Grenze International Journal of Engineering and Technology, June Issue

Security Challenges in Controller Area Network (CAN) in Smart Vehicles

Nishant Biradar[1], Yashodhan Mohite[2], Niket Pandey[3], Shreyas Dugad[4], Shubham Khandajkar[5], Vaishali Mishra[6] and Madhuri Karnik[7]
[1-7]Department Of Computer Engineering Vishwakarma Institute of Information Technology,Pune
Email: nishant.21810886@viit.ac.in,yashodhan.21810924@viit.ac.in,niket.21810825@viit.ac.in,
shreyas.21810916@viit.ac.in,shubham.21810923@viit.ac.in,vaishali.mishra@viit.ac.in,madhuri.karnik@viit.ac.in

***Abstract*—In the past couple of years, the automotive industry has seen some big changes. With all the devices that we know and use in our day to day lives, getting smarter and smarter, it shall be no surprise that the automotive industry is also trying to achieve the same. Although this change has brought connectivity, comfort and functionality, it has also created new ways and opportunities to get attacked. These security challenges should be well studied as this industry is constantly getting updated. The in-vehicle architecture of these vehicles neglects security of the vehicle. We see that the CAN Bus, used to transfer information from one ECU to another, has many vulnerabilities that may turn out to be fatal for the consumer and the manufacturer. In this paper we will discuss the working of the CAN bus, possible vulnerabilities of the CAN bus and different kinds of attacks and ways to mitigate them. This paper will try to draft possible solutions to make the CAN Communication protocol more secure and safe.**

***Index Terms*— CAN,ECU,IDS, CAN HG.**

I. INTRODUCTION

The vehicle industry is going through a major reform. Combustion Engines are expected to decline and electric vehicles are to take their place. The increasing environmental concerns and lack of fossil fuel has made it clear that we have to move on and make electric vehicles the future of the automobile industry. Vehicles these days are not only electro-mechanical instruments but are slaves to the software that dictates each and every action that it performs. With the world becoming smart where all the devices are connected and work together to make things much more efficient and comfortable, vehicles are also following the same path. With 5G networks to soon be incorporated, the in-vehicle, vehicle to vehicle and vehicle-internet communications are expected to happen with no delay. This will boost our developments in the field of smart vehicles where concepts of smart traffic management, speed control automation, emergency assessment and self-driving cars will be implemented. With seamless communication of vehicles with the surrounding, real time decisions can be taken. Its impact will be huge where we can control and manipulate the system in such a way that we can ensure road safety. The large amount of data that will be generated, can be analyzed and insights can be drawn which may lead to fruitful conclusions.

To accomplish this, a mesh of electronic computational systems and sensors are used. These sensors are controlled by embedded electronic control units(ECUs). ECUs control the entire car. According to [1,2], a modern automobile is fitted with more than a hundred ECUs, and this number is envisaged to increase in the

Grenze ID: 01.GIJET.8.2.511_2

future. Different types of ECUs used in modern cars are the door control unit, electric control unit, electric power starting unit, braking system(ADS/EBD), stability control unit etc. These ECUs work in coordination by communicating via serial buses and gateways. Controller Area Network(CAN) bus is prominently used in modern cars to connect the ESUs. It provides a pathway to transfer information from one ECU to another. Being the most common in-vehicle communication protocol for vehicle applications, CAN offers advantages such as cost-effective wiring, immunity to electrical interference, self-diagnosing, and error correction.

However, despite these benefits we observe that it is not designed keeping security in mind. CAN is vulnerable in a very straightforward manner as it has no authentication or encryption. In CAN protocol, masquerade attacks can be performed very easily. CAN uses a broadcast mechanism where all the instructions are transferred to every ECU. The ECUs read the information and decide whether it is meant for it and act accordingly. CAN also does not require any permission to add any new ECU to the bus. This loophole can be used by the attacker to manipulate an existing ECU or add a new ECU and use it to control other ECUs over the CAN bus. This can be fatal to the consumer and also the manufacturer. As the broadcasted data is not encrypted, it may lead to invasion of privacy where driver's personal details, bank details and transactions can be acquired. Up until now, only in-vehicle communications were prominent. But as vehicles are now being connected to the internet and other vehicles and devices, we must ensure that the communication protocols also must be reconsidered. Using the same old CAN bus without any upgradation can be fatal. Hackers may manipulate vehicles and cybercrimes may escalate. For instance, the safety of the driver and passengers can be jeopardized by the attack on airbag [3] or ABS systems. Cybersecurity of vehicles must be taken seriously and proper measures must be taken to ensure the safety of the vehicle and the information it receives and transmits.

