Securing In-Vehicle Control Networks: A Comprehensive Survey of CAN and its Variants

***Abstract*—Abstract – Automotive control networks, anchored by the Controller Area Network (CAN) and its variants, con- stitute the digital backbone of modern vehicles, overseeing a spectrum of critical functions. As the automotive industry embraces connectivity and automation, the security of in-vehicle control networks emerges as a paramount concern. Potential cy- berattacks on these networks can have far-reaching consequences, from compromising privacy to jeopardizing vehicle safety. This project conducts an in-depth examination of recent attacks on automotive networks, encompassing CAN, Local Interconnect Network (LIN), and FlexRay, to identify enduring vulnerabilities and quantify the computational and communication resources required for potential assailants. The insights gained from this analysis will inform the development of advanced security mea- sures, enhancing the integrity of in-vehicle control networks and fortifying the safety and reliability of modern automobiles.**

**Project Focus:**

**This project focuses on reviewing recent attacks on automotive networks, including CAN and its variants. The goal is to identify remaining vulnerabilities and assess the computational and communication resources required for the success of potential attacks. Understanding the threat landscape and quantifying the resources needed for attacks is essential for designing robust security measures to protect in-vehicle control networks against cyber threats.**

**In conclusion, automotive control networks are the techno- logical backbone of modern vehicles, enabling seamless commu- nication between diverse ECUs. Securing these networks is of paramount importance, and this project aims to address this crucial challenge by exploring recent attacks and enhancing the security of in-vehicle control networks.**

***Index Terms*—Automotive Control Networks, Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, Cybersecurity, Attack Vectors, Vulnerabilities, Threat Landscape, Security Measures, InVehicle Control Networks Project Focus:**

1. INTRODUCTION

*A. Overview of Automotive Networks*

Automotive networks are the intricate web of communi- cation protocols that connect electronic control units (ECUs) within a vehicle. The Controller Area Network (CAN) serves as the backbone, facilitating real-time data exchange for crit- ical functions, including powertrain control, safety systems, infotainment, and more. Alongside CAN, alternative protocols like Local Interconnect Network (LIN) and FlexRay cater to specific requirements. The central challenge lies in securing these networks against cyber threats, as vulnerabilities could lead to unauthorized access, data manipulation, or system compromise. This project delves into recent attacks, assessing remaining vulnerabilities, and gauging the computational and communication resources required for potential breaches, ulti- mately reinforcing the security of automotive control networks. The significance of security in automotive networks cannot be overstated, as it stands at the crossroads of safety, privacy,

and the future of transportation. In an era marked by rapid technological advancement, modern vehicles are no longer merely mechanical marvels; they are complex digital ecosys- tems on wheels. These vehicles rely on intricate networks of electronic control units (ECUs) and sensors to manage everything from engine performance and safety systems to in- fotainment and connectivity. While this digital transformation promises greater convenience and efficiency, it also ushers in a new era of cybersecurity challenges. The integrity of in- vehicle control networks is a linchpin in ensuring the safety of occupants, the privacy of data, and the reliability of the automotive industry. This discussion explores the multifaceted significance of security in automotive networks, shedding light on the critical factors that underpin the imperative need for robust and comprehensive cybersecurity measures.

The significance of security in automotive networks cannot be overstated, and it encompasses a range of critical aspects:

1. Safety: Safety is paramount in the automotive industry. Vehicles rely on numerous electronic control units (ECUs) and sensors to ensure safe operation, control critical functions like braking and acceleration, and provide life-saving features such as airbags. Ensuring the security of in-vehicle control networks is essential to prevent unauthorized access or tampering that could compromise these safety systems, potentially leading to accidents and injuries.
2. Privacy: Modern vehicles collect and process a wealth of data, including driver behavior, location information, and entertainment preferences. Protecting the privacy of vehicle occupants is crucial, as data breaches can lead to unauthorized access and misuse of personal information.
3. Functional Integrity: In-vehicle control networks manage an array of functions, from engine performance to infotainment systems. Tampering with these systems can lead to a loss of functionality, inconvenience, and economic loss for vehicle owners.
4. Economic Impact: Security breaches in automotive networks can have severe economic consequences. These breaches can lead to costly recalls, damage a manufacturer’s reputation, and result in potential legal liabilities.
5. Liability and Regulation: As vehicles become more connected and automated, the issue of liability in the event of accidents or cyberattacks becomes complex. Manufacturers must take steps to secure their products and comply with evolving cybersecurity regulations.
6. Consumer Trust: Trust is a crucial element in the auto- motive industry. Security breaches can erode consumer trust in both vehicle manufacturers and the technology powering modern vehicles. A lack of trust can hinder the adoption of advanced technologies.
7. Cybersecurity Threat Landscape: The threat landscape is constantly evolving, with new attack vectors and vulner- abilities emerging. The automotive industry is a high-profile target for cybercriminals, making it imperative to stay ahead of potential threats.
8. National Security: Vehicles are not just modes of personal transportation; they have vital roles in critical infrastructure, emergency services, and government operations. Breaches in automotive networks can have national security implications.
9. Advanced Technologies: The integration of ad- vanced technologies like autonomous driving and vehicle-to- everything (V2X) communication further emphasizes the need for robust cybersecurity. The failure of such systems due to security breaches can result in accidents and loss of life.
10. OVERVIEW OF CAN, LIN, AND FLEXRAY NETWORKS Security Challenges:

Securing automotive networks is paramount due to the potential implications of cyberattacks. Threats include unau- thorized access, data manipulation, and system compromise. Attack vectors may exploit software vulnerabilities, hardware weaknesses, or weak network segmentation. Given the criti- cality of vehicle functions, any security breach can lead to dire consequences, ranging from loss of privacy to physical harm.

Security Solution:

Controller Area Network (CAN) and its alternatives, namely Local Interconnect Network (LIN) and FlexRay, play a pivotal role in the automotive and industrial automation industries due to their distinct characteristics and applications. Here’s a dis- cussion on the importance and usage of these communication protocols:

*A.*

* 1. *Controller Area Network (CAN : Description and Tech- nical Features:* Controller Area Network (CAN): CAN is a widely used communication protocol known for its robustness and efficiency. Its importance and usage in various domains are as follows:

Automotive Industry: CAN is the backbone of automo- tive networks, facilitating real-time communication between electronic control units (ECUs) that control various vehicle functions. It ensures the seamless operation of engine control, powertrain management, safety systems, and more.

•

Industrial Automation: CAN is not limited to the automo- tive sector. It is employed in industrial automation, connecting PLCs, sensors, and actuators. Its determinism and reliability make it suitable for time-sensitive industrial processes.

•

Cost-Efficiency: CAN is cost-effective, making it a pre- ferred choice for applications where high-speed data transfer is not critical. It strikes a balance between performance and cost, which is essential in industries like automotive manufacturing. The Controller Area Network (CAN) is an essential part of vehicle communication systems. Initially developed by Bosch in the 1980s for automotive applications, CAN has since become a standard in various industrial control environments. The primary purpose of CAN is to allow multiple microcon- trollers and devices within a vehicle to communicate with each

•

other without requiring a central computer. This feature makes it highly effective in managing complex operations where multiple subsystems need to interact seamlessly.

Technically, CAN is distinguished by its method of trans- mitting messages in a robust and efficient manner. Its message- based protocol, as opposed to address-based, allows the net- work to prioritize messages based on their content rather than their source or destination. This prioritization is vital in automotive applications where certain data, such as brake signals, must take precedence over less critical information.

CAN operates at speeds up to 1 Mbps, although this speed can vary depending on the network’s length and the electromagnetic environment. The network is characterized by a multi-master design, where any node can transmit data if the bus is free. This approach significantly enhances the system’s flexibility and responsiveness. The network’s physical layer usually consists of two wires forming a twisted pair, which helps in reducing electromagnetic interference. This robust design enables the CAN network to function reliably in the harsh electrical environments of vehicles. Additionally, CAN’s error handling capabilities are sophisticated, featuring error detection mechanisms like frame check, bit monitoring, and acknowledgment, as well as fault confinement to prevent faulty nodes from disrupting the entire network.

In terms of security, while CAN provides robust data transmission, it was not designed with security features to prevent malicious attacks. This lack of inherent security has become a concern in modern automotive systems, where the threat of cyberattacks is rising.

* 1. *Local Interconnect Network (LIN : Description and Technical Features:* Local Interconnect Network (LIN): LIN is an alternative to CAN with its own set of importance and applications:

Supplement to CAN: LIN is often used in conjunction with CAN in vehicles. It complements CAN by handling non-critical, low-speed functions like interior lighting, climate control, and infotainment systems. This ensures that CAN resources are reserved for critical tasks.

•

Cost Reduction: LIN is a cost-effective option for ap- plications that don’t require the real-time performance of CAN. Its simplicity and lower data rates reduce hardware and implementation costs.

•

Energy Efficiency: LIN is designed with energy efficiency in mind, making it suitable for functions that must run con- tinuously with minimal power consumption.

•

The Local Interconnect Network (LIN) is a simpler, more cost-effective alternative CAN designed for less critical com- munication tasks within vehicles. Developed in the late 1990s, LIN is primarily used for managing simple actuators and sensors, such as mirror adjustments, seat positions, and rain sensors.

LIN operates as a single-master, multiple-slave network, where a central master unit controls the communication with several slave nodes. This architecture simplifies the network design and reduces costs, making LIN an ideal choice for simpler and lower-speed applications. The communication speed in a LIN network is typically around 20 kbit/s, which is sufficient for the non-time-critical tasks it handles. A notable

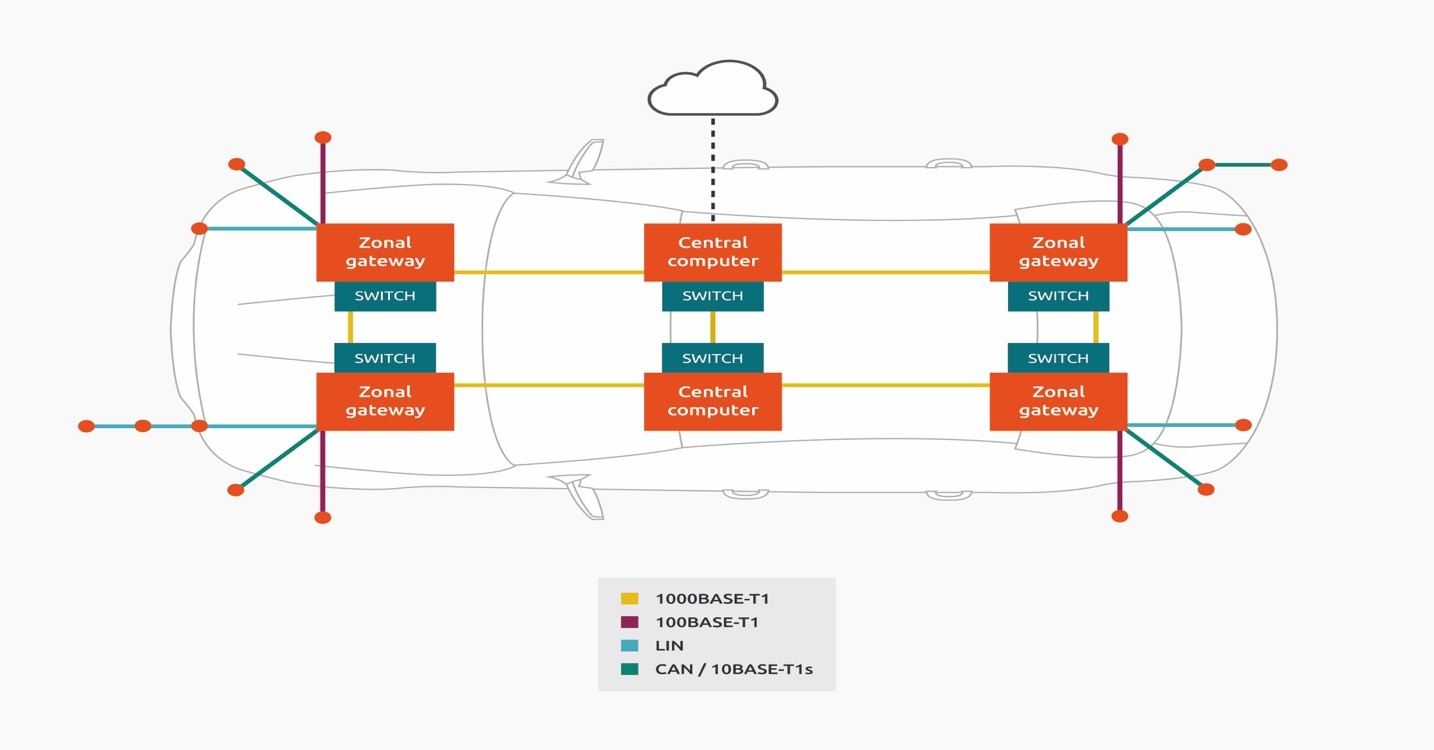


Fig. 1.

