Proceedings of the International Conference on Edge Computing and Applications (ICECAA 2022)
IEEE Xplore Part Number: CFP22BV8-ART; ISBN: 978-1-6654-8232-5

Survey on CAN-Bus Packet Filtering Firewall

Sahana Y P
Digital electronics and advanced communication
Manipal academy of higher education
Karnataka, India
sahanaprakashyarnool@gmail.com

Ajey Gotkhindikar
Subject matter expert
Automotive Cybersecurity
KPIT Technologies Ltd, India
ajey.gotkhindikar@kpit.com

Shailendra Kumar Tiwari
Department of ECE
Manipal Academy of Higher Education
Karnataka, India
sk.tiwari@manipal.edu

2022 International Conference on Edge Computing and Applications (ICECAA) | 978-1-6654-8232-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICECAA55415.2022.9936152

***Abstract*— The world is moving towards autonomous vehicles and the vehicle is exposed to various types of communication, like Vehicle-to-vehicle (V2V), Vehicle-to-Grid (V2G) and Vehicle-to-Everything (V2X). This communication facilitates telematics, diagnostics and over the air software update features. The vehicle is also connected via various interfaces like Wireless Fidelity (Wi-Fi), Bluetooth (BT), Universal Serial Bus (USB), and On-board Diagnostics (OBD) to the external world for various purposes. This opens possibility for several cyber-attacks through external ports, network interfaces if there are no adequate cyber security mechanisms implemented, and cybersecurity risks are not treated. Controller Area Network (CAN-bus) is a central nervous system of the modern vehicle and most of the in-vehicle communication takes place on it. Unfortunately, the CAN-bus is inherently insecure and lacks basic security features like authentication and encryption. The insecure nature of CAN-bus in a vehicle lead to several security exploits and malicious activities which put driver and passengers at risk. Therefore, security measures need to be implemented in the automotive network. This paper addresses CAN vulnerabilities, critical attacks, and security measures to protect CAN bus such as cryptographic measures, firewall and methods to detect and prevent such attacks. Certain approaches have been identified and discussed in this paper. Moreover, this paper attempts to bring together essential background knowledge required to work on security for CAN network in automotive embedded systems.**

Keywords*— *CAN Vulnerabilities, Attacks on CAN, Security Measures, Packet filtering firewall, Binary Decision Diagram-BDD.

I. INTRODUCTION

In the past two to three decades vehicles are becoming more advanced, more autonomous, more complex in terms of automotive electronics. An embedded system that controls an electrical subsystem is called an Electronic Control Unit (ECU) in a vehicle. There are more than 70 ECUs in a modern car which provides entertainment, navigation, central locking mechanisms, and other safety systems like adaptive cruise control, automated lighting, anti-lock braking system, airbag control, traffic warnings, Collision avoidance etc. There should be quick and reliable communications between these electronic modules for the normal operation of the vehicle. The electronic control modules, the sensors, actuators, and other devices communicate through the in-vehicle networks like CAN, FlexRay, Local Inter Network (LIN), and Media Oriented Systems Transport (MOST) as shown in the Fig.*1* and Ethernet for higher bandwidth. CAN protocol is considered as a de-facto communication standard for various electronic control units to communicate between sensors, and other devices. As the cars get exposed to the outside world through the internet connectivity, Bluetooth wireless link to connect cell phones to have hands-free calls and Telematics functionalities, this results in increased number of attacking surfaces and entry points for hacking. There is no source identifier or authentication and encryption built into CAN packets. Because of these shortcomings, it is easy to sniff the packets on the network as well as to masquerade as other ECUs and send modified packets. Therefore, security measures need to be implemented in the automotive network. Firewalls can be considered as the first line of defense and restrict malicious CAN packets entering the in-vehicle network from the external world.