According to the 2019 industry survey[4], safety and security are the highest short-term and mid-term challenges for the automotive industry. Therefore, extensive studies have been carried out to find possible solutions[5,6] to the vulnerabilities of CAN. Some of these studies have performed successful experimental attacks on passenger cars [9–14] and heavy-duty vehicles [15,16].Mukherjee et al. [16] implemented DoS attacks on the SAE J1939 standard [19], which is used in heavy-duty commercial vehicles. They performed three separate DoS attacks: (i) sending too many request messages for a supported Parameter Group Number (PGN) to overload the recipient ECU, (ii) sending manipulated false request to send (RTS) and causing overflow at the recipient buffer, and (iii) keeping the connections open via Clear to Send (CTS) messages and occupying the whole network. This work was one of the first studies to exploit the SAE J1939 specification. Murvay and Groza [15] implemented impersonation and DoS attacks on SAE J1939.At the same time, researchers have also proposed preventative methods for such known attacks. These include network segmentation, encryption, authentication, and intrusion detection systems (IDSs).

In this paper we discuss the following:

- Security challenges faced in modern vehicles including physical and remote access attacks.
- Possible future attacks on the CAN by accessing the current threats.
- Analysis of current CAN security issues and ways to mitigate them.

II. Overview of Controller Area Network(CAN)

CAN bus was developed by Robert Bosch in the early 1980s. CAN bus works on broadcast communication protocol. Every ECU on the network is connected to the CAN bus. Whatever data transmitted on the CAN bus is received by each ECU present on the bus. The ECU decides whether the message was meant for. If the message corresponds to the particular ECU, the data is read and following actions are performed. If the signal is not meant for the ECU the signal is ignored or transmitted further.

Latest CAN bus is CAN FD. CAN FD interface can provide upto 5Mbps[18] compared to the traditional CAN which provides 1Mbps[17]. Both CAN and CAN FD are standardized under ISO 11898-1:2015.

CAN has a two wired bus architecture. The protocol uses differential wiring, CAN_H and CAN_l which helps retain signals against noise and electrical interference.

CAN protocol follows a message based communication provided via frames. CAN message is shown in Figure 2.

CAN message frame has the following components:

- *SOF(Start of frame)*-Marks the beginning of data and remote frames.
- *Arbitration field*-Includes the message ID and RTR (Remote Transmission Request) bit, which distinguishes data and remote frames.
- *Control Field* – Used to determine data size and message ID length
- *Data Field* – The actual data (Applies only to a data frame, not a remote frame)

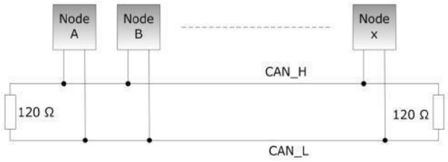

Figure 1:Architecture Of CAN bus

Figure 2:CAN message architecture

- *CRC Field* – Checksum
- *EOF (End of Frame)* – Marks the end of data and remote frames

CAN protocol provides robust communication. When two or more ECUs start the transmission at the same time, then the highest priority ECU transmission continues without interruption. CAN bus provides two error checking mechanisms-*bit level* and *message level.* Bit level error arises when there is a difference in the bit transmitted by the ECU and the bit on the bus. Message based errors include frame check over ACK,CRC and EOF fields. If the message is received successfully then the ACK bit is overwritten with the dominant bit. Otherwise the ACK bit remains recessive which signifies error in transmission. The CRC field send should match with the CRC calculated by the ECU. If it does not match, error is flagged.

