Journal of Engineering Technology and Applied Physics

Comprehensive Review of CAN Bus Security: Vulnerabilities, Cryptographic and IDS Approaches, and Countermeasures

Omer Fayyaz Khan*, Muhammad Mubashir and Jawaid Iqbal
Faculty of Computing, Riphah International University, Islamabad, Pakistan.
**Corresponding author*: omer.fayyaz@gmail.com, *ORCiD*: 0009-0005-3915-6816
https://doi.org/10.33093/jetap.2025.7.1.4
Manuscript Received: 10 January 2024, Accepted: 28 May 2024, Published: 15 March 2025

***Abstract* —Vehicle connectivity environments and advancements in vehicular technologies offer users both functional convenience and safety features, including remote diagnosis and assistance. To enable these capabilities, modern vehicles utilize various automotive serial protocols such as FlexRay, Local Interconnect Network (LIN), and the popular Controller Area Network (CAN). The CAN bus serves as a key protocol for in-vehicle networks (IVNs), facilitating the exchange of vehicle parameters among Electronic Control Units (ECUs). Despite its merits, the CAN bus has been found to have internal and external vulnerabilities. While numerous countermeasures are currently in place, the continuous advancements in vehicular interfaces have introduced new attack vectors, necessitating the development of additional safeguards. Existing research has primarily focused on CAN attacks initiated through direct interfaces, telematics and infotainment systems, and sensors. In this study, we aim to present an adversarial model for the CAN bus while also evaluating cryptographic and Intrusion Detection System (IDS) approaches considering real-time constraints and other relevant variables. Furthermore, we will classify available countermeasures into relevant categories and discuss their effectiveness. By conducting a comprehensive analysis of published works, our goal is to provide a comprehensive overview of CAN-related studies. This includes exploring potential mitigation techniques and identifying new research opportunities for IVNs. The synthesis of this information will offer valuable insights into the current state of CAN security, the challenges it faces, and the directions for future exploration. In summary, our study aims to address the vulnerabilities of the CAN bus, considering both existing and emerging attack vectors. By examining cryptographic and IDS approaches, we will assess their viability in real-time scenarios. Additionally, we will categorize and discuss the effectiveness of available countermeasures. Through this analysis, we strive to provide a holistic understanding of CAN-related research, paving the way for prospective mitigation techniques and identifying new horizons for IVNs.**

***Keywords*—CAN, Vulnerabilities, Cybersecurity, Cryptography, Authentication**

I. INTRODUCTION

In recent years, remarkable functions like the lane assist, anti-lock braking system, auto-parking and cruise control have been introduced to the automobile industry. To facilitate these and many other similar features ECUs have been included to control all the components in modern day vehicles. The CAN is a commonly used communication standard among ECUs. CANs connecting a vehicle to another vehicle are known as V2V and V2I when connecting to an external infrastructure. This increased connectivity has widened the cyberattack surface with vehicle-based systems being vulnerable to attacks not only from the inside but also from the outside. CAN bus Denial of Service (DoS) and bus injection are common attacks [1]. Once the attacker gains access to the vehicle's CAN, they can sway its operations by feeding malicious packets. The CAN protocol itself lacks sufficient security support, which limits the means for securing communication between different components within a vehicle. These limitations, studied by researchers, reveal how attackers manage to gain control of different vehicle parts like the lights, brakes, gears and steering functionality [2]. Also, they help reiterate the fact that vehicular vulnerabilities are existent and crucial issues that must be addressed on priority.

Network isolation and/or firewalls are a basic technique used to protect the CAN. As per the researcher's observation [1], 57 percent of the subject vehicles are in isolation from external environments.

Published by MMU PRESS. URL: https://journals.mmupress.com/index.php/jetap/index

The creation of controls such as does not make the CAN unexploitable. As a matter of fact, auto manufacturers have developed an open access port that bridges the internal and external networks to collect CAN data so as to facilitate telematics like remote diagnosis or to support future automotive research.

A. Paper Organization

As can be seen, Section I caters for the introduction. The rest of the paper takes the following course: Section II shares context information related to CAN. Section III states the outcomes of identified attacks. Section IV and V identify protective systems. The following Section VI discusses research directions in the security world. And Section VII presents our conclusion.