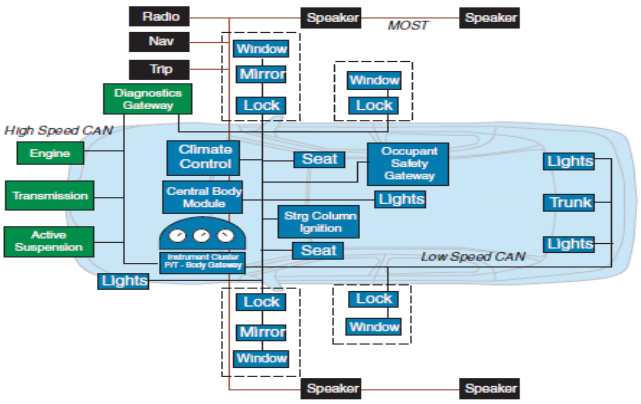


Fig.1. Typical Automotive Network [1]

This paper is divided into different sections as follows. Section I, Introduces the In-vehicle network. Section II is focused on CAN protocol format, Vulnerabilities and critical attacks on CAN. Mitigations and security approaches are explained in Section IV and also introduce firewall, its types and the significance of the firewall. The literature survey is focused on firewall technologies which are explained in the Section V.

II. BACKGROUND

A. CAN-bus

In 1985, Robert Bosch developed a serial bus communication protocol for the in-vehicle network called CAN bus. The protocol was officially released at the Society of Automotive Engineers (SAE) conference in 1986, Detroit, Michigan [2]. There are several versions of the CAN specification were published. There are two parts part-A and part-B in the latest standard 2.0 published by the Bosch in 1991. Part-A is for the standard format with an 11-bit identifier CAN 2.0A and part-B is for the extended format with a 29-bit identifier CAN 2.0B [3]. The CAN standard and extended format are shown in Fig.*2*.

ISO1898 standard is released by ISO (International Society of Organization) in 1993 and divided into two parts. The protocol defines the lowest two layers of OSI (open system interconnect) data link layer (ISO 11898-1) and physical layer (ISO 11898-2) for high speed. Later ISO 11898-3 is released, which is for the physical layer for low speed and fault tolerant. In 2012, Bosch released CAN FD 1.0 (CAN with Flexible Data-Rate), which was developed to meet the automakers demands for more accurate and for real-time applications, this is designed for transmitting and record data along with errors between devices and microcontrollers without the help of host computer This specification has different formats which allow different data lengths and for operating with a faster bit rate once the arbitration is decided.

As the CAN-FD is compatible with present CAN 2.0 specification, these devices can be connected on the same network along with CAN 2.0 devices. There are several CAN-based higher-layer protocols that are standardized. The user choice is according to the application. These are used in a variety of applications including industrial automation, autonomous devices, defense and underwater vehicles and medical equipment. This protocol is message based and it is denoted as a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), where the protocol listens to other nodes in the network for avoiding collisions. It also contain error detecting and error handling methods. It can handle bit rate up to 1 Mbps when the physical distance between the nodes is less than 40m within the network. Four different message formats are present in CAN, they are data, remote, error and overload frames.

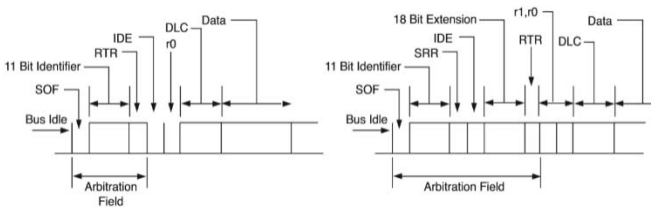


Fig.2. CAN message frames [1].

The data frame is explained in detail and is as shown in the Fig.*3*.The data frame begins with the Start-of-frame (SOF) bit which is of the single dominant bit, next is arbitration field which consists of eleven-bit Identifier and RTR-bit (Remote transmit request). The RTR-bit must be 'dominant' in the data frame and 'recessive' in the remote frame. Followed by the control field which includes data length code (DLC) and two bits for future expansion are reserved. The data length code is four-bit wide which defines how many bytes of data is present in the data field. The data field can be zero to eight bytes of data. The data field is followed by cyclic redundancy checksum (CRC), which enables the receiver that the data received is not corrupted. Acknowledge field (ACK) contains two bits and these will be 'recessive' at the transmitting station. It is replaced by a dominant bit by the receiver to acknowledge that it received the valid message. Both Data frame and Remote frame ends with EOF (End-of-frame) which contains a flag sequence of seven recessive bits.