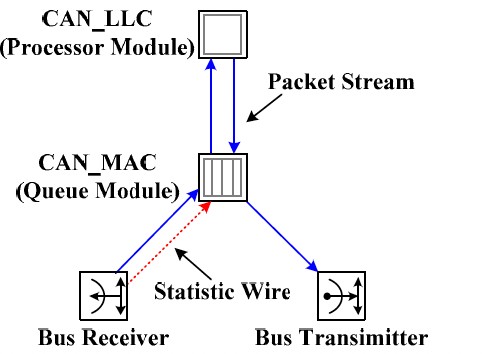


Fig. 2. CAN NODE Architecture

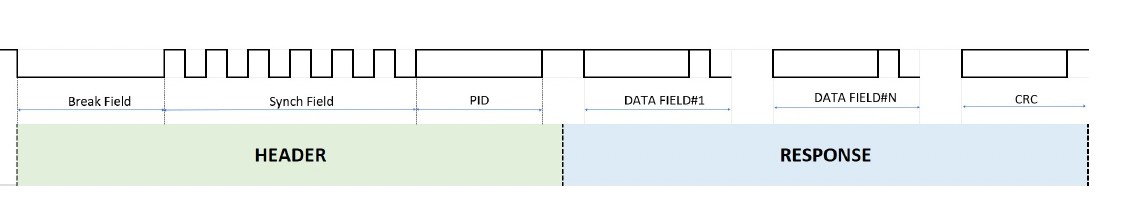


Fig. 3. LIN Frame

feature of LIN is its single-wire design, contrasting with the two-wire design of CAN. This single-wire approach, combined with the lower data rates, results in significant cost savings and simplicity in wiring. However, this design also means that LIN is less robust against electromagnetic interference compared to CAN.

While LIN is not as advanced as CAN in terms of speed and error handling, it serves its purpose well in providing a lightweight communication protocol for less critical applica- tions in vehicles. LIN often works in conjunction with CAN, where LIN handles less critical tasks, and CAN manages more demanding communication requirements. The simplicity of LIN also extends to its security aspects. Since LIN is used in less critical functions, the security risks are generally lower. However, as with CAN, the increasing connectivity of automotive systems raises the need for improved security measures in LIN networks as well.

* 1. *FlexRay: Description and Technical Features:* FlexRay: FlexRay is a high-speed communication protocol that serves specific high-performance applications:

Advanced Driver Assistance Systems (ADAS): FlexRay is crucial for real-time, safety-critical functions in advanced driver assistance systems, like adaptive cruise control and lane- keeping assistance. It provides the necessary determinism and redundancy for these applications.

•

Time-Critical Systems: FlexRay is used in applications where timing precision is paramount, such as in aviation and aerospace systems, medical devices, and advanced robotics.

•

Redundancy and Fault-Tolerance: FlexRay’s dual-channel design ensures redundancy and fault-tolerance, making it suit- able for critical applications where system failure is not an option.

•

FlexRay is the most advanced protocol among the three, designed to cater to the needs of complex and safety-critical systems in modern vehicles. Developed in the early 2000s by a consortium of automotive companies and suppliers, FlexRay addresses the limitations of CAN and LIN in handling high-speed and reliable communication required in advanced applications like x-by-wire systems.

FlexRay boasts a data transmission rate of up to 10 Mbps, which is significantly higher than both CAN and LIN. This high data rate enables it to support complex control systems such as advanced braking, steering, and driver-assistance sys- tems that require rapid and precise data transmission. One of the defining features of FlexRay is its support for both time- triggered and event triggered.

Controller Area Network (CAN) is a widely used commu- nication protocol in various industries, and it serves as the backbone for many applications. In Automotive industry, CAN is extensively used in modern vehicles for various purposes, such as engine control, transmission control, airbag systems, anti-lock braking systems (ABS), entertainment systems, and more. It enables different electronic control units (ECUs) to communicate with each other.

Controller Area Network (CAN) in the automotive industry can be classified into three generic groups based on their functions and the security concerns they pose:

1. VEHICLE CONTROL AND SAFETY: Powertrain Control: Includes the control of the engine and

transmission and is crucial for vehicle performance and safety. Chassis Control: Manages functions like anti-lock braking systems (ABS) and electronic stability control (ESC), directly

•

•

impacting vehicle stability and safety.

Airbag and Safety Systems: Focuses on the security of systems critical to passenger safety, such as airbags, seatbelt tensioners, and collision detection.

•

Advanced Driver Assistance Systems (ADAS): Encom- passes safety-critical features like adaptive cruise control and lane-keeping assistance that require secure communication to ensure safe driving.

•

1. VEHICLE ACCESS AND SECURITY:

Body Control: Involves access control and security for vehicle doors and lighting systems, which are essential for vehicle security.

•

Instrument Cluster: Ensures that the data displayed to the driver is accurate and reliable, affecting the driver’s under- standing of the vehicle’s status.

•

1. VEHICLE MAINTENANCE AND DIAGNOSTICS: Diagnostic and Maintenance: Focuses on the security of

diagnostic and maintenance systems, which are important for vehicle health checks, maintenance, and data privacy.

1. *Comparison of Functionalities and Use Cases*
2. *1Performance and Speed*
3. CAN NETWORK:

The Controller Area Network (CAN) offers a performance level that balances speed and reliability. Its maximum data transfer speed of up to 1 Mbps is well-suited for moderate- speed applications. This speed facilitates real-time commu- nication critical for several functions in vehicles, such as engine management and airbag deployment. The speed of CAN ensures a timely response to various sensor inputs, a crucial factor in automotive safety systems.

1. LIN NETWORK:

The Local Interconnect Network (LIN) is designed for lower-speed applications, with a maximum data rate of ap- proximately 20 kbit/s. This speed suffices for its intended applications, which involve non-critical vehicle functions such as controlling door locks, windows, or mirror adjustments. LIN’s lower speed is a trade-off for its simpler and more cost- effective design, making it an ideal choice for less demanding communication tasks within a vehicle.

1. FLEXRAY NETWORK:

FlexRay stands out with its superior performance, offering data rates up to 10 Mbit/s. This high-speed capability is es- sential for advanced vehicle applications that require rapid and precise data transmission, such as advanced driver-assistance systems (ADAS) and brake-by-wire systems. FlexRay’s speed enables more complex and safety-critical applications, setting it apart from CAN and LIN.

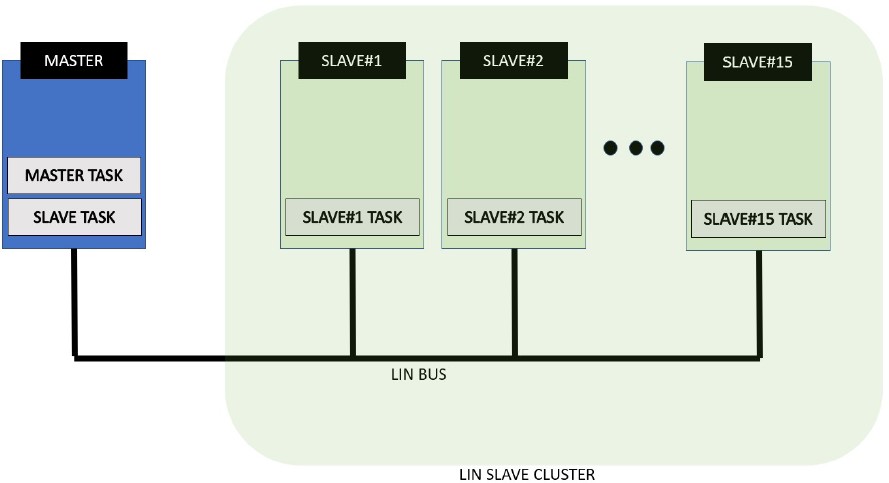


Fig. 4. LIN Bus

*A.*

* 1. *Reliability and Error Handling:*
  2. *CAN Network::* CAN networks are renowned for their robust error handling and fault confinement mechanisms. These features are integral to maintaining the network’s integrity, especially in an automotive environment where reliability is paramount. The CAN protocol includes error detection through mechanisms like cyclic redundancy check (CRC), frame check, and acknowledgment, as well as fault confinement to isolate faulty nodes, thus ensuring reliable communication even in harsh conditions.
  3. *LIN Network::* While LIN is less complex than CAN, it also offers basic error detection capabilities. However, it lacks the advanced error handling and fault confinement features of CAN. This limitation is acceptable given LIN’s role in managing less critical vehicle functions, where the demand for ultra-reliable communication is lower.
  4. *FlexRay Network::* FlexRay provides the most advanced error handling and fault tolerance among the three. Its design includes sophisticated error detection and correction mech- anisms, ensuring data integrity and consistent performance. This reliability is vital for the network’s target applications, which include the most critical and safety-sensitive systems in a vehicle.
  5. *Cost and Complexity:*
  6. *CAN Network::* CAN strikes a balance between perfor- mance and cost, making it a popular choice in the automotive industry. Its design is more complex and costly than LIN but less so compared to FlexRay. The widespread adoption of CAN has also led to the availability of cost-effective components, further reducing the overall cost of implementing CAN networks.
  7. *LIN Network::* LIN is the most cost-effective and sim- plest among the three networks. Its design focuses on min- imalism and efficiency, reducing both hardware complexity and cost. This simplicity makes LIN an attractive option for vehicle manufacturers to integrate basic control functions without significantly increasing the vehicle’s cost.
  8. *FlexRay Network::* FlexRay’s advanced capabilities come at a higher cost and increased complexity. The network’s design, catering to high-speed and highly reliable communica- tion, requires more sophisticated and therefore more expensive components. This cost is justified for applications where performance and reliability cannot be compromised, such as in high-end vehicle control systems.
  9. *Specific Use Cases:*
  10. *CAN Network::* CAN is extensively used in various applications within vehicles, including engine control units (ECUs), anti-lock braking systems (ABS), airbags, and power steering systems. Its reliability and speed make it suitable for these critical applications, where failure or delay in data transmission can have significant consequences.
  11. *LIN Network::* LIN is primarily used for simpler con- trol tasks in vehicles, such as controlling the interior lighting, air conditioning, infotainment systems, and seat adjustments. Its role is to manage functionalities where the speed and reliability requirements are not as stringent as those in critical control systems.
  12. *FlexRay Network::* FlexRay is deployed in the most demanding applications in modern vehicles, such as active sus- pension systems, advanced ADAS, and drive-by-wire systems. These applications require the high data rates and reliability that FlexRay offers, as they are critical to vehicle safety and performance.