B. Contributions

Considering the drastic consequences of CAN related cyber-attacks, this research is not aimed at a better grasp of the analysis and obstacles involved but to act as a thorough guide for establishing a secure CAN by highlighting relevant attack surfaces and their corresponding protection techniques.
The contributions of this write-up are;

- Categorization of attack surfaces: By examining attack methods presented in [3, 4] attack surfaces can be classified into: physically accessible, wirelessly accessible requiring initial physical access, and wirelessly accessible without any physical access. Additionally, we define two types of adversaries: ones who can compromise an ECU and others who can only access the CAN.
- Classification of possible countermeasures: Defensive methods present in [5 - 7], may fall into the categories of preventive protection (anti-analysis & fuzzing), authentication, and after protection (recognition and patching). Also, this study dives into the merits as well as demerits associated with such protection methods and assess their effectiveness.

II. BACKGROUND OF CAN

Here, an insight into the CAN context shall be provided in order to earn a finer grip of CAN security.

A. CAN and ECU

A CAN network is composed of nodes that are connected through a differential bus. Each node in the network is managed by ECU. The ECU is responsible for controlling and coordinating the operations of the node it is associated with within the CAN network [8]. CAN dispenses dependable means for communicating in ECUs. Normally, new automotive bear various units that manage component systems like the brakes, engine and steering. Normally, an ECU is a combination of a CAN controller and transceiver along with a processor in Fig. 1 [9].

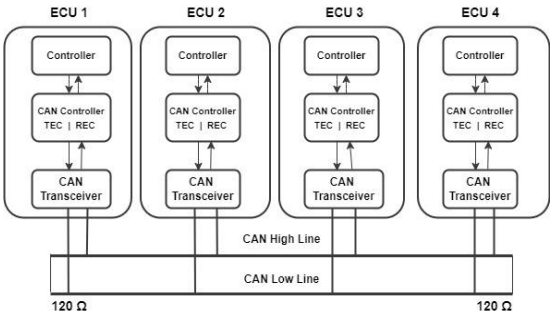


Fig. 1. Four components of ECUs.

These transceivers help the controller to connect with the CAN bus. They essentially bear two pins: a high line and low line pin. Making use of high and low line, it can return a dominant (zero) or recessive bit (one). In order to transfer a zero bit on the bus, a transceiver releases approximately 3.5 V on the high line and 1.5 V on the low line. And, in order to transfer a one bit, the transceiver releases approximately 2.5 V on both the high and low lines. Based on the differential voltage, receiving units read packets relayed on the bus in Fig. 2.

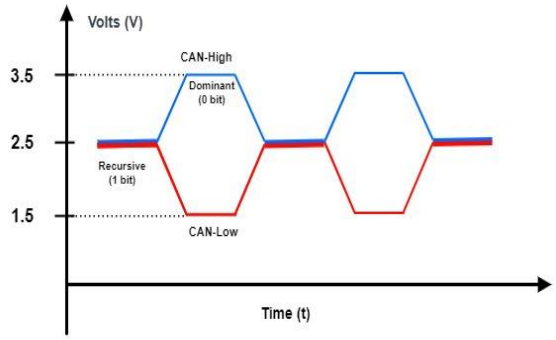
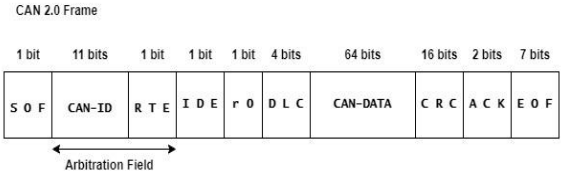


Fig. 2. Voltage level of the CAN physical layer.

B. CAN Frames and Arbitration

There are four types of frames: A data, remote, error and overload frame [10]. An 11-bit identifier is present in each data frame known as the CAN ID. Normally, most units intermittently relay their data frames facilitating sharing of status or any particular command to other units in Fig. 3 [9].



SOF: Start of frame, RTR: Remote transmission request, IDE: Identifier extension bit, r0:Resrved bits, DLC: Data lenght code, CRC: Cyclic redundancy check, EOF: End of frame

Fig. 3. The formats of CAN data frames.

