NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 8, Aug. -2021

CYBER SECURITY IN AUTONOMOUS VEHICLE NETWORKS

Maheswari Kota
GITAM University, Vizag, India.

ABSTRACT

In today's world of a rapid increase in the autonomous vehicle, with the features like AEB which uses radar, cameras, and lidar technology to assess the road ahead and work out potential collisions. These technologies work together to map the vehicle's position and its proximity to everything around it. Due to this, there is a high demand for these vehicles, since they provide a lot of benefits to the people using them. But, usage of these highly equipped or automated vehicles(cars), there are many chances of getting attacked.

In this exposition, we will see the threats towards autonomous vehicles through various fields and their resolution techniques or algorithms to avoid data breaches or any other incident to the person using them.

Keywords: AEB (Autonomous Emergency Braking)

INTRODUCTION

There are various levels of autonomous vehicles depending upon the degree of autonomy- for the lower degree of autonomy driver has more power and functionality for managing, on coming to the fully automated vehicle like Tesla are expected to have full control over the functions.

In this automation, the information is gathered by the on-board sensors without any communication. Moreover, these automated vehicles can communicate with each other and can share information about the environment. Communication is not limited to communication between cars (vehicle-to-vehicle (V2V)), nor communication between the vehicles and the infrastructure (vehicle-to-infrastructure (V2I)) (Jawhar et al., 2013). A cyber-attack on automated vehicles (AVs) starts with control technology tools embedded in the system like electrical window controls. An attacker can modify the code during the design and implementation. And the code is targeted by the attacker so he can destroy the information or corrupt the performance. Upon successful capture of door locking messages, this virus was able to remotely lock a vehicle's door. A cyber attacker can configure the settings, modify code, and implant viruses and malware (Uma and Padmavathi, 2013; Petit et al., 2014).

Some cyberattacks involve the use of malware like computer viruses, worms, Trojan horses, spy-ware. Cybersecurity aims to prevent unauthorized access to digital devices like PCs, laptops, and smartphones, as well as to wireless communication protocols and wireless routers. Some of the private browsers have protocols that have default settings that can get affected by malicious attacks just by accepting the cookies leading to communication between them.

The rest of this paper is organized as sections: (a) presenting different cyberattack scenarios involving AV networks, (b) describes a system model for data and cybersecurity AV networks, (c) explains the implementation of secure V2V communications and (d) concludes the paper.

METHODS

Cyber-attack scenarios on AVs:

(a) On sensor networks- Most of the AVs sensors can be accessed internally, ensure to check the vehicle keeps on running. Only a few types of applications are involved in perceiving the environment. Sensory perception is the process of converting the physical environment into digital signals for further processing, such as measuring forces or distances (Raiyn, 2013a). Sensor networks are targets of interest to attackers. The work of (Knoll, 2014) examines external attacks, but their focus is
limited to gaining entrance via exploitable input and output channels, such as Bluetooth, keyless entry systems, and wireless maintenance ports.

(b) On GPS- Cyber-attacks can use smart phone apps to track online activities and users plans. In global positioning system (GPS) spoofing an attacker modifies code to report incorrect GPS locations data which misleads drivers.

This section will describe currently available global navigation satellite systems (GNSS) (ToledoMoreo,

2010). The main task of a GNSS is to provide localization and time synchronization services. Several systems of this type are available, the most famous of this type the global positioning system (GPS) (Zandbergen, 2009). There are several methods for augmenting GNSS data, to get a better estimate of location. Three of these methods are satellite-based augmentation systems (SBASs), assisted-GPS and differential-GPS. SBASs are commonly used in airplanes, for critical phases such as the landing phase.

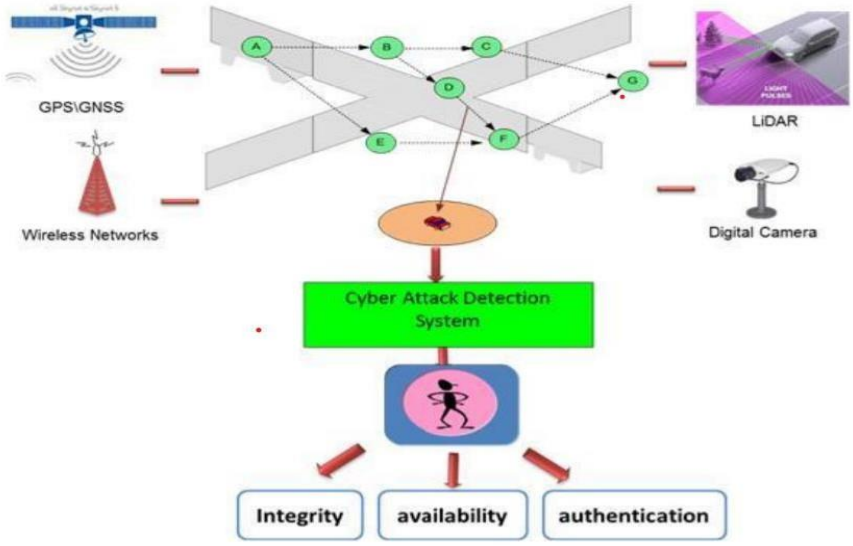

Figure 1. Information cyber security

They consist of a few satellites and many ground stations.