III. Vulnerability in CAN Bus Protocol

CAN protocol is extensively used in vehicles. It is essential that we must check and assess the security problems of the CAN protocol. We will consider confidentiality, integrity and availability to assess the vulnerabilities of the CAN bus.

Confidentiality means to safeguard the data and provide its access to only authorized persons.

CAN protocol does not have any inherent cryptography or authentication methods to ensure confidentiality. This allows invasion of privacy and cybercriminals to violate the vehicle and data.

Integrity means to preserve the accuracy and validity of the data. CAN bus has CRC to ensure integrity against transmission errors. But when malicious data is injected to the CAN bus by third part nodes, integrity of the CAN bus fails.

Availability is readiness of the vehicle to execute instructions of the user. But the CAN bus follows priority based messaging, which executes higher priority messages before the lower priority messages. This may lead to the system unavailability if higher priority messages are already under action.

According to the above assessment we can say that CAN protocol needs upgradation in the security measurements against attacks.

IV. Attacks on CAN Bus

A. How to get on the CAN bus

To know about the attacks on the CAN bus we must first see how the CAN bus is accessed. One of the ways to access the CAN bus is to attach a CAN controller and transceiver.

Physical access of the CAN bus is required for this. OBD-II dongles on the CAN bus can be used to attach controllers where messages and injection attacks can be performed. Third party devices and hacking devices can be used to get data and inject malicious code to disable or disrupt the normal working of the vehicles.

Another way to get access to the CAN bus is by hijacking a system already connected to the CAN bus. This allows the CAN bus vulnerability to be exploited. Malwares may be injected and executed which may attack the infotainment system, braking system etc. which may be fatal for the consumer. Private data may be exploited and used for malpractices

Remote access to the CAN bus is also very much likely as the vehicles have Bluetooth connectivity, Wifi, Cellular networks, GPS and Radio channels. The hacker does not require direct access to the vehicle. He can get connected to the vehicle using wireless transmission and use malware and viruses to disrupt the device.

B. Types of Attacks

- Frame attacks using CAN controller-CAN frames are sent to the bus in compliance with the CAN protocol. For example, an OBD-II dongle is connected via Bluetooth to the laptop and using Socket CAN API different ECUs can be hacked.
- Protocol attacks are made via CANTX pins. Specialized attacks are performed to exploit features of the CAN protocol. It does not need to follow CAN rules and any pattern of data can be sent on the bus.
- Frame Spoofing Attack-This is the most commonly performed attack on the CAN bus. It is an authentication attack. A CAN controller is used. Receivers on the CAN frame are made to legitimate the authentication of the unauthorized user.
- Bus Flood Attack-Legitimate frames are sent on the CAN bus but are sent more often than allowed. The CAN bus is flooded with such frames. This results in lower priority frames exceeding their latencies which causes lost frames, timeouts and disruption. This attack is denial of service attack.
- Reconfigure I/O ports-In this attack we get the malware inside the ECU. Once the malware is in, we bypass the on-chip CAN controller and turn CANTX into a GPIO pin. And then we use the bit banging software to drive the pin. Crafted signals of a particular pattern are sent directly out of the CAN TX pin. So the CAN controller has complete control of the software and accesses all the functionalities of the vehicle.
- Bus-off Attack-In this attack, an ECU is targeted. We wait for the frames coming out of the particular ECU using its ID. We wait until the frame comes past and pull the CANTX pin to 0 and destroy that frame. We wait for the CAN recovery process and once the frame comes again, we destroy it. This repeatedly occurs until the error handling forces turn the bus off. Basically, we cut off an ECU from the CAN bus. This is a denial of service attack where we disrupt the service besides spoofing. For example, braking systems and GPS signals could be disrupted which could be fatal for the user.
- Double Receive Attack-In this attack the frame is forced to be received twice by exploiting the corner case in CAN protocol. It is a straightforward attack where the CANTX bit is set to 0 for the last bit of EOF field. This results in resending of the frame. This is a denial of service attack that causes events to be acted on twice. For example, if the button is pressed to lock the door the frame is sent twice which in turn unlocks the door.
- Freeze Doom Loop Attack-In this we freeze the bus for an arbitrary time. This causes frame latencies to increase. Overload of frames results in timeouts and lost frames. This is a denial of service attack.
- Janus Attack-It is a spoofing attack where different receivers see different payloads of the same frame. So different ECUs will see different payloads of the same frame. This can be used to spoof through the intrusion detection system and malwares can exploit the ECUs.