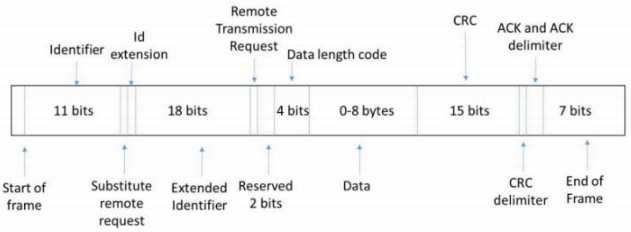


Fig.3. The CAN message format

B. Arbitration

As stated earlier, messages are identified by the static identifier (ID). All messages are transmitted over the bus based on the priority. The priority of the messages resolved by the arbitration. The conflict occurs whenever two or more transmitting nodes are sending messages over the same network and at the same time. Arbitration helps to overcome this conflict. Messages with lower Arbitration ID will get the bus and the message transmitted. Arbitration is handled by CAN transmitter. By comparing the value being processed and the value on bus, CAN transceiver checks both the values. If the values are same then it continues transmission else stop transmitting. The transmitted value is AND'ed bit wise with value on the bus. So, the transmitted value is 0 and the bit on the bus is 1, the result zero will be transmitted. Thus, the lower value node wins the arbitration. Due to arbitration DoS type of attack is possible if an attacker send high priority messages for an example sending sequence of dominant bit '0'. The bus will not be available for other ECUs to transmit messages and this may affect the normal operation of the vehicle.

C. CAN Vulnerabilities

III. The lack of inherent security mechanism of CAN lead to attacks from physical attack surfaces through OBD port and from wireless attack surfaces such as GPS, GSM module, Bluetooth and Wi-Fi. Various attacking surfaces are shown in the

Fig.4. Table1 gives the summary of vulnerabilities, different possible attacks and security measures for CAN network.

Table 1: Summary of violated security aspects, potential attacks and security measures (to CAN network)

Violated Security aspects	Vulnerabilities of CAN protocol	Possible Attacks	Security Measures
Confidentiality/privacy	Message broadcasting	Eavesdropping	Encryption algorithms
Integrity	Lack of authentication/ addressing	Sniffing/Spoof	Cryptographic hash functions, MAC or Digital signatures
Authenticity	Lack of authentication	Masquerading	MAC or Digital signatures
Availability	Lack of addressing/authentication	Replay, Injection, flooding/DoS attacks	IDS, IPS and Firewalls
Non-Repudiation	Encryption	Sniffing	Forensics support

Weakness of vehicle security arise from the widely used CAN is highlighted in [4], and it is listed below

- Message Broadcasting: Once the message is sent on the CAN bus it is present at every node of the network. Any node or controller has access to it can accept or reject. A passive attacker can read a message by having access from the diagnostic port or by inserting a malicious node on the CAN bus. Eavesdropping can take place which is kind of sniffing on the network.
- Lack of addressing: Nodes in a typical CAN network does not have identification address, all nodes (real or malicious) can send and receive information anytime inside the network without the verification that a source of the information is valid.
- Lack of Authentication: As the source authentication is not present, it is not possible to ensure if message received from valid source. Therefore masquerade attack takes place, in which an attacker acts as an authorized user of the system.
- A common point of entry: Once an attacker gains access to the CAN network, there is no limit that what are the parameters they can obtain within the network. Diagnostics port is the common gateway to the in-vehicle network where all the systems connected. Example OBD-II port provides access to all the systems.
- Limited Bandwidth: Complex authentication or security algorithms requires more bandwidth and processing power for robust communication. But, CAN with 11-bit and 29-bit identifier message structures provides only 64-bit of data in payload and less data for security purposes. The complex authentication algorithms could not be implemented on CAN bus because of the limited bandwidth.
- Lack of Encryption: The robust encryption could not be implemented as there is no higher bandwidth is available in the present CAN bus. For a few sensitive messages and security-related protocol need protection against eavesdroppers. Encryption is necessary for critical data exchange between any two in the CAN network.

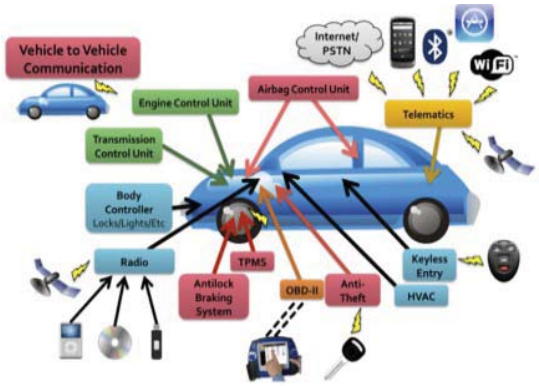


Fig.4. Possible entry points of the modern car [4].