(d) **Communication in AV networks-** In some types of autonomous automation, information about the environment is gathered entirely from on-board sensors, without any active communication with other vehicles or the infrastructure. Furthermore, AVs can communicate with each other and share information about the environment. Communication is not limited to communication between (V2V), nor to that between cars and the infrastructure (V2I). Autonomous vehicles used vehicle –to-vehicle communication for lane changes, intersection crossing, and cooperative merging on highways.

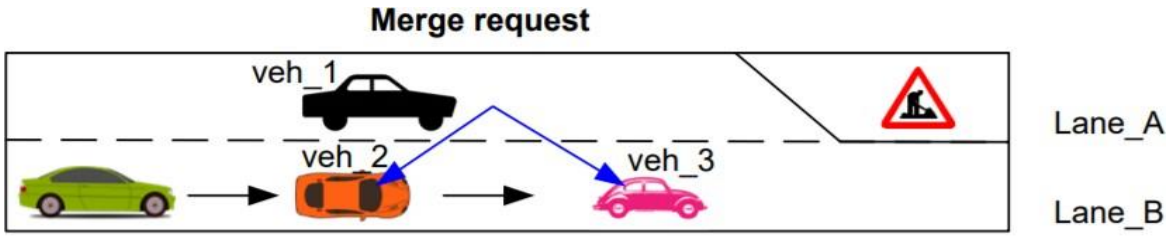

Figure 3. Road lane change

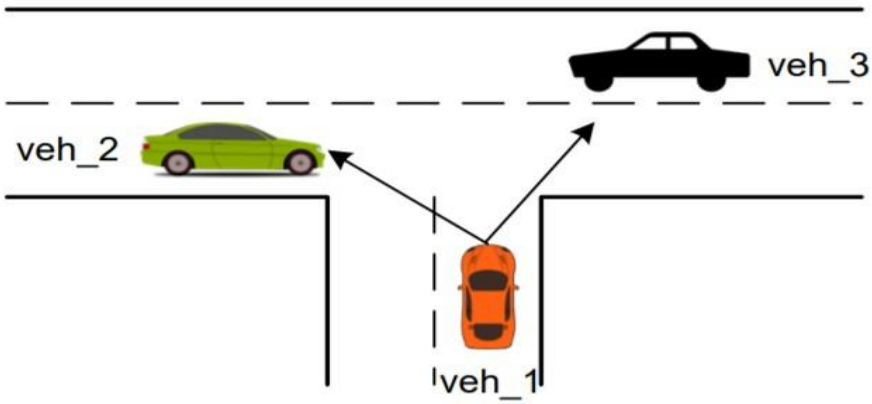

Figure 4. Intersection crossing

RESULTS

Algorithm

I. An AV-agent is created, by operating the VA.
II. The AV agent sends a notification to central control unit (CCU).
III. The CCU builds an augmented trip for the AV.
IV. Data transmission between the CCU and the AV is secured by a biometric identification system.
V. The biometric data (DNA of the AV) is presented in a sequence of machine language. [001 ↔ 1 head, 111 ↔ 2, 001 ↔ 3, ..., $N \leftrightarrow n$ tail] The first part (head) of the biometric sequence is allocated to the CCU. The last part (tail) of the sequence is allocated to the AV.
VI. For data transmission only the body of the biometric sequence is sent randomly.
VII. The biometric identification system orders the sequence using a key.

CONCLUSION

The good news is that carmakers are working hard to address the growing threat against connected car security. They are teaming up with security experts and investing in new technology. Last year, for example, a consortium of car manufacturers invested US$30 million in-car cybersecurity start-up Upstream. Motorists must take responsibility too. After all, no end of technical protection will help if hackers can just use social engineering to dupe the connected car driver.

In 2016, security firm Promon proved this when it created a free Wi-Fi hotspot and asked drivers to install an app on their phones. The app was infected with malware and gave hackers the ability to take control of the car.

REFERNCES

1) Amar, N., (2006) LIDAR technology overview. ETI–US Geological Survey, Retrieved August 17.
2) Broggi, A. et al. (2013) Extensive Tests of Autonomous Driving Technologies. IEEE Transactions on Intelligent Transportation Systems, 14.3. 1403–1415.
3) Chirchi, V.R.E et al. (2011) Iris Biometric Recognition for Person Identification in Security Systems, International Journal of Computer Application, 24, 9. 0975- 8887.
4) Jawhar, I, Mohamed, N. and Usmani, H. (2013) An Overview of Inter-Vehicular Communication Systems, Protocols and Middleware. Journal of Networks, 8, 12. 2749–2761.
5) Kastner, R. and Michalke, T. (2010) Attention-based traffic sign recognition with an array of weak classifiers. (IV), 2010 IEEE (June 2010). 333–339.
6) Kerns, A.J., Wesson, K.D. and Humphreys T.E. (2014) A blueprint for civil GPS navigation message authentication. Position, Location and Navigation Symposium - PLANS 2014 (May 2014), 262–269.