The CAN bears a protocol which is synchronous in nature. Where multiple units simultaneously initiate frame transmission, the priority is identified via arbitration extractable from their IDs. Here, a zero or dominant bit supersedes a one or recessive bit.

III. ATTACKS

It is essential to identify weaknesses within a port in order to execute a CAN based attack. Here, we shall shed light on established vulnerabilities of automotive CAN and certain ways they may be exploited in Fig. 4 from [9].

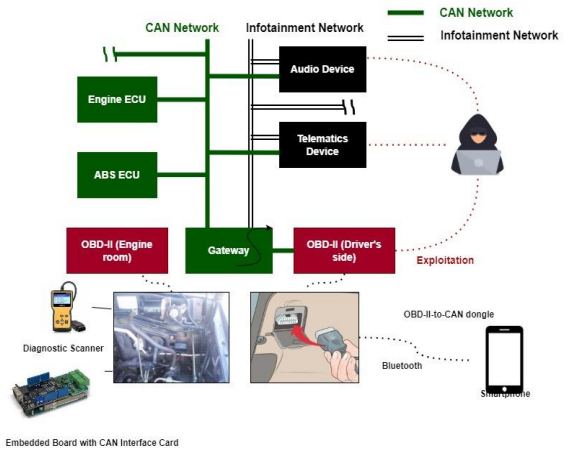


Fig. 4. Common Access Points to Automotive CAN: Audio and Telematics Systems in Modern Vehicles.

A. Surfaces

Surfaces for attacks may be categorized in the following manner.

i. Based on Physical Access

Automotive, nowadays, bear ports like the On-Board Diagnostics-II (OBD-II) enabling tangible access points to the CAN and Universal Serial Bus for diagnostics and updates to the firmware. These ports may still be taken advantage of by CAN bus attacks.

a) On-Board Diagnostics-II

On-Board Diagnostic-II represents the second generation of the On-Board Diagnostics system [11]. The OBD-II port was squarely exploited by the attacker's system to infect the bus with erroneous packets.

To look for loopholes, In [12] Checkoway *et al.* opted a frequently used PassThru device, which runs a variant of Linux. These devices facilitate ECUs to reprogram and diagnose themselves. The select device is armed with a Universal Serial Bus, Wireless Fidelity and an adapter that connects to the OBD-II port. As identified by the researchers, attackers using the same Wi-Fi as the device could easily gain access to it. This was due to the absence of authentication in the process. As a result, the attacker installed a hostile code to jeopardize the unit via system updates.

Another hostile tool 21ontact was used to perform On-Board Diagnostic-II attacks like packet injections and denial of service.

b) Universal Serial Bus of Audio Systems

In [12] Checkoway *et al.* exhibited that an audio system instantly updates itself once it identifies a certain file title on a thumb drive. An attacker can relay hostile code to the bus using an altered file.

Additionally, the researchers identified weaknesses within the MP3 and WMA parsers utilizing backwards engineering on the system firmware. The file's volume was not checked while being read. An attacker could generate an audio file that works fine on a personal computer but pass hostile content to the bus of the said audio system. Such files can be speedily broadcasted over P2P networks potentially causing widespread disaster.

ii. Based on Wireless Access (some Physical Access required)

The previous type of attack has a limited range. Here, attacks with an extended range depending on non-wired mediums are considered. Generally, two such mediums are fastened to a CAN in automotives nowadays: an On-Board Diagnostic-II adapter bearing a Bluetooth or a cellular interface, and a device based on telematics. Attackers may manoeuvre these mediums to remotely transmit hostile code, if an OBD-II adapter is connected to the automotive, or to take advantage of a telematics device using a USB or SD card. Below are instances of such attacks [13].

a) On-Board Diagnostics-II Adapter using a Wireless Medium:

Woo *et al.* exhibited a strike using an OBD-II adapter bearing an application performing diagnosis on its own. They deduced that even enterprise commodities could be abused in this fashion.