A. Critical attacks on CAN

- Replay attack: The attack in which the transmitted data is delayed or repeated maliciously. Masquerade attack is followed by a replay attack where it needs to pretend to be some other node and retransmits the copy of the message it has received from the bus. The copy of the message may be unaltered or modified. Even though there are tables to match the message id to the sender and determine the identity of the sender at the other nodes but there is no concept to authenticate it. Aruljothi and Priyadarshini [5], have demonstrated a practical wireless attack using a real vehicle in a connected vehicle environment, and they also propose a security protocol for CAN as a countermeasure designed in accordance with current CAN specifications with RKP(random key pre-distribution).
- Injection: In this attack, injecting malicious message on the network appearing to be legitimate. It involves disturbing normal operations of the vehicle. This attack can be done by the node in the trusted network. Any node can send any message in the CAN network.
- Denial of Service (DoS): DoS is a cyber-attack in which the resources are unavailable to intended users temporarily or to damage permanently and weakening the performance of the system. Flooding the network with higher priority messages by sending the sequence of dominant bits continuously. By inducing too many errors to the target node or device where the node on CAN bus goes to so-called bus-off state and removed from the bus so it cannot send or receive further messages. Doing this can disable a device (e.g. critical safety systems) and compromises certain vehicle functionalities. Murvay and Groza [6] have

explained about DoS attacks at different layers of CAN protocol. Concentrated more on DoS attacks of Data link layer as it's very difficult to mitigate with application layer mitigations techniques.

- Man-in-Middle attack: Secretly, an attacker receives and pass the message and alters communication between two nodes for a certain period. Robert Buttigieg et al [7] have explained how the rogue device is inserted in CAN network as a man in middle attack using Proof of Concept (POC) by instrument cluster and vehicle simulator. The main aim of their project was to look into the lack of security in the CAN-Bus protocol, in particular, the lack of authentication of devices and the lack of data encryption. This experiment focused on the possibility that an unauthorized man in the middle device can be connected to the CAN-Bus with the ability to send spoofed messages.

IV. SECURITY APPROACHES

A. Authentication

There is a possibility of changing the program of an authorized node and spoof the messages on the CAN network and also add a rogue device as there is no authentication. Many researchers have been working to implement effective authentication mechanism for the in-vehicle network. These measures should be implemented at every node of the network. [8] specifies use of Message Authentication Code (CMAC) for authenticating each ECU and CAN messages to prevent spoofing attack. Nicolas Bravo et al [9] proposed Public key/secret key authentication scheme for CAN by using Hash-based Message Authentication Code (HMAC). One pair of public and private keys were given to each node of the network where it shares the signed messages.

B. Encryption

Encryption is a cryptographic approach to hide the intelligence of the message from unauthorized users. Complete security of any information is not secured by encryption alone. Authenticity, integrity and confidentiality are ensured by using various cryptographic algorithms. Symmetric and Asymmetric are the two different cryptographic algorithms. Asymmetric algorithms such as RSA (Rivest–Shamir–Adleman), Elliptic curve cryptography (ECC) use different keys and ensures more reliability than symmetric algorithms like Advanced Encryption Standard (AES) which uses a single secret key. To meet the vehicle communication requirements such as computation, capacity, and timing, a combination of symmetric and asymmetric algorithms are used. Asymmetric encryption methods are used for secure key distribution and symmetric encryption for secure communication broadcast inside the vehicle-bus system. Public Key cryptographic techniques are more effective for securing communications with external entities including telematics, service providers and internal communications between safety-critical systems, sensors against cyber-attacks.

Cryptographic algorithms require intense computation to have effective secure communication considering acceptable latencies. Hence, to protect the confidentiality of stored keys, certificates and user credentials requires hardware support. These cryptographic algorithm requirements are beyond the resources available in typical automotive microcontrollers today. A Tiny Encryption Algorithm, Feistel type cipher was used to encrypt the message on CAN bus for a particular microcontroller and proved that this algorithm can be used to hide confidential data on the bus from eavesdropping.
The confidential data like vehicle identification number or other sensitive information. This methodology was designed for a particular processor with the defined parameters by [10]. The mechanism in [11] produces a new field called CAN Message-Authenticator (CMA) which contains both the hash value and timing information which will be used to generate the hash. Authentication of each CAN messages can be done thus it can resist replay attack. Here they have considered CAN Identification Number (CIN) which is unique for each ECU in a particular vehicle. The CMA will be used to verify the legitimacy of the message by a legitimate ECU upon receipt of a frame.