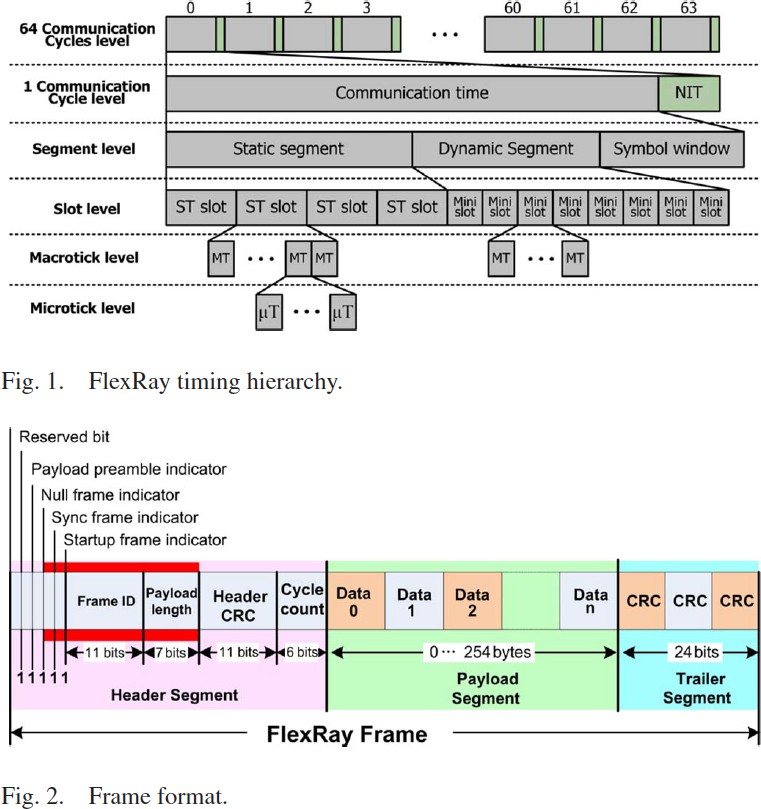


Fig. 5. FlexRay Timing Heirarchy

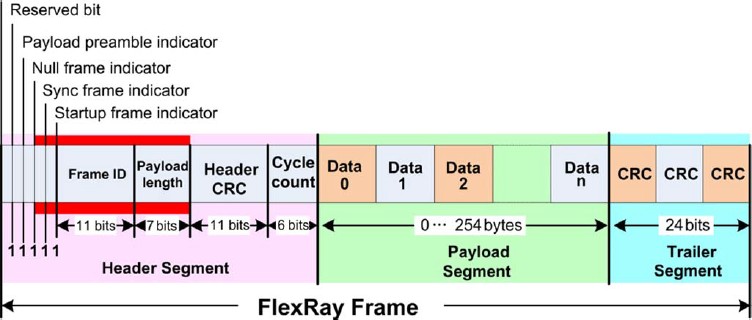


Fig. 6. FlexRay Frame Format

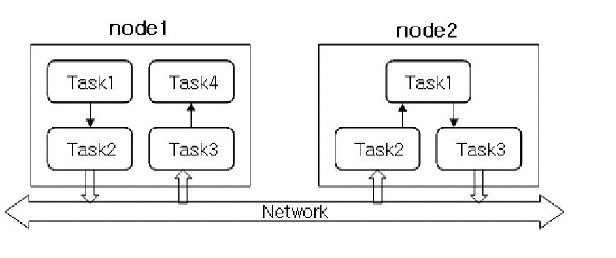


Fig. 7. CAN base model for Integration to other applications.

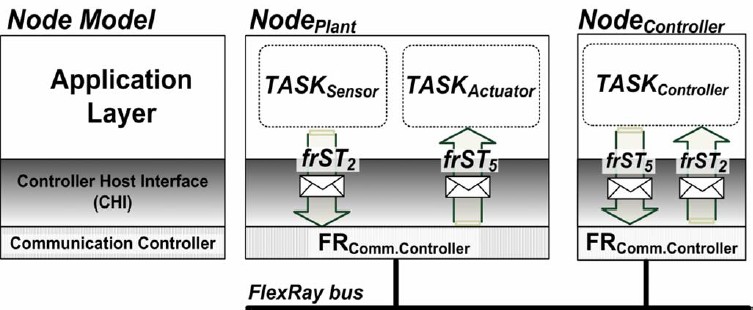


Fig. 8. FlexRay System Model

In summary, each network – CAN, LIN, and FlexRay – has distinct characteristics making them suitable for specific applications within automotive and industrial control systems. Their differences in speed, reliability, cost, and complexity cater to a wide range of requirements, from basic control functions to the most advanced and critical vehicle systems.

1. *Security Concerns and Challenges in Each Network Type*
2. *CAN Network: Vulnerabilities and Security Measures*

The Controller Area Network (CAN) is widely used in auto- motive and industrial control systems due to its robustness and reliability. However, when it comes to security, CAN presents several vulnerabilities primarily because it was not designed with modern cybersecurity threats in mind. CAN’s open design allows for any device on the network to listen to all traffic and send messages without any form of authentication. This openness, while beneficial for efficient communication, makes it susceptible to a range of attacks, including eavesdropping, message injection, and Denial of Service (DoS) attacks.

One of the most significant vulnerabilities of CAN is its lack of encryption and authentication mechanisms. Without these security measures, attackers can easily intercept and manipulate data, potentially causing hazardous situations, es- pecially in automotive contexts where CAN is used for critical control systems. For instance, an attacker could potentially

take control of a vehicle’s braking or steering system by injecting malicious messages onto the CAN network.

To address these vulnerabilities, several security measures have been proposed and implemented. One approach is the use of hardware-based security modules that provide encryption and secure authentication of messages. These modules ensure that only authorized devices can communicate on the network and that the data they transmit is protected from interception and tampering.

Another solution is the development of intrusion detection systems (IDS) specifically for CAN networks. These systems monitor network traffic for signs of unusual or malicious activity. Using a combination of anomaly-based and signature- based detection techniques, these IDS can identify potential threats and trigger alerts or countermeasures.

Furthermore, advancements in secure CAN protocols are being made, adding layers of security to the existing CAN standard. These enhancements include message authentication codes (MACs) and encrypted payloads, which significantly increase the difficulty for attackers to successfully compromise the network.

Despite these efforts, securing CAN networks remains a challenge due to the need to balance security with the net- work’s inherent design and performance requirements. Imple- menting robust security measures often involves additional costs and complexity, and can impact the network’s latency

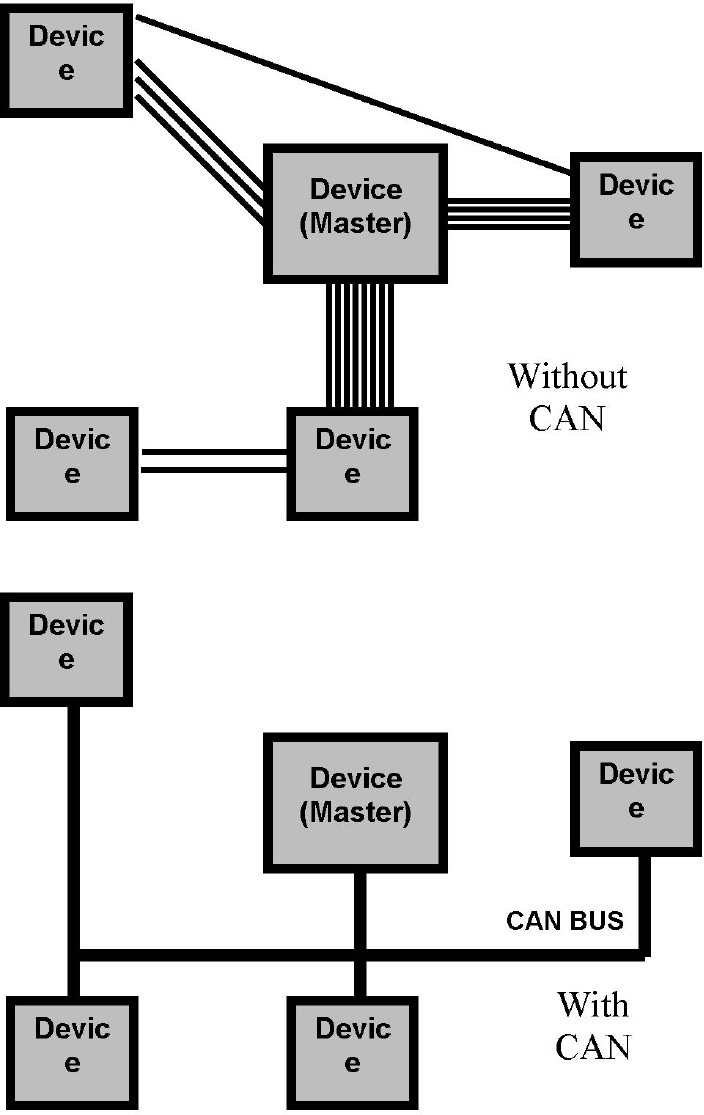


Fig. 9. Cost Effective CAN Implementation

TABLE I

**Feature CAN Network LIN Network FlexRay Network**

**Performance and**

**Speed Reliability and Error Handling Cost and Complexity**

Up to 1 Mbps, suitable for

moderate-speed applications. Strong error handling and fault confinement mechanisms.

Balanced cost; more complex than LIN but less than FlexRay.

Approximately 20 kbit/s, designed for

lower-speed, non-critical functions.

Basic error detection; less robust compared to CAN.

Most cost-effective and simple; minimal hardware complexity.

Up to 10 Mbit/s, ideal for

high-speed, complex applications. Advanced error detection and correction; highest reliability.

Higher cost and complexity due to advanced capabilities.

**Specific Use Cases** Engine control units, ABS, airbags,

power steering.

Interior lighting, air conditioning, infotainment systems, seat adjustments.

Active suspension, advanced ADAS, drive-by-wire systems.

and throughput.

FIG.Anomaly Sequence tree FIG. Anomaly detection flow diagram

1. *LIN Network: Vulnerabilities and Security Measures*

The Local Interconnect Network (LIN) is simpler and less expensive than CAN, making it suitable for less critical control applications in vehicles. However, this simplicity also means that LIN comes with its own set of security vulnerabilities. Similar to CAN, LIN lacks built-in security features like encryption and authentication, making it vulnerable to similar types of attacks, such as message interception and unautho- rized message transmission.

However, the impact of security breaches in LIN networks is typically less severe than in CAN networks due to the nature of the applications LIN controls. For instance, compromising a LIN network might allow an attacker to manipulate the vehicle’s windows or air conditioning system, which, while inconvenient, is generally not as hazardous as taking control of more critical systems managed by CAN.

Nevertheless, the security of LIN networks should not be overlooked, especially considering how interconnected vehicle systems are becoming. A vulnerability in a LIN network could potentially be exploited as a gateway to access more critical systems, especially in vehicles where LIN and CAN networks are integrated.

To mitigate these risks, the implementation of basic security measures in LIN networks is recommended. These measures include simple cryptographic techniques for message authenti- cation and ensuring secure initialization and pairing of devices on the network. Additionally, regular security assessments and updates are crucial to protect against emerging threats.

The challenge with implementing security in LIN networks lies in maintaining the network’s low-cost and simplicity. Adding advanced security features can increase the cost and complexity of LIN systems, contradicting their original pur- pose. Therefore, security measures for LIN networks must be carefully designed to be effective yet not overly burdensome.

1. *FlexRay Network: Vulnerabilities and Security Measures*

FlexRay is known for its high data rates and reliability, making it suitable for critical control applications in vehi- cles. However, with these advanced capabilities come more complex security challenges. FlexRay’s use in safety-critical systems means that any security breach could have severe

consequences, such as compromising the vehicle’s braking or steering systems.