b) Universal Serial Bus of a Telematics Machine

Jo *et al.* studied an automobile bearing a telematics machine with Android OS [14]. Periodic updates, utilizing an SD card, are advisable subject to the nature of services being provided by the subject device. Jo et al. observed that the update, for signing, makes use of a publicly accessible Google key. The researcher concluded that an attacker may sign, in a cryptographic fashion, an altered file by using the said key. Eventually, installation of that file could result in a disaster.

iii. Based on Wireless Access (No Physical Access Required)

Physical access is limited to individuals with some sort of authority of doing so. In light of these shortcomings, attackers have focused their efforts around remote attacks with no physical intervention suggested in [12, 15, 16]. Such abuses manoeuvre weaknesses of non-wired mediums, infecting the CAN bus with hostile code via telematics machines. Below is a description of these attacks.

a) Bluetooth Medium

Checkoway *et al.* exhibited how a Bluetooth medium may serve as an easy passage to a CAN bus. The researchers identified weaknesses in the STRCPY function which failed to check volume of input. This was done over a telematics machine by backwards engineering a code associated with a Bluetooth protocol. They demonstrated, with the help of a buffer overflow, that a compromised machine connected to a telematics machine may run a hostile code on it.

b) Wifi Medium

Tesla's park and drive units were exploited utilizing a masquerade attack via their repair shop's SSID. In order to connect to the telematics machine, the spoofed Service Set Identifier assisted the adversary making use of the WiFi's auto connect attribute on the automobile. As a result, remote exploits executed on the web browser of the telematics unit.

c) Cellular Medium

OnStar, General Motors's telematics service, was considered next in Checkoway *et al.* The researchers backwards engineered aqLink communication protocol and concluded that 1024 bytes is the maximum size of the packet. Post analysis of the authentication pattern it was found that the number generator, which worked in a random fashion, got reset each time the machine booted. Accordingly, the researchers iterated that an adversary could remotely exploit this these vulnerabilities.

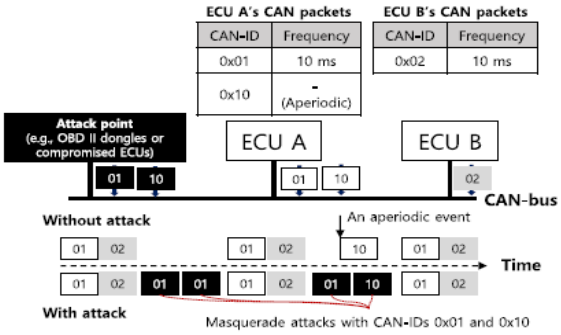
Similarly, weaknesses were identified by Miller *et al.* in Uconnect which was Jeep's proprietary service. This made Jeep recall 1.4M automobiles. These exploits were based on a cellular network access point. The researchers, connecting via HTTPS or Telnet service, attained a shell of the access point device. Eventually, evading the process of authentication, all Jeep vehicles were accessible through Uconnect. Hence, arbitrary packets, initiated in a similar fashion, could be sent to the CAN bus.

B. Scenarios

i. Masquerade Attack

In a masquerade attack in Fig. 5 from [9], to gain unsanctioned entry into a vehicle, an attacker may send harmful instructions with fake IDs through the bus by imitating an unexploited unit. In such attacks, in order to mess with the automotive functions, an attacker may utilize replaying as well as fabricating the message. While replaying a message, CAN packets are sent through without any alteration. The attacker makes up a packet by falsifying the ID and data fields, while fabricating the message.

ii. Denial of Service Attack

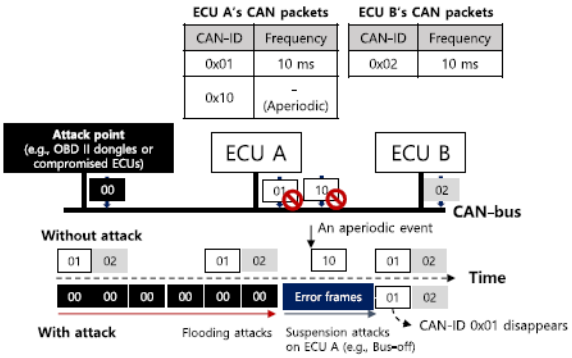


(a) Masquerade attacks

Fig. 5. Masquerade Attack.