C. Software & Hardware Approaches

Gateways in the modern car are used to connect the different networks. In order to have a secure communication between these networks, messages must be checked at the gateways before broadcasting the messages on to the networks. For example, messages from the ECUs connected to the networks like LIN and MOST should be prevented from entering into the critical-safety bus systems such as CAN and FlexRay. Firewalls can control the messages based on certain rules and rules may depends upon the ECU capabilities. Firewalls can be a best option to control the messages and it even checks the incoming network traffic.

Intrusion detection and prevention system (IDPS) can be an alternate for cryptographic techniques to regulate external and internal communications as it needs hardware support which is not beyond what is already there in typical microcontrollers present in ECUs especially to secure CAN bus. IDPS monitors the traffic of vehicle bus and detects if there are an unusual activity and initiate processes to bring back the system to safe-mode and prevent from further damage. By regulating the OBD-II port with creating hardware key or password to access the port where it is physically located can protect against illegal entry of devices into CAN. The security mechanisms are effective until it is upgraded eventually. Security software updates may be over-the-air or dealer distributive, are bound to be an integral part of security and safety of the automotive system.

D. *Significance of Firewall*

Firewalls have been the frontier defense to secure networks against attacks and unauthorized traffic by filtering out unwanted network traffic coming into or going from the secured network. The filtering decision taken according to a set of ordered filtering rules defined based on predefined security policy requirements [12].The complexity of managing firewall policy limited the effectiveness of firewalls even though it is the main step to secure the network.

Al-Shaer and Hamed [13] have developed an anomaly-free firewall rule editor, which greatly simplifies adding, removing and modifying rules into firewall policy. They used the Java programming language to implement these algorithms in one graphical user-interface tool called the "Firewall Policy Advisor". The rule is set according to one or more different filtering fields.

There are two types of hardware and software firewall as per the user point of view. There two types of firewalls for CAN network as follows [14].

- Packet Filtering Firewalls: Static packet filtering firewalls sequence the packets concerning allow or deny. This is done by considering the field's information on the header such as host/destination address, port number. The depth analysis is not done at this stage. Each packet is examined as a single entity. It is unable to defend the fragment and spoofing attacks.
- Circuit Level Gateway Firewalls: These are deployed at the session layer. To determine the requested session is legitimate or not, Gateway firewalls monitor Transmission Control Protocol (TCP) handshake between the packets. By doing this, the public IP addresses are provided to the outside network and not exposing the internal private IP addresses to the external potential intruders. Circuit-level gateway firewalls do not filter individual packets. An attacker may take advantage of this once the connection is established.
- Application-level Gateway Firewalls: The firewalls decide to allow or drop the packets based on application information which is present in the packet and provide protection for specific application layer protocol. The best example for this kind of firewalls is Proxy server firewalls. Both the client and server are connected to these proxies instead of direct connections so any suspicious data or connections can be dropped by these proxy servers. Application firewalls do deep inspection of each session and decide to drop or allow them to pass through the proxy server by using information present in the application protocol payload or header. Application Gateway firewalls can increase the network performance and makes easier to log traffic.
- Stateful Multilayer Inspection Firewalls: The combination of all the types of firewalls listed till now is called Multilayer Inspection Firewall. These firewalls can filter packet at Network layer using Access Control Lists (ACL), identify the legitimacy of sessions at session layers and evaluates at the Application layer. This firewall can provide a transparent mode in which direct connection is available for the client and server. These can also implement algorithms and complex modules to make connections more secure.

E. *Packet filtering firewall in the automotive network*

The CAN and its security have become hot-topic for researchers and automakers after a number of high-profile hacking activities in the past couple of years. An attacker can have direct access to the CAN-bus through the OBD port. Charlie Miller demonstrated the vulnerabilities of the onboard computers and networks like CAN-bus by linking these onboard computers in the mid of 2010. Miller and Valasek demonstrated the car attack by altering the CAN message and controlled steering wheel by spoofing park assist [15]. The attackers created software called CarShark to monitor communications between the ECUs and insert fake packets of data to carry out attacks [16].

