Intrusion Detection System: An Approach to Autonomous Vehicles

Rashmi B H
Executive Engineer, Elektrobit India Pvt. Ltd, Bangalore, Karnataka, India

Abstract **- Due to advance in changing technology in modern vehicular systems which consist of many sensors, electronic control units and actuators and with the advent of Intra-Vehicular systems, whose task is to control and monitor the state of the vehicle comprises of a Complex vehicular system. In addition to this, modern vehicles are becoming a surface for Cyber-attacks, because it is being increasingly connected to V2X (Vehicle-to-Everything) Technologies. So, it is highly recommended to ensure vehicle safety and customer trust. To manage the above challenges, countermeasures should be taken to prepare a vehicle, in order to be protective from Cyber-security threats and also a reliable mechanism should be in place to detect the possible intrusions entering the vehicle when it is in operation, this mechanism or practice is known as Intrusion-Detection system (IDS). This paper provides a structured view of Intrusion detection system in intra-vehicle for passenger vehicles. This paper also provides an insight of some ongoing research challenges and some gaps in intra-vehicle systems.**

Index Terms **- Vehicle-to-Everything (V2X), Intrusion Detection System (IDS), Cyber-attacks, CAN.**

I.INTRODUCTION

The rapid increase in the new technologies by multiple car production managers has made a revolutionary impact on modern connected vehicles. These rapid advancements include new features such as Automation features and vehicles getting connected to outside world, in simple it could be termed as Vehicle-to-Vehicle(V2V) and Vehicle-to-Infrastructure(V2I) communications. These communications enable safety and co-operation among vehicles.

The typical modern vehicle may comprise of several network components like Sensors, Electronic Control Units (ECU's), actuators and many communication related devices. Sensors basically helps in perceiving the surrounding environment and to stimulate the driver functions based on the surrounding environment. Next coming to ECU's. These control units will be having many features and these features will be grouped into subnetworks and these subnetworks will be interconnected through many gateways. Basically, ECU's communicate through a device called as Controller Area Network (CAN). This CAN device acts as a Network protocol for in-vehicle communication.

Many features of CAN like Low cost, reliable and some fault tolerable property enables programmers or architects to use CAN as a standard measure for in-vehicle communication. Since CAN can be used as a standard measure for communication purposes, it is more prone to Cyber-attacks. The major loophole in this CAN protocol is that it lacks message authentication and broadcast transmission. An intruder who wants to surface an attack on the vehicle, it can be done easily by sending a message through CAN after having access to it. Since CAN does not have a policy to authenticate the origin, Intruder can easily perform an attack on the vehicle.

Basically, vehicles are more prone to cyberattacks, because these vehicles are not designed keeping security requirements in place. So, in order to avoid vehicles from being affected by Cyber-attacks, an encryption algorithms or access control mechanisms are incorporated in some modern connected vehicles. One such mechanism incorporated in recent vehicle technology is Intrusion detection systems (IDS). Intrusion detection system provides certain security measures and also will be able to detect certain potential cyber threats affecting intra-vehicle system. This paper focuses on certain challenges and issues of Intra-vehicle IDSs and also on the categories of intra-vehicle IDSs.

II.INTRA-VEHICLE NETWORKS

Intra-Vehicle networks in vehicle communication facilitates data sharing and communication among sensors, actuators and ECU's, which enables the operation among vehicles. There are five widely used intra-vehicular networks in intra-vehicle communication systems.

- Local Interconnection Network (LIN)
- CAN
- FlexRay
- Ethernet
- Media Oriented Systems Transport (MOST)

Local interconnection Networks (LIN) have a low fault tolerance capability and also has a lower bandwidth compared to Ethernet, FlexRay and other intra-vehicle communication systems, whereas other intra-vehicle communication systems like FlexRay, Ethernet and CAN have higher bandwidth also these are more reliable for bandwidth demanding applications. FlexRay is widely used as Safety Radars and ethernet and MOST are used in Infotainment systems. CAN is most widely used among all the above Intra-vehicular communication system, as it is reliably low cost and has showcased acceptable performance and highly fault tolerant.

The major advantage of CAN is that it doesn't require any global synchronization to regulate the vehicle communication. This is possible because of transmission nodes present inside CAN which triggers sending and receiving of messages with respect to communication of Vehicle. CAN uses Bus topology and reception filter of each node present inside CAN decides upon which message needs to be sent to vehicle based on the ID.CAN allows the usage of Carrier Sense multiple access with collision avoidance protocol (CSMA/CD) ,when multiple nodes wants to transmit the messages to vehicle.