V. Protecting CAN

The defense of the CAN bus is of utmost importance. CAN bus controls the workflow of the entire vehicle. All the moving parts of the vehicle are controlled through CAN bus. Perimeter defenses that are being used like adding IP firewalls, protecting cloud APIs etc. are necessary but not sufficient as it is going to get worse as the complexity rises dramatically as more and more automation is added to the vehicle. CAN is so important that it needs its own defenses as it carries commands to control the actuators. It is unrealistic to rely on applications defending themselves as CAN attacks can be combined in devious ways where the system can be abused. So we need special methods that don't rely on applications defending themselves. We will discuss the mitigation techniques that can help us protect the vehicles from attacks.

VI. Mitigating Attacks

There are four main mitigation techniques:

A. IDS

Intrusion detection systems are software that use a CAN controller to monitor all the traffic on the bus. It looks for anomalies that occur on the bus. For example, frames arriving more often than expected can be a spoofing attack. But observing the system for some time won't make any difference. We need a very good IDS model to monitor the frame rates and understand the action according to the traffic. As the frame rates will be variable for an on road vehicle, IDS must access and know what frequency of frame rate is not an attack. Fortunately, smart vehicles are not dynamic systems, but are embedded systems with a specific design. DBC files are used to

describe traffic and calculate specific latencies to build a good IDS model. However some attacks are invisible to the IDS. For example, Freeze Doom Attack and Janus attack fool the IDS. IDS also plays an important role in post-incident forensics. The data retrieved from the IDS can be used to determine whether the incident was caused by a hack or modification to the system or a spurious error. Insurance companies benefit from it a lot to assess how the incident took place. Manufacturers also keep track to update and develop new systems.
An IDPS(Intrusion Detection and Prevention System) model that uses a per-frame timing model must be considered. A burst of frames with an overall period and a vulnerability in the period(burst-period-jitter) can be used to feed the IDPS the rate at which frames must be received. These parameters can then feed into the CAN timing model. Then we can calculate the worst frame latencies of all the frames on the bus. The IDPS can enforce that timing model and then any ECU that steps out of that is a violation of the model. Then the IDPS can send commands to shut off the ECU. This system can also help in cutting off the failed ECUs on the CAN bus. It can act as an indicator for failed ECUs on the system and warnings and instructions may be given to reconfigure them.

B. Security Gateways

These gateways are used to filter traffic between untrusted and trusted buses with drop/forward rules. Eg-OBD-II port goes on its own bus and only frames with 11 bit ID 0xDF are forwarded and only frames with 11 bit ID 0xEF are sent back. So only certain IDs are passed and all other IDs are blocked. If the software contains buffer flow vulnerabilities then the gateway itself could be hijacked and all the protections are lost. So, proper coding standards must be followed while developing gateways. At the very least we must use MISRA C and proper analysis tools. The rules must be reprogrammable to allow updates post manufacture. The reprogramming mechanism must be secure for the whole gateway or the hackers may reprogram the gateway to change IDs.

C. Encryption

Encryption provides message secrecy and authenticity. This helps in preserving the personal data that flows through the CAN bus. Authenticity is a very important property. Encryption attaches message authentication code(MAC) to every message. CMAC algorithm using AES is generally recommended as it provides comparatively more authenticity. Generally Public key encryption is not used because of the time taken. CAN frames are 8 bytes. MAC minimum size is 64 bits which is entire CAN frames worth. One solution is to use a faster networking protocol. CPU time for a small crypto operation is huge. So even small devices need hardware acceleration. Modules for the HIS SHE standard for HSMs are becoming more and more common on microcontrollers. HIS SHE is a very good encryption standard as it not only handles acceleration AES encryption operations and message authentication code calculations, it also stores keys securely so they can't be read by the host. It also has protocols where while communicating with the key distribution system we can put the key into the system without the CPU knowing what that key is. Key security is very crucial in using encryption. Keys must be distributed and all the ECUs must have the keys stored securely. Otherwise, malware injection may read out the keys. One of the downsides of encryption is that it cannot mitigate denial of service attacks(DOS).