CAN protocol was designed concerned about reliability but not intended to provide secure communication. The embedded computers present in the cars have strong hardware constraints for computation power and memory left for security mechanisms. Because of which ECUs cannot perform complex cryptographic algorithms to perform strong encryptions. Where an attacker can have limitless hardware to perform cryptanalysis and can break simple algorithms. The security mechanism for a car should be such that its requirements should be within the constraints.

The advantage of packet filtering firewall is, firewall requires fewer resources and computation power. The data exchange with the external world can be restricted by the firewall. Even though an external device is authenticated and starts sending data or signals to the network, it is not wise to accept all those data because those external devices might be compromised. Hence there should be a firewall at the gateway which can control the access to the internal network by external devices and acts as a secondary security mechanism [17].

V. LITERATURE SURVEY

Wolf et al [18] have given Exposures to Automotive Bus systems, Gateway firewalls and its importance. A secured approach was proposed using modern cryptography which is against manipulation and provides authentication and secrecy. This gives the best way to tackle many of the vehicle security issues.

Alex Oyler and Hossein Saiedian [19] have explained how one can compromise CAN bus and ECU through Telematics and found attacking surfaces. The device can be installed via the cellular network on OBD. Countermeasures for this is to separate external network from the internal network by combining firewall and Intrusion Detection System (IDS) at Central Gateway System (CGS).

Tharaka et al [20] present a detailed study of firewall technologies and firewall capacity along with other firewall technologies in order to prevent unauthorized accesses. They mentioned that high capacity firewall can provide high performance but it is expensive.

Wei YAN has designed a Bi-directional firewall module which includes vehicle status logger, a CAN message filter and storage module. The storage module is used to store a White-list and a Black-list and the CAN message filter is configured selectively chooses any one of these according to the status of the vehicle [21].

Hamed Salehi et al [22] have mentioned that as soon as detecting higher priority attack by Network Intrusion Detection System (NIDS) send some recommended protection information to the firewall which will set appropriate rule to destroy the connection it. The deep inspection of six layers has been explained in this paper.

Adel El-Atawy and Ehab Al-Shaer [23] explained how rules and policies can be represented as Boolean expressions. Implementation and maintenance of this expression can get complex hence they used Binary Decision Diagram (BDD), where each variable need to be checked only once thus improving packet matching time.

Masud et al [24] have implemented a data-driven firewall. Using a classifier, first finds the packet matching to a class contains a setup of rules. Then finds a matching rule for that respective packet. The results showed that the time required for finding matching rule is six times faster than the conventional methods. In this, they used offline training data for classifier and have considered only the packet header. The last rule is with default empty condition so that any packet could match at least one rule.

Anshu Aneja & Vivek Thapar [25] have explored alternate representations for rule sets which are used to remove the redundant computation using Binary Decision Diagram (BDD) approach and implement the multi-dimensional filtering. This takes less space for storage and less look-up time for accepting or rejecting the incoming packets. They obtained average results of 75.24% and 33.74% for comparison for "Most Reject Packets" and "Most Accept Packets" respectively for about one million incoming packets. Results are shown in the Fig.5.

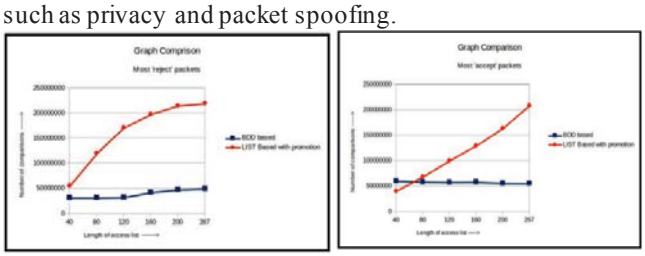
Dongre and Shikalpure [26] attempted to improve the rule matching time by maintaining two different files. The log file consists of information related to the captured packets recently and this is the sub set of the main file. Another file is Index file, which stores Hash values calculated for each packet. Here each incoming packet is not mapped to the main file instead succeeding packets related to the same flow are compared with the log file.

Gupta and McKeown [27] proposed a method for Packet Classification using Hierarchical Intelligent Cuttings (Hi-Cuts). The HiCut algorithm works by carefully preprocessing the classifier to build a decision tree data structure. Each time a packet arrives, the decision tree is traversed to find a leaf node, which stores a small number of rules. High dimensional (considering many fields) requiring smaller storage and comparable query time when compared with other schemes.

