brett Yaniero, Mitchell Schumacher, Kelvin Boatey, Jordan Hartman, “CyberSecurity considerations for an interconnected self-driving car system of systems”, June 2017.

[3] Shusuke Morimoto, Fang Wang, Ranchao Zhang, Jinghui Zhu, “Cybersecurity in Autonomous Vehicles”, May 2017.

[4] Simon Parkinson, Paul Ward, Kyle Wilson, Jonathan Miller, “Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges”, March 2017.

[5] Mahmoud Hashem Eiza, Qiang Ni, “Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity”, April 2017.

[6] Qiyi He; Xiaolin Meng; Rong Qu, “Survey on cyber security of CAV”, October 2017.

[7] Abdullahi Chowdhury, Gour C. Karmakar, Joarder Kamruzzaman, Alireza Jolfaei, “Attacks on Self-Driving Cars and Their Countermeasures: A Survey”, January 2020.