Like CAN and LIN, FlexRay was not originally designed with strong cybersecurity measures. Its vulnerabilities include the risk of unauthorized access and message manipulation, potentially leading to control of critical vehicle functions. However, given its use in more sophisticated systems, the security requirements for FlexRay are inherently higher.

To address these security concerns, more advanced mea- sures are necessary for FlexRay networks compared to CAN and LIN. These measures include the use of sophisticated encryption algorithms and robust authentication protocols to secure communications. Additionally, FlexRay networks can benefit from more complex IDS that monitor for anomalies or suspicious activities specific to the network’s high-speed and deterministic nature.

Another key aspect of securing FlexRay networks is ensur- ing the integrity of the software running on the devices con- nected to the network. This involves secure boot mechanisms, code signing, and regular software updates to protect against vulnerabilities that could be exploited by attackers.

Moreover, given FlexRay’s complexity and critical appli- cations, a layered security approach is often adopted. This approach involves multiple security layers, including physi- cal security of the network hardware, secure communication protocols, and application-level security measures.

The challenge in securing FlexRay networks lies in achiev- ing the necessary level of security without compromising the network’s performance. Security measures must be efficient and effective, ensuring the integrity and confidentiality of communications while maintaining the network’s high data rates and reliability.

In summary, while CAN, LIN, and FlexRay networks each have distinct applications and characteristics, they share com- mon security vulnerabilities stemming from a lack of inherent security features. Addressing these vulnerabilities requires a combination of hardware and software security measures, tailored to the specific needs and applications of each network. As vehicle systems continue to evolve and become more interconnected, the importance of network security becomes increasingly critical, necessitating ongoing research and de- velopment in this area.

# Security Concerns in Network Types

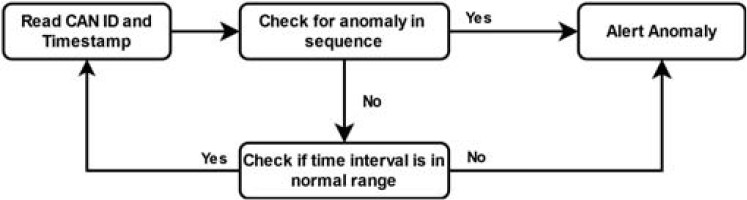


Fig. 10.

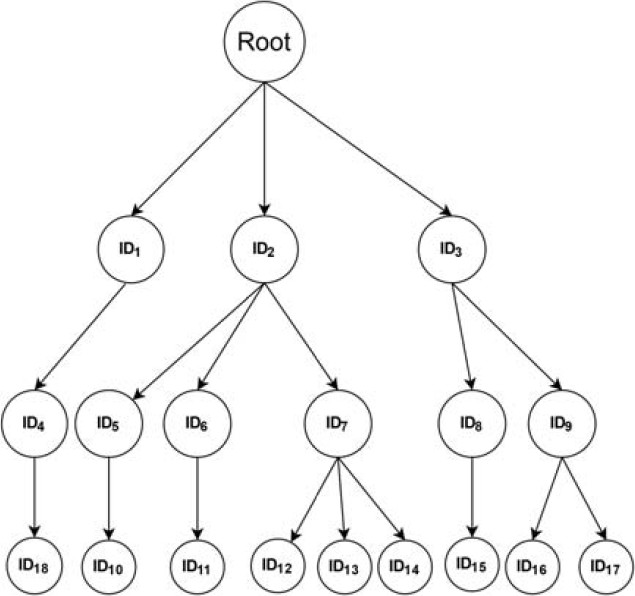


Fig. 11.

**Network Type**

TABLE II

**Vulnerabilities Security Measures**

CAN Susceptible to cyberattacks, lacks encryption and authentication.

Hardware-based security modules, intrusion detection systems, secure CAN protocols.

LIN Similar to CAN but less targeted; simpler use cases. Basic cryptographic techniques, secure device initialization and pairing.

FlexRay Vulnerable due to high complexity and critical applications.

Sophisticated encryption, robust authentication protocols, secure software practices.

1. TECHNOLOGICAL EVOLUTION AND FUTURE PROSPECTS
2. *Advancements in Network Technologies*

The realm of automotive network technologies has wit- nessed substantial advancements over the years, driven by the need for higher performance, enhanced reliability, and improved security. These advancements are not just confined to the hardware components but also extend to software and protocol levels.

CAN Network Evolution: The introduction of CAN FD (Flexible Data-rate) marks a significant advancement in the CAN network domain. CAN FD extends the capabilities of the classic CAN protocol by allowing for higher data rates and larger data fields in messages. This improvement addresses the need for increased bandwidth in modern vehicles, which now incorporate more sensors and execute more data-intensive operations. The evolution of CAN FD is a direct response to the challenges posed by emerging automotive technologies, such as advanced driver-assistance systems (ADAS) and the growing number of electronic control units (ECUs) in vehicles. LIN Network Enhancements: In the case of LIN, the ad- vancements are geared towards refining the robustness and integration with other network types like CAN. The focus has been on enhancing the LIN protocol to support more efficient communication and easier integration in a mixed network environment. These improvements are crucial in maintaining the relevance of LIN in modern vehicle architectures, where

cost-effectiveness and simplicity remain key drivers.

FlexRay’s Progressive Developments: FlexRay continues to evolve, especially in its application in safety-critical and high- performance systems. The advancements in FlexRay tech- nology are centered around increasing data rate capabilities and enhancing its deterministic communication features. Such developments are vital for the support of next-generation au- tomotive applications, including autonomous driving systems, where the need for high-speed data transmission and absolute reliability is paramount.

Cybersecurity Focus: Across all these networks, a critical area of advancement is cybersecurity. As vehicles become more connected and integrated with external networks, the potential for cyber threats increases. This has necessitated the development of sophisticated encryption methods, intrusion detection systems, and secure authentication protocols specif- ically tailored for automotive networks. The challenge is to implement these security measures without compromising on the performance and efficiency of the network.

1. *Future Trends in Vehicle Network Systems*

The future of vehicle network systems is shaped by several emerging trends, prominently influenced by the advancements in technology and changing consumer demands.

V2X Communication: Vehicle-to-everything (V2X) com- munication is expected to become increasingly prevalent. This technology extends the vehicle’s communication capabilities to other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and network (V2N). Such interconnectedness will necessitate vehicle networks that are not only faster and more reliable

but also equipped with robust security protocols to safeguard against potential cyber threats.

Electric and Autonomous Vehicles: The rise of electric and autonomous vehicles is reshaping the requirements for vehicle network systems. These vehicles need sophisticated networks capable of managing large volumes of sensor data and supporting complex decision-making algorithms. This scenario may lead to a shift towards more unified or stan- dardized network architectures to streamline development and integration processes.

Cloud and Edge Computing: The integration of cloud and edge computing in vehicle networks is becoming more promi- nent. These technologies offer potential benefits in terms of efficient data management and enabling new functionalities like real-time traffic updates, predictive maintenance, and ad- vanced navigation systems. The challenge lies in balancing the data processing between on-board systems and cloud services to optimize performance and response times.

# Technological Evolution and Integration

1. INTEGRATION AND INTEROPERABILITY
2. *Interplay Between CAN, LIN, and FlexRay*

The integration of CAN, LIN, and FlexRay in modern vehicles illustrates the trend towards more complex and inter- connected automotive systems. Each network serves specific purposes and needs to function cohesively for optimal vehicle operation. CAN continues to handle a wide range of applica- tions, balancing speed and reliability. LIN complements CAN in managing simpler control tasks, providing a cost-effective solution. FlexRay caters to the most demanding applications with its high data rate and robustness.

This interplay is critical for achieving a holistic vehicle system. For example, while FlexRay might manage critical brake control functions, CAN could handle engine control, and LIN might manage the vehicle’s climate control system. The integration of these networks ensures efficient data sharing and processing, enhancing both vehicle performance and safety.

1. *Challenges and Solutions in Integration*

Integrating diverse networks like CAN, LIN, and FlexRay presents several challenges. Compatibility between different communication protocols is a primary issue. Each network has distinct protocol standards, data rates, and operational charac- teristics, which can complicate seamless communication.

Gateway modules are commonly used to address these challenges. These modules act as intermediaries, translating data between different network protocols and ensuring proper communication between CAN, LIN, and FlexRay networks. Advancements in gateway technology focus on improving the efficiency and reliability of these translations.

Maintaining system integrity and security across different network types is another significant challenge. As networks become more interconnected, a vulnerability in one network could potentially compromise the entire system. A comprehen- sive approach to security is required, where each network is secured individually and as part of the larger vehicle network ecosystem.

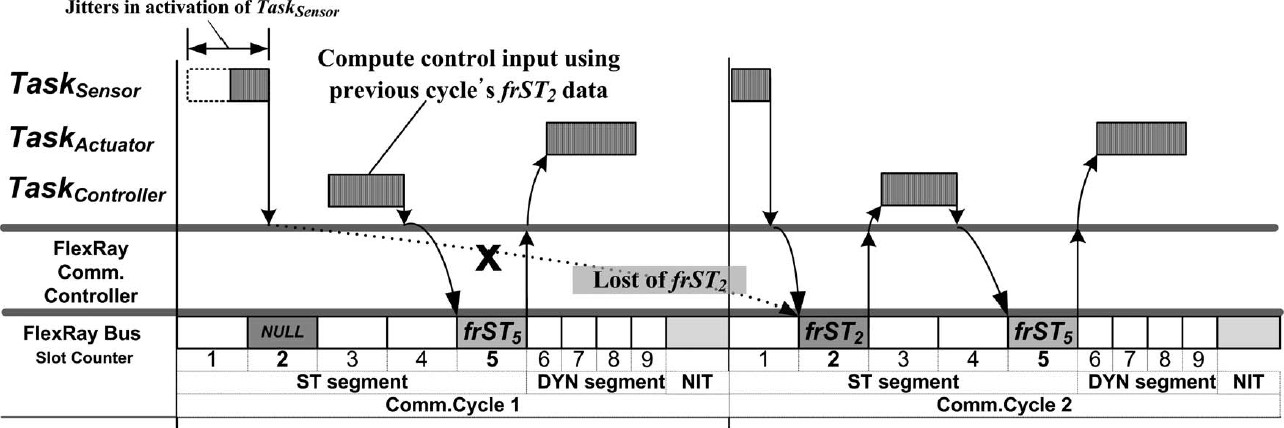


Fig. 12. Flexrayadvanced level of coordination and optimization achievable

TABLE III

**Aspect CAN Network LIN Network FlexRay Network**

Technological

Evolution

CAN FD for higher data rates. Enhanced robustness and easier

integration with CAN.

Increased data rates, improved time-triggered

communication.

Integration & Interoperability

Used with gateway modules for integration with LIN and FlexRay.

Simpler integration, often complementing CAN.

High-speed applications, integrated through sophisticated gateway technology.