An attacker may undertake a flooding attack on CAN to exhaust network resources or a suspension attack on a certain unit to interrupt the flow of messages in Fig. 6 from [9].

Fig. 6. DoS attacks (Flooding and Suspension attacks).



(b) DoS attacks (Flooding and suspension attacks)

a) Flooding

Here, an attacker repetitively dispatches numerous high priority packets. During the attack, unintended incidents take place as packets of other units having low priority fail to transport over the bus.

b) Suspension

During suspension, a unit may not be able to communicate over the CAN bus. The bus-off attack [17] is one method for such an attack.

iii. Combined Attack

Attackers altogether undertake a DoS and Masquerade attack to earn access to sensitive units. The ABS unit of Cherokee did not permit control of the brake due to periodic CAN packets, hence fabrication of the message was not sufficient. Therefore, the relay of turn turn off instructions of the ABS unit were countered through suspension [15]. This way, in a deceptive fashion, instructions successfully relayed at an acceptable periodicity [18].

IV. PROTECTIVE SYSTEM

We describe Fuzzing and Anti-analysis.

A. Fuzzing

Generally, consistent dispatching of distorted input in order to identify zero-day weaknesses of a said system may be done via fuzzing [5]. As per the available fuzzing methods, fuzzers contain an instruction generator as well as a monitor. The generator generates malformed instructions transmitted to the subject unit in order to push for unexpected failures and the monitor helps identify if that input affected the unit in Fig. 7.

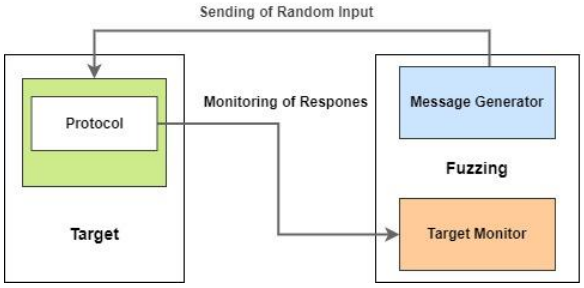


Fig. 7. Fuzzing.

B. Anti-Analysis

Following are a few anti-analysis techniques in use nowadays.

i. Firmware Protection

As per currently known attacks on CAN that manoeuvre firmware weaknesses, a tool for diagnosis, a port for debugging and an authentic weblink have been utilized to acquire a unit's firmware. Encrypting as well as obfuscating the firmware can help prevent straightforward accessibility [19].

ii. Anti-Monitoring

Monitoring steps of automotive CAN are commonly utilized to identify packets that target crucial units such as for the engine or the brakes. As packets are not ciphered, an attacker can take advantage of them. The work exhibited a technique for CAN to simulate a hurdle between the packet and the attacker. Here, a centralized node verifies all the units. Later, a key is distributed to all verified units. Accordingly, an attacker finds it difficult to track down and utilize a packet to gain access to a critical unit.

V. MESSAGE AUTHENTICATION

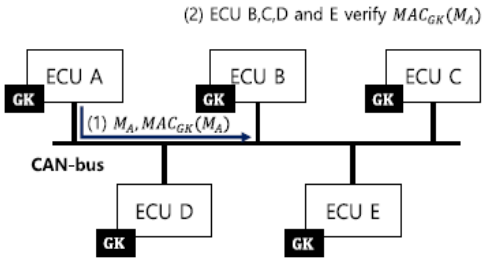
Methods to authenticate messages, utilizing authentication tags, have been engineered to tackle masquerade attacks. With reference to automotive CAN, it is important to consider the way authentication keys are shared and authentication tags are transmitted. 64 bits is the volume a data field of a packet can hold which is insufficient to hold the said tag [20]. Following are the available researches on these two issues.

A. Authentication Key Sharing

For authentication of messages, keys are shared through two approaches. Their advantages and disadvantages are as mentioned below.

i. Group Key

Here, a single key is shared by all units to produce tags for their correlating packets. Various works have taken on this approach of key sharing [7, 21, 22] There isn't a requirement of producing and passing on multiple tags as all units dispense a single key. It is important to note that only one tag is produced per packet in Fig. 8 from [9].