James Joy et al [17] presents an architecture for secure automotive communication both external and internal, by using the Smart Gateway which consists of an external and an in-vehicle gateway and a firewall. The Smart Gateway handles authentication, data integrity and secure key storage and management for both external devices connected to the vehicle as well as for the network communication between ECUs.

Pese et al [28] have shown where internal firewalls can be deployed in the E/E architecture and introduced in automotive. The Hardware (HW) firewall (located at the connectivity gateway) shall handle a large, simple and generic rule set to restrict the traffic between domains whereas the Software (SW) firewall shall focus on a small filter rule set for custom-made rules and Stateful packet inspection. Packets which pass the first layer of security (HW firewall) are shunted to the SW firewall for a deeper analysis.

Wei Si et al [29] proposed a hybrid wired/wireless protocol using Backpressure Collection Protocol (BCP) to mitigate DoS attacks by placing a ZigBee at all critical nodes which monitors link qualities and schedules packet transmission accordingly. Emerge of wireless communication into the intra-vehicular network need to face security issues such as privacy and packet spoofing.



"Most Rejected packets" "Most Accepted packets"

Fig.5. Graph comparison for "Most Rejected packets" and "Most Accepted packets" [25].

VI. CONCLUSION

In this paper, we give a brief introduction of in-vehicular networks and explained CAN protocol. We summarize certain vulnerabilities on CAN protocol and possible attacks on it. There are many effective cryptographic techniques to secure any network but when it comes to the automotive systems it has few due to resource constraints. IDPS can track traffic inside the network and detect the anomaly activities and prevent before it affects the system. A firewall prevents unwanted traffic from the outside network and acts as a defender at the entry level. There will be fewer chances of

getting hacked if we can control the access before the data or signals enter the trusted boundary.

The effective way of securing CAN bus is to implement Packet filtering firewall at the Central Gateway. It is feasible to implement a software firewall on the Gateway as the software need not know the developer resources and it is embedded during the ECUs software build process. Software updates can easily be done regularly during the scheduled service visit or by over-the-air updates as the firewall present on the gateway. Algorithms like BDD for packet filtering firewall requires less space for storage and lookup time to accept or reject the incoming packets by comparing the results with the listed order method. One should consider all constraints and develop a security framework for automotive system. Further research is needed to bring out the experimental results to decide which optimizing algorithms are best for the automotive systems. The background knowledge of security measures and its drawbacks depicts that the need for firewall and IDPS systems in the car to reduce attacks on CAN network.

Future work: We are motivated for the development of effective countermeasures to secure CAN bus by focusing on practical CAN based attacks in automotive systems. We are exploring ways to deploy firewall at Central gateway and concentrating on a few ECUs which exchange data between an outside world like telematics, Infotainment, and Diagnostics units. We are working on software firewall for CAN bus with framework considering resource constraints of embedded microcontrollers of ECUs at present.

REFERENCES

[1] J. A. Cook, J. S. Freudenberg, "Controller Area Network (CAN)", EECS 461. Fall 2008.

[2] https://en.wikipedia.org/wiki/CAN_bus, Date accessed: 5/11/2018

[3] CAN Specification, Version 2.0, Robert Bosch GmbH, 1991.

[4] K. Koscher et al. "Experimental security analysis of modern automobile", in Security and Privacy (SP), 2010 IEEE Symposium on, Oakland, CA, USA, May 2010, pp. 447–462.

[5] M. Aruljothi and C.S. Priyadarshini, "Security-Based Protocol Design for In-Vehicle Controller Area Network", International Journal of Science and Engineering Research (IJOSER), 2016.

[6] Pal-Stefan Murvay and Bogdan Groza, "DoS Attacks on Controller Area Networks by Fault Injections from the Software Layer", In Proceedings of ARES'17, Reggio Calabria, Italy,2017.

[7] Robert Buttigieg, Mario Farrugia, and Clyde Meli, "Security Issues in Controller Area Networks in Automobiles", an 18th international conference on Sciences and Techniques of Automatic control & computer engineering - STA'2017.

[8] H. Ueda, R. Kurachi, H. Takada, T. Mizutani, M. Inoue, and S. Horihata, "Security authentication system for in-vehicle network", SEI technical review, 81, , 2015, pp.5-9.