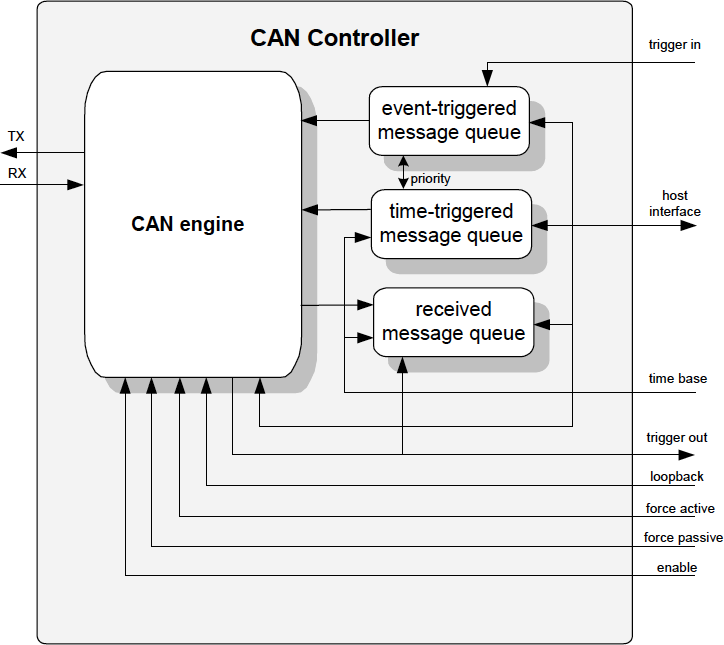


Fig. 13. FIG. CAN INTEGRATION CONTROLLER BLOCK DIAGRAM

Additionally, the growing complexity of vehicle networks has increased the demand for advanced diagnostic and man- agement tools. These tools must be capable of monitoring and troubleshooting issues across different network types, aiding technicians in identifying and resolving problems efficiently.

In conclusion, the integration and interoperability of CAN, LIN, and FlexRay networks are crucial for the development of sophisticated vehicle systems. The challenges in achieving seamless integration and maintaining security and integrity in these complex networks are significant. However, ongoing advancements in technology, including gateway modules, net- work protocols, and diagnostic tools, are continually enhanc- ing the capability and reliability of vehicle network systems.

# Real-world Applications and Case Studies

1. *Case Studies Highlighting Network Applications*

The real-world applications of CAN, LIN, and FlexRay networks are vast and varied, spanning across different sectors, primarily in automotive and industrial domains. These case studies provide insights into how these networks are applied and the benefits they bring.

CAN in Automotive Diagnostics: A notable application of the CAN network is in automotive diagnostics. A case study of a leading automotive manufacturer demonstrates how CAN is used to connect various electronic control units (ECUs) for real-time monitoring and diagnostics of vehicle systems. Through CAN, technicians can access data from different systems, such as the engine, transmission, and braking system, to quickly diagnose and address issues. This application not only enhances vehicle maintenance efficiency but also ensures higher standards of safety and performance.

LIN in Vehicle Comfort Systems: The use of LIN networks in managing vehicle comfort systems is another significant application. For instance, a European car manufacturer inte- grated LIN to control functions like mirror adjustment, seat positioning, and ambient lighting. This integration resulted in reduced wiring complexity and cost, while still maintaining efficient control over these functions. The LIN network’s sim- plicity and cost-effectiveness were key factors in its selection for these applications.

FlexRay in Advanced Driver-Assistance Systems (ADAS): A case study involving FlexRay’s application in ADAS show- cases its capacity to handle high data rates and ensure re- liable communication in safety-critical systems. A premium vehicle model equipped with FlexRay demonstrated enhanced performance in systems like adaptive cruise control, lane- keeping assistance, and collision avoidance. FlexRay’s high- speed data transmission and fault tolerance were instrumental in the success of these systems.

1. *Lessons Learned and Best Practices*

From these applications, several lessons and best practices have emerged:

Importance of Network Design: The design of the vehi- cle network architecture is crucial. Efficient network design ensures optimal performance and cost-effectiveness. For in- stance, the use of CAN and LIN in combination, where each

handles appropriate tasks based on their capabilities, results in a balanced and efficient network system.

Cybersecurity Measures: The increasing connectivity of vehicle systems underscores the importance of robust cyberse- curity measures. Continuous monitoring, regular updates, and advanced encryption are essential to protect against potential cyber threats.

Standardization and Interoperability: Ensuring standardiza- tion and interoperability among different networks enhances the ease of integration and maintenance. Adopting industry standards can simplify the development process and improve compatibility between different vehicle systems.

Future-proofing Networks: Considering future technology trends and potential upgrades in network design is crucial. This approach ensures that the vehicle network systems remain relevant and adaptable to emerging technologies.

# Emerging Technologies and Their Potential Impact

1. *Next-Generation Network Protocols*

The evolution of vehicle network protocols is ongoing, with new advancements aimed at addressing the limitations of current systems and meeting the demands of future automotive technologies. Next-generation network protocols are being developed with a focus on higher data rates, enhanced security, and greater scalability.

For example, the advent of Automotive Ethernet offers the potential for much higher data transmission speeds compared to CAN, LIN, or FlexRay. Automotive Ethernet is poised to revolutionize vehicle networks by providing the bandwidth necessary for advanced applications like autonomous driving and comprehensive vehicle-to-everything (V2X) communica- tion.

Another emerging protocol is the Time-Sensitive Network- ing (TSN) standard, which is an extension of Ethernet. TSN aims to provide deterministic communication on standard Eth- ernet, a critical feature for real-time applications in vehicles. The integration of TSN into automotive networks could lead to more streamlined and efficient architectures capable of handling the complex data flows of future vehicles.

1. *Impact of IoT and AI on Vehicle Networks*

The integration of the Internet of Things (IoT) and Artificial Intelligence (AI) into vehicle networks represents a significant shift in how vehicles are connected and managed. IoT enables vehicles to connect with a broader range of devices and infrastructures, offering opportunities for enhanced vehicle functionality, improved traffic management, and personalized user experiences. For instance, IoT can facilitate real-time traf- fic information, predictive maintenance, and improved energy management in electric vehicles.

AI’s impact on vehicle networks is equally transformative. AI algorithms can analyze data from various sensors and systems within the vehicle, providing insights for advanced decision-making. In autonomous vehicles, AI plays a crucial role in processing sensor data, making driving decisions, and learning from various driving scenarios to improve safety and efficiency.

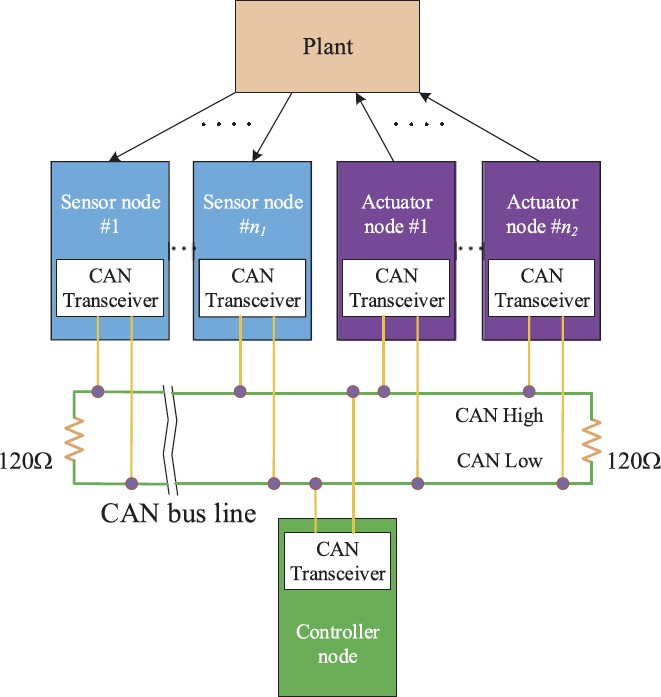


Fig. 14. NCS with CAN

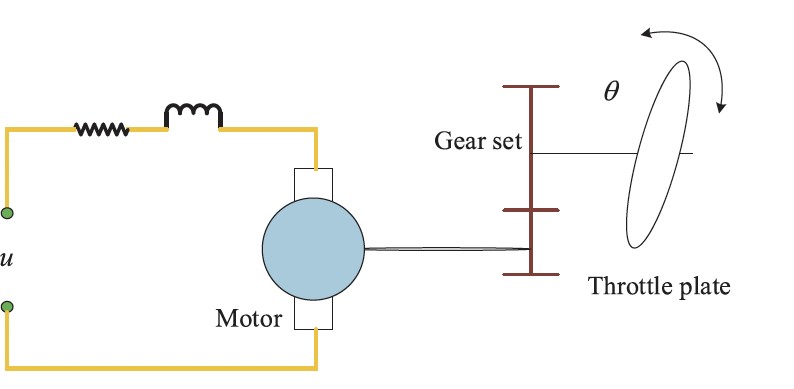


Fig. 15. Electronic throttle valve with CAN

The convergence of AI and IoT in vehicle networks also presents challenges, particularly in terms of data management and security. The vast amount of data generated by these tech- nologies requires robust data processing and storage solutions. Moreover, ensuring the security and privacy of this data is paramount, given its sensitivity and the potential consequences of breaches.

In conclusion, the future of vehicle networks is set to be shaped by these emerging technologies, with next-generation network protocols, IoT, and AI playing pivotal roles. These technologies will drive advancements in vehicle functionality, safety, and user experience, while also presenting new.

1. RECENT ATTACKS ON CAN AND ITS VARIANTS AND

ATTACK FEASIBILITY AND REQUIRED RESOURCES

*A. Specific Attack Vectors and Methodologies*

1. VULNERABILITY ASSESSMENT OF THE CAN PROTOCOL

The Controller Area Network (CAN) protocol, a critical component in automotive communication systems, has been subjected to extensive vulnerability assessments due to its significant role in vehicle functionality and safety. A detailed analysis based on the principles of confidentiality, integrity, and availability reveals inherent weaknesses in the protocol, making it susceptible to various cyber attacks

Confidentiality Concerns: Confidentiality, the principle of ensuring data accessibility only to authorized entities, is compromised in the CAN protocol due to its lack of inherent cryptographic methods. This omission allows intruders to access sensitive user data, leading to potential invasions of privacy and unauthorized data breaches.

•

Integrity Issues: Integrity in data communication entails the assurance of data accuracy, completeness, and validity. The CAN bus utilizes a Cyclic Redundancy Check (CRC) for the verification of data integrity against transmission errors. However, this mechanism is insufficient in preventing data injections by malicious entities, leading to a breach of data in- tegrity. The protocol’s lack of comprehensive integrity checks results in its inability to sustain the integrity of communicated data.

•

Availability Vulnerabilities: The principle of availability im- plies that authorized users should have consistent and reliable access to the system. In the CAN protocol, the priority-based messaging system can be exploited, wherein messages of the highest priority can dominate the network. This manipulation results in making the network inaccessible to lower-priority nodes, thereby violating the principle of availability.

1. AUTOMOTIVE ATTACK SURFACE EXPANSION The evolution of automotive technology, especially the

increase in embedded electronics, has led to a proportional rise in the attack surface for potential cyber threats. The integration of advanced electronic components and systems, such as sensors, actuators, control units, and communica- tion systems, has transformed vehicles from closed to open systems. This transformation has introduced complexities in vehicle communication and expanded the potential for cyber

attacks, which can now be executed remotely without physical access to the vehicle.

Types of Attacks: Automotive cyber attacks can be cate- gorized into physical access attacks and remote access attacks. Physical access attacks require direct interaction with the vehicle’s network, typically through the On-Board Diagnostic (OBD) port or by installing a malicious node in the vehicle’s network. Remote access attacks are executed via wireless com- munication interfaces, such as Bluetooth, Wi-Fi, and cellular networks, allowing attackers to exploit vulnerabilities from a distance.

•

1. NOTABLE PHYSICAL ACCESS ATTACKS Physical access attacks involve direct interaction with the

vehicle’s network systems, often through accessible ports or by installing unauthorized devices within the vehicle’s network.

On-Board Diagnostics (OBD) Port Attacks: The OBD port, being a direct gateway to the vehicle’s network, is a primary target for attackers. By exploiting the OBD port, attackers can manipulate various vehicle modules, including critical systems like brake and engine control. Such attacks have demonstrated the ability to release brakes, prevent brake activation, manipulate instrument clusters, change engine pa- rameters, and even disable the engine while the vehicle is in motion.