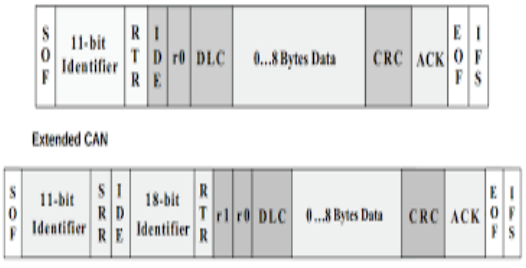

Figure 1: Standard CAN Frame Format

The Figure 1 shows the Standard and Extended Frame format of CAN. A CAN frame consists of seven fields as follows:

- SOF (Start of Frame): This fields indicates the start of the Transmission of all nodes.
- Arbitration Field: This field has 2 sub fields names Identifier Field and RTR (Remote Transmission Request) field. The Identifier field represents the ID of the message/Frame used during transmission process and RTR field will be determined according to the kind of CAN frame.
- Control Field: It has two reserved bits and four Data Length Code (DLC).
- Data Field: This field has the information regarding the actual data being used or transferred to other nodes.
- CRC Field: This field is error detection and correction field which basically validates the messages. All the nodes verify the received messages using this code.
- ACK Field: This field sends an acknowledgement when it receives a valid message or node.
- EOF (End of Frame): This field indicates the end of CAN frame format.

III. INTRUSION DETECTION SYSTEMS(IDSs) for INTRA-VEHICLE NETWORKS

There are multiple mechanisms encountered against Cyber threats which may include few security countermeasures like Encryption algorithms and access control mechanisms in order to ensure vehicle safety. These countermeasures would protect the vehicle from external cyber threats but will be having very limited capability towards protecting the vehicle from internal cyber-attacks. In order to provide vehicle safety from both external and internal cyber-attacks, a reactive countermeasure like IDSs (Intrusion detection systems) is being employed. Intrusion- Detection systems are categorized into 2 types namely:

- Knowledge based IDS
- Behavior/anomaly-based IDS

Knowledge based IDS basically uses signatures or patterns to compare the existing attacks with the known attacks. This category of IDS triggers an intrusion or alarms an intrusion when there is a match among the existing/observed attack with the known attacks. The Knowledge based IDS has a low false positive rate, since it only reacts to previously known attacks(not able to recognize any new attack other than the known attack).One more challenge with

Knowledge based IDS is that the Signature database must be updated as and when the new attacks arose.
Anomaly based intrusion detection system identifies the attack based on the significant behaviour of the system. If there is a significant deviation from the normal behaviour of the system, then this category of IDS employs an intrusion indicating malicious behaviour in the operation of the system. This category of IDS does not depend on any Signature or a pattern for an attack. Anomaly based detection system requires less memory compared to knowledge-based intrusion detection system.

IV. CATEGORIES OF INTRA-VEHICLE IDSs

Intra-vehicle IDSs are categorized into 3 types namely as shown in the Figure 2.

- Flow Based IDS
- Payload based IDS
- Hybrid based IDS

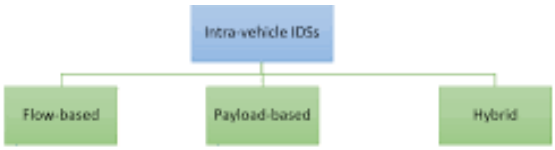

Figure 2: Categories of IDSs

Flow based IDS category of Intrusion-Detection system monitors the internal network of a vehicle. Flow based IDS typically focuses on CAN bus and tries to extract certain features related to message interval and message transmission frequency from the messages being transmitted on the network. Later Flow based IDS uses these features to identify the distinguished or abnormal behaviour of the vehicle system from the normal behaviour. This type of IDS will not verify the payload/information of the messages.
Payload based IDS examine the payload (Content/Information) of the messages to identify abnormal behaviour in the vehicle called Intrusions.
Hybrid based IDS is a combination of the above 2 categories of Intrusion detection systems. In this type of IDS each ECU registers with other ECU's by sending a frame of point called Domain-Activation-Frame. The registered ECU scans the CAN messages and looks for the Forged messages which would have been sent by any malicious entity. The registered ECU's will delete the forged messages before it triggers an Intrusion on vehicle. Later, again the Registered ECU's will start sending a Domain-Activation-Frame.

Intrusion detection system depends on certain observations on data entities or data sets.

- FEATURES and FEATURE SELECTION-Each and every intrusion detection system will maintain a dataset, where-in this dataset consists of certain instances and data records, these data records or instances will be in the form of certain events, objects or processes. Each instance of events or objects is characterized by certain set of features. These instances of features will be able to detect the intrusion among normal or the abnormal behavior of the system. The Feature selection could be based on two types of namely Physical Features and Cyber Features. Physical features of intrusion detection system describe the physical state of the system, whereas Cyber features describes the data or communication aspects of the system. Feature selection can be done manually and automatically too. Sometimes it would be a tedious task doing manually because it might require deep understanding of the data, and how that data could be used to solve the problem of several intrusions, in such cases automatic methods are taken up.
- DATASETS- An appropriate dataset is required in order to understand several scenarios of intrusions. There are several types of datasets namely Real data and simulated data. Real datasets refer to the type of data extracted from test vehicles, whereas simulated data refers to the type of data obtained by simulation or by prototyping (not obtained by any particular /definite source).
- ATTACKS IN AUTONOMOUS VEHICLES - Connected /autonomous vehicles are prone to large number of Cyber-attacks. Generally, these attacks are classified as Passive and Active attacks. Passive attacks would break the integrity/ confidentiality of system's security which could lead to leakage of Information (Privacy Leakage). Active attacks could probably lead to the control of certain primary functionality of the system by insertion, deletion or modification of the messages. The following are some of the attack

types which affect intra-vehicle communication system.