D. Hardware to Provide CAN Security

Basically, to ensure that CAN is safe we are majorly trying to resolve two things. Firstly, any ECU on the device must know that the frame is coming from the source of the implied ID(authentication). Secondly, system integrators must know that frames will always get through in a bounded time(DOS prevention). Although the above mentioned techniques provide security in one form or the other, they have some shortcomings which do not provide assured security. So, we try to take a completely different approach to use a combination of hardware and software to ensure CAN safety.

E. NXP's secure CAN transceiver

It contains a table of CAN IDs that the host can send. Any ID that the host sends and is not on the table is considered to be a spoof. If any ID that is on the list but not sent by the host is encountered, then it is considered to be a security breach(frame spoofing).This prevents frame spoofing and is used to detect security errors. The CAN error mechanism destroys the frame before receiving it .Along with this it also provides an anti-DOS(denial of service) feature. The hardware contains the leaky bucket algorithm that measures the rate limit of frames coming out. So, attacks like bus flow attacks are prevented. We can say that this solves our authentication problem and also prevents one kind of DOS attack performed on the CAN bus. With all these benefits, we must also look out for issues that may occur while using the transceiver so that we can ensure that we make the

hardware as safe as possible. The IDs must be programmable. They must be programmable over the air(OTA) as we are talking about smart vehicles. There has to be a secure method that must be used to program the IDs otherwise malware can just re-write the list. Also the Leaky bucket algorithm provides added security but is pretty weak against other DOS attacks. CAN protocol attacks face no resistance by the hardware. So, different techniques must be combined to ensure security.

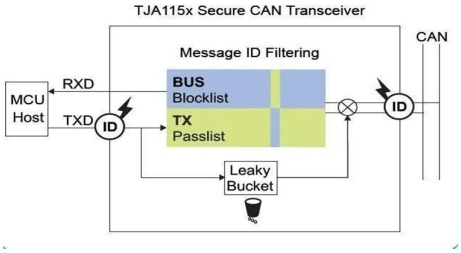

Figure 3:NXP's secure CAN transceiver

F. CAN HG Security

It is a way to augment a standard CAN for high performance with security features to guard the bus. Out-of-band data is put inside the CAN frame and the data is invisible to the CAN controllers. It is fully compatible with CAN. We can use existing CAN hardware and wiring topology. We can mix CAN and CAN-HG on the same bus. Out-of-band data encodes a hardware source address of the CAN frame. The central IDS/IPS(IDPS) extracts the hardware source address. It checks the CAN ID to see if the expected source address matches. If not then the frame is a spoofed frame. IDPS generates a CAN error so that frame is never received by the CAN controller. When the CAN frame is received we know that it is a legitimate frame.

Destroying the spoof frame is only the first layer of protection. After destroying it the transmitter will simply transmit the frame again. The IDPS will again destroy it and this will go on till 32 frames before the sender goes bus off. So, without DOS the spoof attack becomes a DOS attack. CAN HG guardian software also provides a DOS protection. CAN HG guardian hardware accepts IDPS commands in the can frame and sends it with ID 0(highest priority).IDPS can command that the host is cut off from the CANTX pin on the transceiver. Cutting the host to CANTX pin prevents further attacks. Host can be admitted again later.

VII. Discussion on CAN Security Research

Cyber Security of automotive vehicles is getting more and more attention. Standardizations are being proposed to tackle cybersecurity problems. Cybersecurity guidebook for Cyber-physical vehicle systems and the fundamental principles of automotive cybersecurity specification (PAS 1885:2018) were published by SAE in 2016 and British Standards Institute in 2018 consecutively[20,21]. ISO/SAE 21434[22] published recently in August,2021 states the cybersecurity standards in each level of production in road vehicles.The CAN protocol has also gained attention from the industry to its vulnerabilities, and companies are now manufacturing high-end secure ECUs. The SHE[23] specification becomes the open standard and many companies are using it to develop ECUs[25].Some ECUs have inbuilt IDPS systems to prevent attacks.