•

Selective Denial-of-Service (DoS) Attacks: These attacks disrupt the network without necessitating full message trans- mission. They can be executed by overwriting specific bits in the transmitted data, thereby generating transmission errors and exploiting the vulnerability of the CAN standard. Research in this area has focused on exploiting these vulnerabilities, leading to government alerts and increased awareness of the susceptibility of vehicles to such attacks.

•

Indirect Physical Access Attacks: These attacks do not require direct access to the vehicle’s network. For instance, hacking the IT system of a car service can provide indirect access to the CAN. Another method includes attacking via multimedia devices like CDs, USBs, or MP3 players. While these attacks may not directly breach the CAN, they can affect the driver by flashing warnings on the screen or playing alarm signals.

•

1. REMOTE ACCESS ATTACKS

Remote access attacks represent a significant threat in modern vehicles due to the integration of various wireless interfaces necessary for communication with systems like anti-theft devices, tire pressure monitoring systems (TPMS), Bluetooth, and telematics units.

Exploiting Wireless Interfaces: These interfaces, typi- cally connected to the CAN via a gateway ECU, have been demonstrated as vulnerable points for hacking. Successful compromises of these systems can lead to unauthorized control over the vehicle, including unlocking doors and manipulating vehicle functions remotely.

•

OTA Software Update Vulnerabilities: Over-the-Air (OTA) updates, while convenient and cost-effective for soft- ware delivery, present another attack surface. Hackers can

•

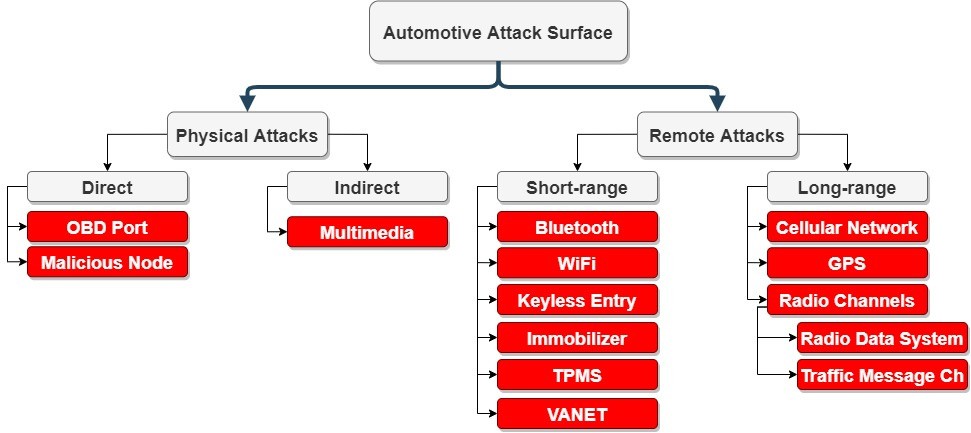


Fig. 16.

potentially intercept these updates to infiltrate the vehicle’s communication network, leading to ransomware attacks or other forms of cyber sabotage.

V2V and V2I Communications: The advent of vehicle- to-vehicle (V2V) and vehicle-to-infrastructure (V2I) commu- nications, which are integral to vehicular ad hoc networks (VANETs), introduces new vulnerabilities. These systems, designed for traffic optimization and collision avoidance, can be compromised by spoofed messages, resulting in disruptions to in-vehicle communication networks.

•

1. CLASSIFICATION OF ATTACKS ON IN-VEHICLE NETWORK SYSTEM

The in-vehicle network system is prone to various attacks, with the following being the most significant entry points for attackers:

OBD-II Port: This port, used for monitoring vehicle diag- nostics, is a critical vulnerability as attackers can easily collect diagnostic data, gaining access to the in-vehicle network and deploying malicious programs.

•

USB and Charging Ports: These ports are susceptible to severe security threats, such as the installation of malicious codes and reprogramming of the controller processor, enabling hackers to control critical vehicle systems like braking and engine control.

•

TPMS, LiDAR, and Keyless Entry Ports: These systems can be exploited for eavesdropping attacks, signal jamming, and interception of key signals, leaving the vehicle network open to unauthorized access and manipulation.

•

Bus Network Ports: The lack of communication protection in CAN protocols allows attackers to send fake frames to each node, leading to unintended vehicle behavior.

•

Vehicular Communication Ports: Enabled with technolo- gies like Bluetooth, Wi-Fi, DSRC, and cellular networks, these ports are vulnerable to various attacks, including jamming

•

and eavesdropping, potentially allowing attackers to gain full access to vehicles

*A. Detailed Discussion of Notable Attacks with Examples*

1. LOCK PICKING ATTACK ON KEYLESS ENTRY SYSTEMS

The lock picking attack exploits the keyless entry system’s vulnerability, typically used for car doors and garage openers. The attack involves a man-in-the-middle approach using a device that captures the key fob’s transmitted signal while sending a jamming signal on the same frequency. When the key fob user retries, the attacker’s device captures the second code transmission, using the first code to unlock the door while retaining the second code for future unauthorized access. This technique has been demonstrated on various car brands and garage door openers, with devices like Rolljam and OpenS- esame specifically designed for these types of attacks. Despite their widespread availability and potential misuse, sales of these devices have continued unabated, prompting concerns and calls for enhanced security measures from manufacturers.

1. TPMS EXPLOITATION

The Tire Pressure Monitoring System (TPMS) is a well- documented target for exploitation, lacking essential security safeguards. TPMS, which continuously monitors tire pres- sure and communicates with the vehicle’s Electronic Control Unit (ECU), can be attacked passively or actively. Passive attacks allow attackers to track vehicle movement by capturing TPMS signals, while active attacks involve wirelessly injecting spoofed signals to deceive the ECU. These attacks can result in displaying false tire pressure measurements, posing significant risks to vehicle safety. Countermeasures include using hard- ware pairings and encrypted signal transmissions to mitigate these vulnerabilities.

1. ROAD INFRASTRUCTURE ATTACKS

The increasing connectivity of vehicles has brought road infrastructure components into the scope of potential cyber threats. Vehicle-to-infrastructure (V2I) connectivity, encom- passing elements like smart traffic lights and road signs, presents new attack vectors. One notable incident involved the compromise of networked road signs in multiple states, displaying messages indicating they were hacked. Although initially perceived as pranks, such attacks have serious implica- tions, especially during emergencies. Mitigating these attacks requires stringent password management and secure design of sensors for V2V and V2I communications.

1. CAN BUS SPECIFIC ATTACKS

The classical CAN and CAN FD buses are susceptible to a range of attacks once access is gained:

CAN Sniffing: Attackers can passively monitor and an- alyze data on the CAN bus, using devices like the CANdo board, to manipulate and generate similar messages.

•

CAN Fuzzing: This involves sending random CAN data frames to observe changes in vehicle behavior, like speed alterations, during frame injections.

•

Frame Falsifying and Injection Attacks: Attackers modify CAN message payloads or inject data at abnormal rates to simulate events, leading to fake events that can drastically affect vehicle behavior.

•

DoS Attacks: These attacks use the highest priority CAN frames to monopolize the bus, preventing other nodes from accessing it, thus disrupting sensor parts and overall vehicle functionality.

•

1. ECU IMPERSONATION

Attackers can impersonate an ECU by analyzing traffic on the CAN bus and simulating the behavior of an ECU, including its CAN ID, payload range, and transmission rate. Sophis- ticated spoofing ECU attacks can exploit the error-handling mechanism of the CAN bus protocol, causing legitimate ECUs to be disconnected and dropping all CAN bus communication.

1. JEEP HACK VIA CELLULAR NETWORK

The Jeep hack, a landmark event in automotive cyberse- curity, demonstrated the vulnerability of in-car networks to remote attacks. In 2015, security researchers Charlie Miller and Chris Valasek exploited the cellular network interface of a Jeep Cherokee to gain remote control over the vehicle.

1. METHODOLOGY AND IMPACT:

The attack was initiated through the Uconnect system, which is connected to the cellular network and controls entertainment and navigation, and is connected to the CAN bus. By exploiting a vulnerability in the Uconnect system, the attackers remotely accessed the Jeep’s CAN network.

Once they gained access, Miller and Valasek were able to control various functions of the Jeep, including the air condi- tioning, radio, windshield wipers, transmission, and ultimately the braking system—all while the vehicle was in motion.

This attack highlighted the potential dangers of interconnected vehicle systems and the need for robust security protocols in vehicle-to-network interfaces.

1. MANIPULATION VIA OBD-II PORT Koscher et al.’s Research:

In a significant study, researchers Karl Koscher and his team at the University of Washington and the University of California, San Diego, demonstrated how the OBD-II port could be used to manipulate critical vehicle control systems.

Techniques and Consequences

The researchers were able to directly connect to the ve- hicle’s CAN network through the OBD-II port. By sending malicious CAN messages, they could control critical functions like the brakes and engine.

Notably, they showed it was possible to disable the brakes or falsely engage them, turn off the engine, and interfere with other crucial systems. This research brought to light the vulnerabilities inherent in the OBD-II port, which is typically used for vehicle diagnostics and is easily accessible.

1. SELECTIVE DENIAL-OF-SERVICE (DOS ATTACK Palanca et al.’s Contribution:

A team led by Palanca, et al., demonstrated a selective Denial-of-Service attack on an unmodified car, emphasizing the vulnerabilities in the CAN standard.

Execution and Implications

The attack involved overloading the CAN network with high-priority messages, effectively blocking other legitimate messages from being processed. This type of attack can render certain vehicle functions inoperable or cause erratic behavior in the vehicle’s electronic systems.

This form of attack was particularly concerning because it could be executed without requiring significant modification to the vehicle, demonstrating that even standard, unaltered vehicles are at risk.

1. SAE J1939 STANDARD ATTACKS

Mukherjee et al. and Murvay and Groza’s Findings: Researchers Mukherjee et al. and Murvay and Groza fo-

cused on the vulnerabilities within the SAE J1939 standard,

which is commonly used in heavy-duty commercial vehicles. DoS Attacks and Protocol Vulnerabilities:

Mukherjee and his team demonstrated the feasibility of DoS attacks on vehicles using the SAE J1939 standard. By sending excessive request messages or manipulating false requests, they could overload the recipient ECUs, causing disruptions in vehicle operations.

Murvay and Groza highlighted both specific protocol vul- nerabilities and general weaknesses in the CAN bus system. Their work emphasized how the architecture of the CAN bus, without proper safeguards, could be exploited to compromise vehicle functions or safety.

*A. Summary of Recent Academic Literature on Attacks on CAN and Its Variants*

1. INTRODUCTION TO CAN AND ITS SECURITY CONCERNS

The Controller Area Network (CAN) protocol, integral to modern vehicles’ communication systems, is facing increasing security threats. This shift from mechanical systems to ad- vanced embedded electronics in automobiles has augmented functionality and safety but also introduced new vulnerabili- ties. The CAN protocol, originally designed as a closed-loop system, now grapples with security issues due to its lack of encryption and authentication. These vulnerabilities allow malicious nodes to potentially cause significant harm, high- lighting the urgent need for comprehensive security analyses and solutions.

# Evolution of the Vehicle Industry and CAN Vulnerabil- ities

Vehicles have undergone a transformative shift towards extensive automation, integrating a plethora of sensors and ECUs. Modern vehicles are equipped with over a hundred ECUs, a number expected to rise, controlling everything from engine management to advanced driver-assistance sys- tems (ADAS). While CAN offers benefits like cost-effective wiring and error correction, it is increasingly susceptible to cyberattacks. The security features built into CAN focus on reliable communication rather than cybersecurity, exposing it to various risks, including jeopardizing passenger safety and causing financial implications for manufacturers.