1. DENIAL OF SERVICE ATTACKS (DoS)- Basically this attack in the name only suggests that, it disrupts the normal functionality of services. This could probably lead to the prevention of private or important information related to safety warnings of vehicle. In CAN, it might avoid the ECU from transmitting high priority legitimate messages related to Vehicle safety. An attacker with limited knowledge can easily launch DoS attack on vehicles.
2. REPLAY ATTACK (Message Injection)-In this type of attack, an attacker gains an access to ECU and will be having complete control over it. When the attacker is having complete control over ECU, he/she can inject fabricated message (malicious messages).
3. MANIPULATION OF MESSAGES-This attack implies that there is no integrity of the messages; it means that messages will be modified and even messages can be deleted. Attacker can easily modify the content of the messages. The attacker can modify the content of the message which has to reach CAN by different ECU's. One of the sub-attacks under message manipulation is Deletion attack whereas entire message will be deleted from the buffer.
4. MASQUERADE ATTACK- This attack is known as Impersonation attack. For an instance attacker tries to know the ID of the CAN bus and also gets the information regarding ECU's transmitting messages. If ECU A and ECU B are both sending a message to CAN to establish a communication, attacker might impersonate as ECU by its ID and frequency and could send the communication details on behalf of A. Here, attacker is impersonated as ECU A.
5. MALWARE ATTACK- Malwares can be in any form like Viruses, worms and many more. This form of malwares can be injected into the systems by exploiting the vulnerability of the system. These viruses and worms can be injected into CAN or any particular system say for an instance, malwares to CAN will be activated, whenever an infotainment system starts playing the music.

ROLE OF IDSs IN SECURING AUTONOMOUS VEHICLES- The main role of IDS is to identify the generation of attacks using a file called Trace file, where it contains complete information regarding CAN communication signals. So these trace files will be used as auditable file to know the generation and impact of the attack too. IDSs also use datasets and features and feature selection mechanism to identify the attacks on connected vehicles. IDS has a taxonomy of process on CAN as shown in the Figure 3.

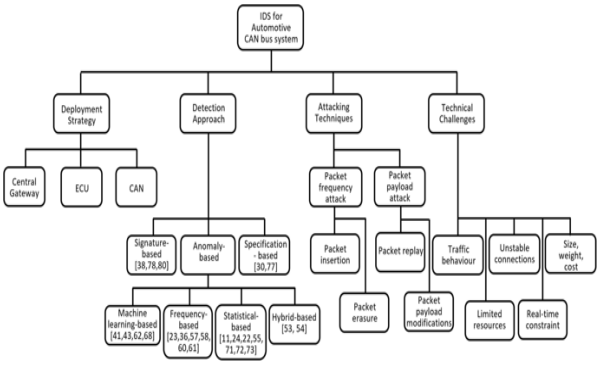

Figure 3: IDS taxonomy for CAN

IDS can be deployed in possible locations of CAN such as CAN, ECU's and gateways. IDS evaluates the sensitivity and effectiveness of attacks occurring on CAN bus and thus reducing certain high impact of these attacks. Several results have suggested that IDS approach is a practical approach in detecting malicious attacks on CAN network.

V. CONCLUSION

Modern day autonomous vehicles are more susceptible to various cyber-threats by eventually providing access to attackers to control the vehicles. Though certain conventional mechanisms provide security against certain cyber-attacks, but usually not applicable to intra-vehicle networks. IDSs represent an essential component of vehicle security. IDSs uses various criterions like Features, feature selection, Datasets, and certain performance metrics to analyse the impact of attack on CAN and to overcome the attack impact on CAN networks of vehicle systems. Using anomaly-based approach and signature-based approach of IDS, attacks can be detected based on patterns or signatures or also content/payload. Intrusion detection system has become the most holistic approach in providing security mechanisms to connected vehicles. Certainly, every proposed methodology will be having further research developments in order to overcome the existing flaws.

IDS can definitely examine the cyber features but fails to recognize the context of the data. This feature could be achieved by using ML-based approach, which looks like a promising candidate for intrusion detection system.

REFERENCE

[1] S. Han, M. Xie, H. H. Chen, and Y. Ling, ``Intrusion detection in cyber physical systems: Techniques and challenges," *IEEE Syst. J.*, vol. 8, no. 4, pp. 1052_1062, Dec. 2014.

[2] Omar Y. Al-Jarrah, Carsten Maple, Mehrdad Dianati, David Oxtoby, And Alex Mouzakitis, “Intrusion-detection system for Intra-vehicle system: A review”, IEEE access, 2019, pg.21266-21289.

[3] Jonathan Petit and Steven E. Shladover,” Potential Cyber-attacks on automated vehicles”, IEEE Transactions on Intelligent Transportation System, 2014, p9 1-11.

[4] Cybersecurity in Automotive, a white paper, Altran technologies.