Although there have been many steps to protect CAN, there are many loopholes that must be fixed.There must be more research on modeling CAN bus attacks and creating databases which must be open source[26,27,28,37,38,39]. This will help researchers and proper benchmarks may be set to work on shared datasheets which will give a reference point for further developments.

VIII. Conclusion

Cyber attacks are getting more complex day by day.Modern CAN protocol facilitating the ECUs is not geared up to prevent and protect the vehicle from such attacks.As more and more automation will get involved in vehicle manufacturing the risk of breaches will escalate.Existing features are not fit to address them.This can result in jeopardizing data privacy and safety of the vehicle consumer and manufacturer. It can go to an extent that criminal activities may be a concern.This will blemish the manufacturers reputation and downgrade the vehicle reliability.

Current attacks are majorly through physical access of the vehicle. However, with growing connectivity of the vehicle where vehicle-to-vehicle communication and vehicle-internet communications will be prominent, we can

expect remote access attacks to also disrupt the vehicles. It is high time that we invest and seriously consider the cybersecurity of vehicles.

In this paper we have discussed the shortcomings of the CAN bus.There are many vulnerabilities of the CAN protocol.We have looked into kind of attacks on the CAN bus. Frame and protocol attacks,authentication and denial of service attacks are discussed.With the current architecture of the CAN bus we can clearly say that it is not upto the standard and breaches and attacks can easily be performed.

Four major countermeasures are discussed: IDS/IDPS, security gateways,encryption and hardware protection.Analysis has stated that facilitated IDPS are the most promising option for strengthening the security.We presume that future vehicles will have IDS solutions not only to secure the vehicle, but to also provide data to the manufacturer to tackle cyberattacks. All these methods will provide extended security solutions, but attacks will keep coming up and we must ensure that more and more filters are added so that it gets more complicated for the attacker to breach the vehicle.

REFERENCES

[1] Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S. et al. Experimental security analysis of a modern automobile. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 447–462.

[2] Palanca, A.; Evenchick, E.; Maggi, F.; Zanero, S. A stealth, selective, link-layer denial-of-service attack against automotive networks. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Bonn, Germany, 6–7 July 2017; Volume 10327, pp. 185–206.

[3] Hoppe, T.; Kiltz, S.; Dittmann, J. Security threats to automotive CAN networksPractical examples and selected short-term countermeasures. Reliab. Eng. Syst. Saf. 2011, 96, 11–25

[4] Tencent Keen Security Lab. Experimental Security Assessment of BMW Cars: A Summary Report; Peerlyst Inc: Shenzhen, China, 2018.

[5] Murvay, P.S.; Groza, B. Security shortcomings and countermeasures for the SAE J1939 commercial vehicle bus protocol. IEEE Trans. Veh. Technol. 2018, 67, 4325–4339.

[6] Mukherjee, S.; Shirazi, H.; Ray, I.; Daily, J.; Gamble, R. Practical DoS Attacks on Embedded Networks in Commercial Vehicles; Springer International Publishing: Cham, Switzerland, 2016; Volume 10063.

[7] Bosch, R. CAN Specification Version 2.0; CAN: Stuttgart, Germany; 1991.

[8] CSS Electronics. CAN Bus Explained; CSS Electronics: Aarhus, DK, Jutland, 2019.

[9] SAE International. J1939: Serial control and communications heavy duty vehicle network. 2018. Available online: https://www.sae.org/standards/content/j 1939_201808/ (accessed on 29 December 2019).

[10] Vehicle Cybersecurity Systems Engineering Committee. J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems;Technical Report; SAE International: Washington, DC, USA, 2016.

[11] BSI. PAS 1885:2018 The Fundamental Principles of Automotive Cyber Security - Specification; BSI Standards Limited: London, UK, 2018.

[12] Macher, Georg & Schmittner, Christoph & Veledar, Omar & Brenner, Eugen. (2020). ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell. 10.1007/978-3-030-55583-2_9.