# Lack of Encryption and Data Privacy Issues

CAN’s design as a broadcast network without encryption significantly impacts individual data privacy. In modern ve- hicles capable of collecting driver’s personal information, the unencrypted broadcast data on CAN allows adversaries to acquire sensitive data, leading to privacy invasions. This vulnerability has been underscored in industry surveys, with safety and security identified as critical short-term and mid- term challenges. Consequently, there is an ongoing effort in the academic community to develop solutions for these vulnerabilities, such as network segmentation, encryption, authentication, and intrusion detection systems.

# Physical Access Attacks

Physical access attacks on CAN require direct interaction with the vehicle’s network. These attacks can be executed through access points like the OBD port. For instance, Koscher et al. demonstrated the manipulation of essential vehicle mod- ules, including brakes and engine control, through the OBD- II port, significantly impacting vehicle safety. Palanca et al. highlighted the feasibility of DoS attacks through physical ac- cess, exploiting the vulnerability of the CAN standard. These studies have shown that physical access attacks, although less practical, pose a serious threat to vehicle security.

# Remote Access Attacks and Wireless Interfaces

Remote access attacks have gained prominence with the integration of wireless interfaces in vehicles. These inter- faces, while essential for modern functionalities like anti- theft systems and TPMS, create new vulnerabilities. For instance, Checkoway et al. compromised multiple vehicle

systems through wireless interfaces, demonstrating the ease of vehicle theft. Valasek and Miller’s survey identified re- mote attack surfaces across various car brands, revealing the widespread nature of these vulnerabilities. The transition to more connected vehicles, with technologies like V2V and V2I communications, only increases the potential for remote attacks.

# Personal Data Breaches

The modern vehicle’s capacity to collect and process per- sonal data presents significant privacy challenges. Investiga- tions have shown that attackers can obtain sensitive infor- mation such as location history and connected phone data by passively listening to the CAN bus. This vulnerability to personal data breaches necessitates urgent attention to securing the CAN network against such intrusions.

1. *Feasibility of Attacks on These Networks*

# Defense Mechanisms Against CAN Attacks

The primary defense mechanisms against CAN attacks include network segmentation, encryption, authentication, and intrusion detection systems. Network segmentation, while straightforward, is limited in effectiveness if the gateway ECU is compromised. Encryption is necessary for data privacy but faces challenges like limited data fields and computational power of ECUs. Authentication methods like VeCure and LiBrA-CAN aim to verify message authenticity but increase network traffic and may not be effective if a node within the trust group is compromised.

# Encryption Challenges

Implementing encryption on CAN is complicated by the protocol’s shared broadcast network nature and lack of a built- in encryption mechanism. Existing commercial and proprietary encryption techniques have been reportedly broken, highlight- ing the need for robust and dynamic encryption methods. Hardware-based encryption methods like FPGA chips and physical unclonable functions (PUFs) offer potential solutions, but they may require significant changes to legacy ECUs and are not backward compatible.

# Authentication Methods

Authentication in CAN is crucial to prevent malicious messages from being accepted as authentic. Methods like VeCure and LiBrA-CAN have been proposed, but they face challenges like increased network traffic and compatibility issues with traditional CAN. The complexity of implementing commercially viable authentication methods is highlighted by the fact that none of the analyzed methods in literature fully meet essential criteria such as cost-effectiveness, backward compatibility, and support for vehicle repair and maintenance.

# Intrusion Detection Systems (IDS)

IDS emerges as a promising solution, not requiring mod- ifications to the current CAN controller or increasing bus traffic. Signature-based detection is effective against known attacks but fails with new ones, while anomaly-based detec- tion, though less accurate, can potentially identify unknown attacks.

Time/Frequency-Based IDS and Physical Characteristics Basic IDS analyzes the frequency of CAN messages, but this approach may be influenced by the vehicle’s operational

•

conditions. Physical characteristic-based IDS, like VoltageIDS, uses the unique electrical characteristics of CAN signals as a fingerprint. However, these methods require sophisticated signal processing and can be influenced by environmental factors.

Specification and Language-Based Detection Specification-based and language-based intrusion detection

•

approaches have been proposed, but they face limitations in attack detection capabilities and require detectors in all ECUs. These methods are not powerful enough to prevent all types of attacks, especially those that are protocol compliant.

Feature-Based System Analysis

•

Feature-based analysis using artificial intelligence tech- niques, like GAN-based IDS and Bloom filtering, provides a memory-efficient analysis of data. However, these methods require heavy computation and may not be feasible for all vehicle systems due to their computational intensity.

# Ongoing Research and Industry Standards

Automotive security is increasingly gaining attention, with standards and specifications being developed to address cy- bersecurity problems. Industry initiatives are focusing on manufacturing secure ECUs and implementing proprietary intrusion detection systems. However, the disparity between industry and academic resources, along with the lack of shared attack data and benchmarks, underscores the need for more collaborative research efforts and open-source datasets.

1. *Computational and Communication Resources Needed by Attackers*

The complexity of attacks on the Controller Area Network (CAN) and its variants in modern vehicles requires diverse computational and communication resources. These resources range from sophisticated software for data analysis to special- ized hardware for network interfacing. This review consoli- dates insights from various academic sources to understand the resources attackers utilize in executing these cyberattacks.

# Data Collection and Analysis

CAN Bus Data Capture: Attackers capture data from a vehicle’s CAN network, often via the On-Board Diagnostics (OBD) port, using tools like Vehicle Spy simulation test software. This process demands precision to avoid packet loss and maintain data integrity. Large datasets are created for deep analysis, requiring significant storage and processing capabilities.

•

Anomaly Detection Algorithms: Post data collection, sophisticated algorithms analyze anomalies in the CAN ID’s message stream, a process that requires substantial computa- tional power. These algorithms discern between normal vehicle operation changes and deliberate tampering, making them crucial in attack execution.

•

# Exploiting Connectivity Interfaces

Hacking Connectivity Systems: Modern vehicles are equipped with a plethora of connectivity interfaces such as Bluetooth, Wi-Fi, and cellular networks. Exploiting these systems requires specialized software capable of intercepting and manipulating wireless communications. Such tools need to be adaptable to different technologies and robust enough to breach security protocols.

•

Diagnostic Port Vulnerabilities: The OBD-2 port, used for diagnostics, is a frequent target for cyberattacks. Attackers use specialized hardware to interact with this port, leading to po- tentially severe safety compromises. The hardware employed here is often compact yet capable of powerful interfacing with the vehicle’s internal systems.

Targeting Vehicle Sensors and Actuators: Physical avail- ability attacks, like signal jamming, are directed at crucial vehicle sensors and actuators. This method requires hardware that can effectively disrupt or manipulate sensor data, such as devices capable of eavesdropping on TPMS signals.

•

•

Signal Jamming and Relay Attacks: Systems like LiDAR and keyless entry are susceptible to signal jamming and relay attacks. These attacks necessitate sophisticated hardware and software to capture and relay signals, enabling unauthorized access to vehicles.

•

1. *Dependencies on Physical Access or Specific Conditions for Successful Attacks*
   1. **Physical Access to the Vehicle:** Many attacks on the CAN network require physical access to the vehicle. This can range from a mechanic to a family member inserting a malicious component into the car’s internal network, usually through the OBD-II port. The impact of these attacks can be profound, allowing control over critical vehicle functions.
   2. **Direct Access through OBD Port and Malicious Nodes:** Direct access attacks are often executed through the OBD port, which provides comprehensive access to the vehicle’s network. Such attacks can control critical vehicle systems, including braking and engine functions. Malicious nodes, once connected, can disrupt the network by intercepting or sending deceptive messages.
   3. **Denial-of-Service (DoS) Attacks:** DoS attacks, particu- larly on commercial vehicles, involve overloading the network with excessive request messages or manipulating network connections. These attacks require an understanding of specific network protocols and the ability to generate substantial traffic to overload the system.
   4. **I ndirect Physical Access:** Indirect physical access attacks involve inserting a physical object into the car, without direct network access. Checkoway et al. developed an indirect access attack model by hacking the car service’s IT system and accessing the CAN via a computer. Another indirect attack involved using multimedia devices like CDs, USBs, or MP3 players. Although these attacks may not directly breach the CAN, they can disrupt the driver by displaying warnings and playing alarm signals, emphasizing the importance of securing both direct and indirect access points to the CAN bus network.
2. COUNTERMEASURES AND MITIGATION STRATEGIES
3. *Existing security measures and their effectiveness*

In the last decade, researchers have explored a wide range of malware defense solutions for computer and mobile sys- tems. Those solutions can be categorized into signature- based, behavior-based, heuristic-based, cloud-based, and ma- chine learning-based techniques. In this section, we present a

detailed review of the main factors of applying these defense systems to protect intelligent vehicles against malware. These factors include the used approach, the used data analysis method, the targeted operating system, the detection time and the detection response, the data source, the main advantages and disadvantages of each defense system. Figure 1 shows the taxonomy dimensions distributed into six classes. We also briefly describe these classes below.

* 1. **Techniques**: We classify the existing malware detection techniques into five categories, i.e., signature-based malware detection techniques, behavior-based malware detection tech- niques, heuristic-based malware detection techniques, cloud- based malware detection techniques, and machine learning- based malware detection techniques. Each of these techniques has certain advantages and disadvantages, we discuss the benefits and drawbacks of each technique.
  2. **Analysis Methods**: The whole detection process is ac- complished with static, dynamic and hybrid analysis methods. The description of each method is presented below.

**Static Analysis**: It’s a malware analysis method that analyzes an executable code without actually executing the code itself. In static analysis, the low-level information from codes is extracted by disassembling the codes by using any disassembler tools. The main advantage of this method is revealing the code structure of the program without executing it. However, this method may fail in analyzing unknown malware. It may also fail to detect malware that employs obfuscation and evasion techniques in its code.

•

**Dynamic Analysis**: It’s a malware analysis method that entails running the malware and monitoring its behavior, interactions with the host system, and its impacts on the host environment. The infected files in this method are analyzed in a simulated environment such as an emulator, virtual machine and sandbox in order to make the environment invisible to the malware. Although this method is efficient in detecting malware, nevertheless, it may fail to detect malware that uses obfuscation code and evasion techniques.

•

**Hybrid Analysis**: It’s a malware analysis method that combines both dynamic and static analysis. It examines almost all of the static features of any malware code then combine them with other behavioral features to better the overall analy- sis process. Despite this method can overcome the limitations of both static and dynamic analysis methods. However, it may result in a rise in the execution time’s total overhead.

•

* 1. **Target Operating System (OS)**. It refers to the operating system analyzed by the system. It can be LINUX, Windows, or Android.
  2. **Detection Time**. It refers to the time between the analyzed event and the detection itself. It can be real-time (online) detection, which enables an automatic response such as blocking the attacker and killing the malware process, or non-real-time (offline) detection.
  3. **Detection Response**. The relevant outcome of the system, which can be a passive response which is an event notification such as printing an alert message, or an active response which is an automatic reaction such as blocking the attacker or killing the malware process.
  4. **Data Source**. It refers to the source of the input data analyzed by the system. It can be host logs which are data from the operating system and system applications or application logs which are data directly generated by applications, or network traffic which are data generated by the network layer.

# Malware detection system taxonomy Signature-Based Malware Detection :

•

The process of signature-based malware detection, promi- nently used in commercial antivirus tools, comprises two main stages. Initially, a unique signature is crafted for each malware, derived from a mix of manual and automated analysis of data from networks and user devices. Then, devices store these signatures to identify malware in files or data streams. This technique, which disassembles and analyzes malware binary codes, is simple, fast, and safe, especially for intelligent vehicles, excelling in detecting known malware but falling short in identifying new, unknown threats due to its vulnera- bility to evasion. In contrast, cutting-edge malware detection methods focus on digital footprints in various log files and employ different analysis techniques, such as static analysis, function call graph similarity, and API call sequences. These approaches are highly accurate for known malware but are limited in detecting unknown malware and not suitable for real-time applications, such as in intelligent cars.