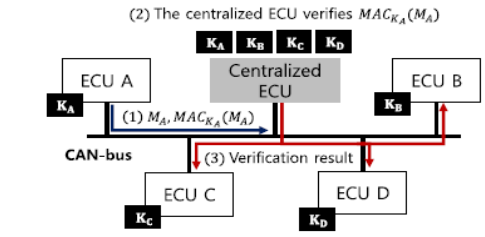


(a) Group key-based approach

Fig. 8. Group Key-based.

Masquerade attacks cannot be choked by the group key approach. Attackers may manoeuvre the key utilized to produce tags.

ii. Centralized Node



(b) Pairwise key-based approach (with a centralized ECU)

Fig. 9. Pairwise Key-based (Centralized ECU).

This approach has been taken on by a few works [23, 24] To save CAN from masquerade attacks accomplished via exploited units, each unit sets up their own key with the central unit. In charge of

message authentication is the central unit in Fig. 9 from [9].

B. Authentication Tag Transmission

A packet should be passed along with the correlating tag to assist with message authentication. Three techniques are suggested for tag transmission due to limited volume of the data field. For ease of understanding, consider the tag size is L bits where L is less than or equal to 64.

i. Basic Approach

To incorporate the data bits (64 minus L) and the tag, the data field is split in two parts. Before utilizing the basic approach, an adjustment to the database's data field is required. Relevant works were proposed in [24 - 27].

ii. Extended ID Approach

There are various nodes in the extended ID field as per CAN 2.0 B specification. Tags may also be transmitted with the help of an extended ID field. An extended ID field is used for carrying tags, a tag may be split into 18 bits in the extended ID field and L minus 18 bits in the data field. Relevant works were proposed in [7, 28, 29].

iii. Advanced CAN Packet Approach

An additional packet is used for passing the tag. As each packet requires another packet for authentication, a delay as well as a network constraint arises. A select technique is advised for critical packets in order to reduce burden on the CAN. In any case, the extra packet carries along the burden of an inescapable delay.

VI. SECURITY RESEARCH DIRECTIONS

Below we describe the prospective research areas regarding modern automotive CAN.

A. Protective System

We shall now proceed with an exploration of various research directions concerning protective systems within the realm of security.

i. Automated Network Fuzzing (In-vehicle)

Similar to the CAN related fuzzing works, a self-acting automotive CAN fuzzing method is required.

In existing fuzzing methods, a fuzzer typically comprises two essential components: a message generator and a target monitor. The primary role of the message generator is to create malformed CAN messages, which are then dispatched to the target Electronic Control Unit (ECU) during the fuzzing process to trigger unexpected failures. The target monitor, on the other hand, serves the purpose of assessing whether the target ECU under examination has been adversely affected by the malformed inputs originating from the message generator.

To create a fuzzing method that is both efficient and accurate, it is imperative to employ a model-driven message generator. In a model-driven message generator, the generation of CAN messages adheres to a systematic approach that considers the significance of each byte within the CAN data field. This data field is defined within a CAN database, which provides information about the purpose of each byte as it pertains to the data field's content in all CAN packets. However, it is worth noting that the existing message generators utilized in fuzzing methods often fail to consider the meaningfulness of the CAN packet data fields or lack a comprehensive description of the message generation model. Therefore, there is a pressing need for the development of a systematic automotive CAN fuzzing method that can infer the significance of every byte contained within the CAN data field and the associated network configurations.

ii. Dynamic Access Control Configuration

Various wireless connections will be utilized in autonomous vehicles to support communication technologies. An access control that can be dynamically set up, based on various factors, is essential for prevention of these systems from being exploited.

To thwart cyber attacks on these communication systems, it becomes imperative to establish an access control system that can adapt in real-time based on various factors like the vehicle's location, time, or its operational states. To develop such a dynamic access control mechanism, software-defined networking (SDN) emerges as a valuable cornerstone for the next generation of in-vehicle networks. SDN bestows superior flexibility and efficient resource management within in-vehicle networks by delivering the capability to program network functions. For instance, SDN controllers, which facilitate dynamic access control as demonstrated in the preceding context, could be harnessed to safeguard safety-critical segments of in-vehicle networks [30].