[13] Mundhenk, P. Security for Automotive Electrical/electronic (E/E) Architectures; Cuvillier Verlag: Göttingen, Germany, 2017.

[14] Soja, R. Automotive Security: From Standards to Implementation; Automotive Microcontrollers and Processors, NXP: Eindhoven, The Netherlands, 2014.

[15] Fröschle, S.; Stühring, A. Analyzing the capabilities of the CAN Attacker. Eur. Symp. Res. Comput. Secur. 2017, 10492 LNCS, 464–482.

[16] Ring, M.; Dürrwang, J.; Sommer, F.; Kriesten, R. Survey on vehicular attacks - Building a vulnerability database. In Proceedings of the 2015 IEEE International Conference on Vehicular Electronics and Safety, ICVES 2015, Yokohama, Japan, 5–7 November 2015; pp. 208–212.

[17] Huang, T.; Zhou, J.; Bytes, A. ATG: An Attack Traffic Generation Tool for security Testing of in-Vehicle CAN Bus. In proceeding of the ACM International Conference Proceeding Series 2018, Hamburg, Germany, 27–30 August 2018; pp. 1–6.

[18] Sensors 2020, 20, 2364 16 of 16 68. Li, F.; Wang, L.; Wu, Y. Research on CAN network Security Aspects and Intrusion Detection Design. 2017. Available online: https://saemobilus.sae.org/content/2017-01-2007/ (accessed on 21 April 2020).

[19] Muter, M.; Asaj, N. Entropy-based anomaly detection for in-vehicle networks. In Proceedings of the 2011 IEEE Intell. Veh. Symp. (IV),Baden-Baden, Germany, 5–9 June 2011; pp. 1110–1115.

[20] Taylor, A.; Leblanc, S.; Japkowicz, N. Anomaly detection in automobile control network data with long short-term memory networks. In Proceedings of the 3rd IEEE International Conference on Data Science and Advanced Analytics, DSAA 2016, Montreal, QC, Canada, 17–19 October 2016; pp. 130–139.

[21] https://www.youtube.com/watch?v=37gI RSLxbYg CAN Bus: Attacks And Mitigations

[22] Scarfone, K.; Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS); Technical Report; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2012.
[23] Wang, Q.; Sawhney, S. VeCure: A practical security framework to protect the CAN bus of vehicles. In Proceedings of the 2014 International Conference on the Internet of Things, IOT 2014, Cambridge, MA, USA, 6–8 October 2014; pp. 13–18.
[24] iddiqui, A.S.; Plusquellic, Y.G.J.; Saqib,F. Secure communication over CANBus. In Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, USA, 6–9 August 2017; pp. 1264–1267.
[25] CANcrypt - Home. Available online: https://www.cancrypt.eu/index.php/en/ (accessed on 29 May 2018).
[26] Yoshida, J. CAN Bus Can Be Encrypted, Says Trillium. EEtimes, 2015. Available online: https://www.eetimes.com/document.asp?doc_id=1328081&page_number=2 (accessed on 29 May 2019)
[27] Wankhede D.S. (2021) Analysis and Prediction of Soil Nutrients pH,N,P,K for Crop Using Machine Learning Classifier: A Review. In: Raj J.S. (eds) International Conference on Mobile Computing and Sustainable Informatics. ICMCSI 2020. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-49795-8_10
[28] K. Bhattacharjee et al., "Survey andGap Analysis of Word Sense Disambiguation Approaches on Unstructured Texts," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 323-327, doi: 10.1109/ICESC48915.2020.9155947.
[29] Mrs. Disha Sushant Wankhede, Dr. Selvarani Rangasamy,"REVIEW ON DEEP LEARNING APPROACH FOR BRAIN TUMOR GLIOMA ANALYSIS" Journal of Information Technology in Industry, VOL. 9 NO. 1 (2021) pp. 395 - 408 , DOI: https://doi.org/10.17762/itii.v9i1.144
[30] Vaishali Mishra, Disha Wankhede, “Intelligent Intrusion Detection Systems with Machine Learning Models for Detecting Cyber Threats in IoT Networks” ISSN: 2278-0181 IJERTV10IS1200