[9] N. Bravo, S. Koppula and M. Chang, 6.857 Final Project "A Public-Key Authentication Scheme for Controller Area Networks", 2015, pp. 1-17.

[10] M. Jukl, J. Cupera, "Using of tiny encryption algorithm in CAN-Bus communication", Research in Agricultural Engineering, 62(2), 2016, pp.50-55.

[11] P. Carsten, T.R. Andel, M. Yampolskiy, J.T. McDonald and S. Russ, "A system to recognize intruders in controller area network (can)", In Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research. September 2015, pp. 111-114.

[12] U. Thakar, L. Purohit and A. Pahade, "An approach to improve performance of a packet-filtering firewall", In 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN) IEEE, 2012 pp. 1-5.

[13] E.S, Al-Shaer and H.H. Hamed, "Firewall Policy Advisor for Anomaly Detection, Rules Editing and Translation", Integrated Network Management 2003, pp. 17-30.

[14] I. Kashefi, M. Kassiri and A. Shahidinejad, "A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities", International Journal of Engineering Research and Applications (IJERA), 3(2), April 2013, pp.585-591.

[15] Charlie Miller, Hackers Remotely Kill A Jeep On The Highway—With Me In It. [Online] Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[16] Hack attacks mounted on car control systems, [Online] Available: https://www.bbc.com/news/10119492.

[17] J. Joy, S. Samuel and V.S. Vinu, "Gateway Architecture for Secured Connectivity and in Vehicle Communication", 16th International Congress Electronics in Vehicles, Oct 2013.

[18] M. Wolf, A. Weimerskirch, and C. Paar, "Secure in-vehicle communication", In Embedded Security in Cars, Springer, Berlin, Heidelberg, 2006, pp. 95-109.

[19] A. Oyler and H. Saiedian, "Security in automotive telematics: a survey of threats and risk mitigation strategies to counter the existing and emerging attack vectors", Security and Communication Networks, 9(17), 2016 pp.4330-4340.

[20] S.C. Tharaka, R.L.C. Silva, S. Sharmila, S.U.I. Silva, K.L.D.N. Liyanage, A.A.T.K.K.Amarasinghe, and D.Dhammearatchi, "High-Security Firewall: Prevent Unauthorized access Using Firewall Technologies", International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016, pp. 504-508.

[21] Wei YAN," Vehicle Communication System Based On Controller Area Network Bus Firewall", the United States, Patent Application Publications YAN, October 17th 2017.

[22] H. Salehi, H. Shirazi and R.A. Moghadam, "Increasing overall network security by integrating Signature-Based NIDS with Packet Filtering Firewall", In 2009 International Joint Conference on Artificial Intelligence, IEEE, April 2009, pp. 357-362.

[23] A. El-Atawy, E. Al-Shaer, T. Tran and R. Boutaba, "Adaptive early packet filtering for defending firewalls against DoS attacks", IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2009, pp. 2437-2445.

[24] M.M. Masud, U. Mustafa and Z. Trabelsi, "A data driven firewall for faster packet filtering", In Fourth International Conference on Communications and Networking, ComNet-2014 IEEE, pp. 1-5.

[25] A. Aneja and V. Thapar, "Optimizing Packet Filter Firewall using Duple Decision Scheme", The SIJ Transactions on Computer Networks & Communication Engineering (CNCE), vol.1, issue.2, May-June 20132013, pp.28-33.

[26] S. A. Dongre, S. G. Shikalpure, "Hashing Based Packet Matching Algorithm for Firewall", International Research Journal of Engineering and Technology (IRJET), vol.2, issue.7, Oct-2015

[27] P. Gupta, and N. McKeown, "Packet Classification using Hierarchical Intelligent Cuttings", Proc. Hot Interconnects VII Aug. 1999 Stanford, IEEE, vol. 20 no. 1 Jan./Feb. 2000 pp. 34.

[28] M. Pese, K. Schmidt and H. Zweck, "Hardware/Software Co-Design of an Automotive Embedded Firewall", SAE Technical Paper 2017, DOI: 10.4271/2017-01-1659

[29] W. Si, K. Starobinski and M. Laifenfeld, "Protocol-compliant DoS attacks on CAN: demonstration and mitigation", In 2016 IEEE 84th vehicular technology conference (VTC-Fall), IEEE, 2016, pp. 1-7.