B. Message Authentication Protocol

Standardized by AUTOSAR, SOME/IP is an upcoming automotive middleware protocol. Elevated data rates and lower network constraints are ensured through it. The protocol provides message relay either in request and response or publish and subscribe form.

SOME/IP communications lack security functionality, which can result in messages being altered, suspended, or removed by attackers. Transport layer security is primarily utilized in modern day vehicles but is not compatible with messages being relayed to multiple hosts. To save modern vehicular systems, a balanced security protocol must be created.

VII. CONCLUSION

We discussed studies on CAN security and techniques for making exploits along with their counter measures in this paper. Also, we exhibited comprehensive attack cases involving masquerade, DoS and a combined attack. Through this, we analyzed the shortcomings of such methods and prospective options to counter them.

As per our work, a combined attack by an attacker is the most impenetrable because a masquerade and DoS attack are executed in parallel. Unfortunately, there is no comprehensive method to efficiently halt all possible damage of such an attack. Therefore, we bring forward research prospects for automotive networks. We have aimed our work at contributing towards a better understanding of present automotive CAN security research and broadening the horizon for new research opportunities pertaining to in-vehicle networks.

ACKNOWLEDGEMENT

Firstly, we are thankful to the Almighty for granting us the courage and knowledge to complete our work. Next, our families deserve our gratitude for their constant support and patience during this project. We sincerely appreciate Dr. Jawaid Iqbal, our supervisor, for his mentoring and insightful advice. Last but not least, we would also like to thank the entire teaching staff at the Faculty of Computing at Riphah International University for equipping us with the requisite fundamental knowledge and abilities.

REFERENCES

[1] J. Deng, L. Yu, Y. Fu, O. Hambolu and R. R. Brooks, "Security and Data Privacy of Modern Automobiles," *Data Analy. Intell. Transport. Syst.*, pp. 131-163, 2017.

[2] R. Currie, "Information Security Reading Room Developments in Car Hacking," *Retrieved August*, 2020.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Experimental Security Analysis of A Modern Automobile," in *2010 IEEE Symp. Secur. and Privacy*, Oakland, USA, pp. 447-462, 2010.

[4] A. Kr Mandal, F. Panarotto, A. Cortesi, P. Ferrara and F. Spoto, "Static Analysis of Android Auto Infotainment and On-board Diagnostics II Apps," *Softw.: Pract. and Exper.*, vol. 49, pp. 1131-1161, 2019.

[5] S. Bayer and A. Ptok, "Don't Fuss About Fuzzing: Fuzzing Controllers in Vehicular Networks," in *13th Escar Europe*, pp. 88, 2015.

[6] T. K. Kuppusamy, L. A. DeLong and J. Cappos, "Uptane: Security and Customizability of Software Updates for Vehicles," *IEEE Vehicul. Technol. Magaz.*, vol. 13, pp. 66-73, 2018.

[7] S. Woo, H. J. Jo and D. H. Lee, "A Practical Wireless Attack on The Connected Car and Security Protocol for In-Vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, pp. 993-1006, 2015.

[8] A. Humayed, F. Li, J. Lin and B. Luo, "CANSentry: Securing CAN-based Cyber-physical Systems Against Denial and Spoofing Attacks," in *25th Europ. Symp. Res. Comput. Secur. 2020*, Guildford, UK, 14-18 September, Part I 25, pp. 153-173, 2020.

[9] H. J. Jo and W. Choi, "A Survey of Attacks on Controller Area Networks and Corresponding Countermeasures," *IEEE Trans. Intell. Transport. Syst.*, vol. 2021, pp. 6123-6141, 2021.

[10] E. Aliwa, O. Rana, C. Perera and P. Burnap, "Cyberattacks and Countermeasures for In-Vehicle Networks," *ACM Comput. Surv.*, vol. 54, pp. 1-37, 2021.

[11] W. B. Dennyson and C. Jothikumar, "A Review on Controller Area Network and Electronic Control Unit in Automotive Environment," *J. Positive School Psychol.*, pp. 269-277, 2022.

[12] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *Proc. 20th USENIX Secur. Symp.*, pp. 77-92, 2011.

[13] S. M. Hossain, S. Banik, T. Banik and A. M. Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," *arXiv preprint*, arXiv:2310.09510, 2023.

[14] H. J. Jo, W. Choi, S. Y. Na, S. Woo and D. H. Lee, "Vulnerabilities of Android OS-based Telematics System," *Wirel. Person. Commun.*, vol. 92, pp. 1511-1530, 2017.

[15] C. Miller and C. Valasek, "Remote Exploitation of An Unaltered Passenger Vehicle," *Black Hat USA*, pp. 1-91, 2015.

[16] S. Nie, L. Liu and Y. Du, "Free-fall: Hacking Tesla from Wireless to Can Bus," *Briefing, Black Hat USA*, pp. 1-16, 2017.

[17] K. T. Cho and K. G. Shin, "Error Handling of In-Vehicle Networks Makes Them Vulnerable," in *Proc. 2016 ACM SIGSAC Conf. Comput. and Commun. Secur.*, pp. 1044-1055, 2016.

[18] M. Chen and M. Yan, "How to Protect Smart and Autonomous Vehicles From Stealth Viruses And Worms," *ISA Trans.*, vol. 141, pp. 52-58, 2023.

[19] L. Yu, J. Deng, R. R. Brooks and S. B. Yun, "Automobile ECU Design to Avoid Data Tampering," in *Proc. 10th annual Cyber and Inform. Secur. Res. Conf.*, pp. 1-4, 2015.

[20] H. Wei, Q. Ai, W. Zhao and Y. Zhang, "Real-time Security Warning and ECU Identification for In-vehicle Networks," *IEEE Sensors J.*, vol. 23, no. 17, pp. 20258-20266, 2023.

[21] J. Schmandt, A. T. Sherman and N. Banerjee, "Mini-MAC: Raising the Bar for Vehicular Security with A Lightweight Message Authentication Protocol," *Vehicul. Commun.*, vol. 9, pp. 188-196, 2017.

[22] Q. Wang and S. Sawhney, "VeCure: A Practical Security Framework to Protect The CAN Bus of Vehicles," in *2014 Int. Conf. Internet of Things*, pp. 13-18, 2014.

[23] B. Groza and S. Murvay, "Efficient Protocols for Secure Broadcast in Controller Area Networks," *IEEE Trans. Indust. Inform.*, vol. 9, pp. 2034-2042, 2013.

[24] H. J. Jo, J. H. Kim, H. Y. Choi, W. Choi, D. H. Lee and I. Lee, "Mauth-can: Masquerade-attack-proof Authentication for In-Vehicle Networks," *IEEE Trans. Vehicul. Technol.*, vol. 69, pp. 2204-2218, 2019.

[25] G. Bella, P. Biondi, G. Costantino and I. Matteucci, "Toucan: A Protocol to Secure Controller Area Network," in *Proc. ACM Workshop on Automot. Cybersecur.*, pp. 3-8, 2019.

[26] A. I. Radu and F. D. Garcia, "LeiA: A Lightweight Authentication Protocol for CAN," in *21st Europ. Symp. Res. Comput. Secur.*, Heraklion, Greece, 26-30 September, 2016.

[27] T. Y. Youn, Y. Lee and S. Woo, "Practical Sender Authentication Scheme for In-Vehicle CAN with Efficient Key Management," *IEEE Access*, vol. 8, pp. 86836-86849, 2020.

[28] B. Palaniswamy, S. Camtepe, E. Foo and J. Pieprzyk, "An Efficient Authentication Scheme for Intra-Vehicular Controller Area Network," *IEEE Trans. Inform. Forens. and Secur.*, vol. 15, pp. 3107-3122, 2020.

[29] K. D. Kang, Y. Baek, S. Lee and S. H. Son, "An Attack-resilient Source Authentication Protocol in Controller Area Network," in *2017 ACM/IEEE Symp. Architect. Netw. and Commun. Syst.*, pp. 109-118, 2017.

[30] S. Woo, H. J. Jo and D. H. Lee, "A Practical Wireless Attack on The Connected Car and Security Protocol for In-Vehicle CAN," *IEEE Trans. Intell. Transp. Sys.*, vol. 16, no. 2, pp. 993-1006, 2015.