Additionally, researchers have explored various sophisti- cated techniques for malware detection, primarily targeting the Windows operating system. These methods include analyzing program bit files without code execution (static analysis) and using unique identifiers like control flow graph signatures and byte sequences of executable files.

# Behaviour-Based Malware Detection :

•

The way of behaving based malware discovery strategy inspects how a program acts to decide whether it’s malevolent. It does this in a safe climate like a virtual machine, without depending on outside frameworks, in any event, for new, never- seen-before malware. Many utilize this strategy to counter malware, taking a gander at expected ways of behaving and utilizing information signs on different working frameworks. In spite of its high location rate, it has disadvantages like significant expenses and intricacy, making it unacceptable for savvy vehicles. While it succeeds in distinguishing new mal- ware, it battles with arranging all ways of behaving precisely, prompting possible bogus up-sides or negatives. Contrasted with signature-based recognition, it’s harder to execute and asset serious for in-vehicle gadgets, presenting difficulties for long haul use in vehicles.

# Heuristic-Based Malware Detection :

•

The heuristic-based malware discovery procedure evaluates program records for dubious attributes or reenacts program execution to recognize possible malignant exercises. This tech- nique, known for its intricacy, draws on previous encounters and utilizes information mining, rule-based frameworks, and AI to learn program qualities. Generally utilized in antivirus programming, it can distinguish different known and obscure malware, including zero-day dangers. In any case, it battles with distinguishing most new and refined malware and is pow- erless to cutting edge code jumbling and avoidance methods. Analysts have proposed static investigation techniques, similar

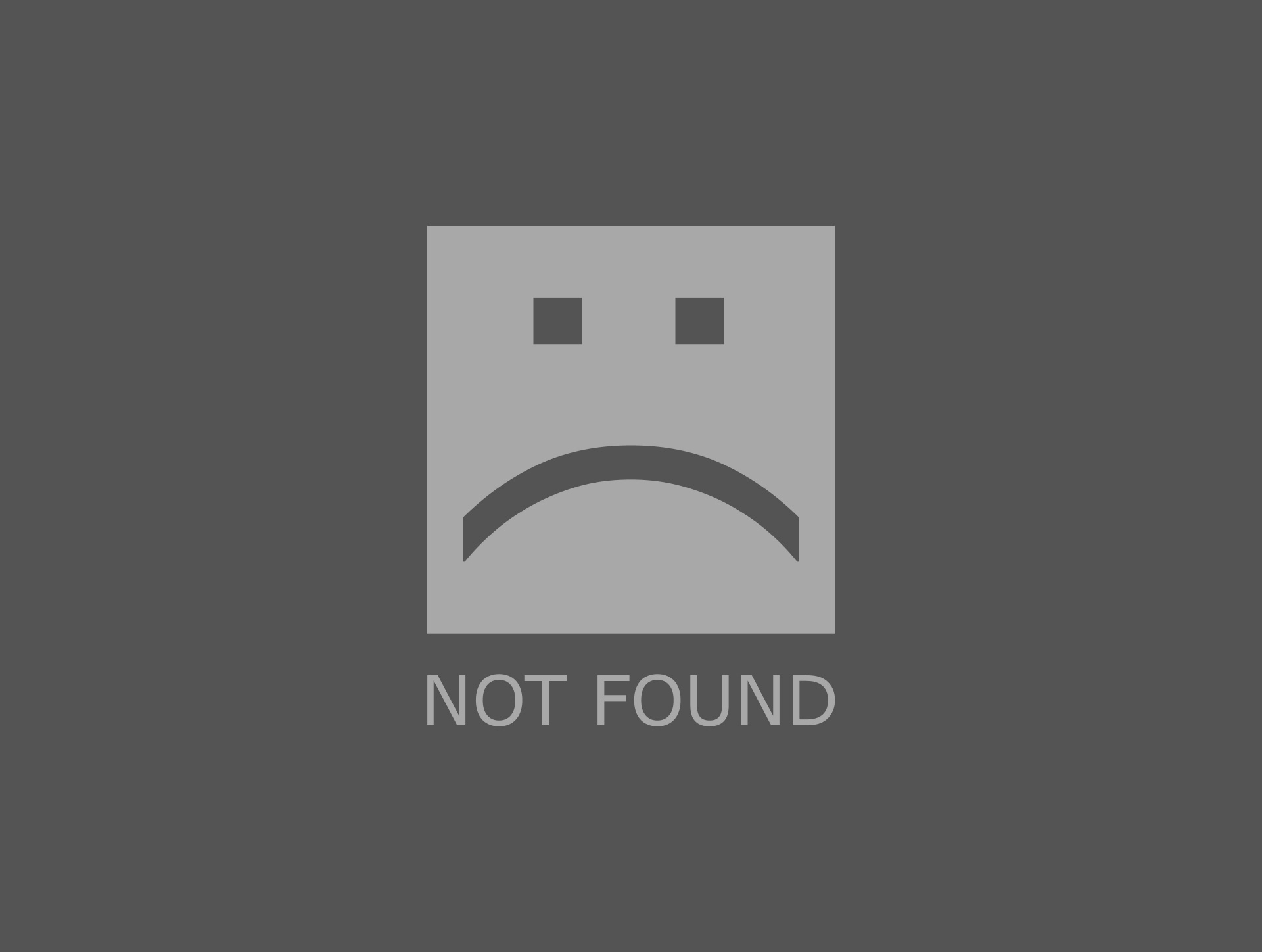


Fig. 17.

to control stream charts, and dynamic strategies utilizing DLLs or Programming interface call organizations. While powerful for known malware, these methodologies are perplexing, have high misleading positive rates, and aren’t appropriate for continuous recognition in that frame of mind because of their tedious nature. In spite of its solidarity in distinguishing obscure malware, the heuristic-based method is really difficult and asset escalated contrasted with signature-based and con- duct based strategies. It may not be great for asset obliged in-vehicle gadgets, given its intricacy and possible outdated nature after some time.

# Cloud-Based Malware Detection :

•

Distributed computing has acquired fame for its helpful access, on-request capacity, and cost-viability. As of late, it has been utilized in malware discovery through the Cloud- based method, utilizing location specialists on cloud servers. This technique permits clients to submit documents for inves- tigation and get writes about their malware status. While it improves recognition execution with broad information bases and figuring assets, it faces disadvantages, for example, depen- dence on a steady and quick web association, powerlessness for continuous record observing, and weakness to jumbling

and avoidance methods.

Scientists have investigated cloud-based strategies for mal- ware examination, utilizing static investigation with highlights like document content and relations, as well as powerful investigation through framework call checking. Nonetheless, these strategies cause significant expenses, above, and time delays, making them unsatisfactory for continuous discovery, particularly in keen vehicles. Notwithstanding the benefits of speedy access and refreshed establishments, the cloud-based approach is tested by the requirement for a solid web associa- tion and defenselessness to cutting edge avoidance strategies, raising worries about its wellbeing in savvy vehicles. The rise of high velocity 5G innovation might work on its reasonability in this specific circumstance.

# Machine Learning-Based Malware Detection :

•

AI has for quite some time been a foundation in the mission to recognize malware, with calculations like Guileless Bayes, Bayesian organization, strategic relapse, and others offering novel qualities. Every calculation’s viability relies on factors like information dispersion and element relationships. Profound Learning, a branch-off of fake brain organizations, has arisen as an amazing asset, particularly in applications, for

example, picture handling, voice control, and, all the more as of late, malware identification. Be that as it may, its power- lessness to jumbling and avoidance, combined with the time- concentrated course of developing secret layers, highlights the requirement for smart application.

Somewhat recently, scientists have proposed different AI based malware discovery methods, utilizing static elements, for example, framework calls, strings, and picture highlights. While these strategies hold guarantee, challenges arise in tending to stowed away damaging exercises and guaranteeing ongoing discovery. Notwithstanding headways, the ongoing scene actually wrestles with the computational requests of microarchitectural highlight based approaches, delivering them illogical for the continuous protecting of smart vehicles. The polarity between the likely advantages and reasonable restric- tions of AI in this setting highlights the continuous mission for more nuanced and successful arrangements in the consistently developing domain of network safety..

# Network Segmentation

•

Carrying out network division by partitioning the CAN organize into subnetworks is a primary safety effort, giving command over access and restricting the expected spread of assaults. This normal methodology in business vehicles includes a door Electronic Control Unit (ECU) directing in- terconnections between subnetworks. Nonetheless, weaknesses emerge in the event that the door ECU is compromised, as exhibited in certain hacking situations. To address this, Kammerer proposed a star coupling switch with upgraded security highlights, yet it doesn’t completely address security inside subnetworks, leaving space for complex assaults. An elective methodology introduced by TU München includes a two-layer design, isolating the infotainment framework and imperative capabilities to forestall outside assaults. While net- work division upgrades security, it is recognized that it alone is inadequate, presents support intricacies, and accompanies inflated costs.

# Encryption

•

The CAN convention, lacking implicit encryption, opens its correspondence to potential listening in by enemies, making the execution of a lightweight encryption framework critical. While business programming based encryption strategies and exclusive methods by producers exist, reports recommend weaknesses in monetarily accessible vehicle encryption frame- works. Challenges in secure Could encryption at any point in- corporate the restricted information field, tended to by sending various CAN outlines for a solitary message, though not great for high-traffic organizations. Moreover, the computational im- peratives of ECUs require dynamic key trade to forestall static key split the difference over a vehicle’s life expectancy. Be that as it may, dynamic key trade presents execution hardships, computational costs, and idleness issues for asset compelled ECUs, making it unacceptable for security basic continuous frameworks. Elective arrangements, for example, equipment put together AES-128 encryption with respect to FPGA chips and the utilization of actual unclonable capabilities (PUFs), have been investigated, each with its benefits and disadvan- tages, featuring the continuous difficulties in getting the CAN convention against different dangers, including replay assaults.

# Authentication :

Distinguishing the source of a CAN message represents a test, permitting foes with network admittance to send unauthenticated pernicious messages acknowledged as true by all hubs. Confirmation instruments become essential for counteraction, and different methodologies have been investi- gated. VeCure confirmation depends on trust bunches sharing a symmetric mystery key, limiting key numbers and relating to the quantity of trust bunches as opposed to ECUs. In any case, the strategy pairs network traffic by sending a confirmation message after each edge and needs security on the off chance that a trust bunch hub is compromised. LiBrA- CAN further develops effectiveness by parting validation keys among gatherings yet requires high data transfer capacity and is contrary with customary CAN. Economically implementable verification techniques face difficulties in gathering rules, for example, cost-viability, in reverse similarity, fix support, execution subtleties, and adequate above. Existing off-the- rack items, similar to NXP’s S32K family, give equipment based validation sped up processes, tending to industry worries about ECU costs. As equipment innovation progresses, safer CAN arrangements might arise, utilizing equipment based confirmation strategies to upgrade security.

•

# Intrusion Detection System (IDS)

•

Getting a wellbeing basic ongoing framework presents difficulties because of restricted assets and time limitations, prompting the investigation of interruption location frame- works (IDS) for Regulator Region Organization (CAN). IDS offers a benefit by regularly not altering the current CAN regulator and keeping away from expanded transport traffic. Two principal classifications of IDS are mark based (abuse) identification, which distinguishes known assaults, and pecu- liarity based location, which perceives deviations from typical way of behaving. While signature-based recognition succeeds at known assaults, it might miss obscure ones, though abnor- mality based IDS might possibly distinguish obscure assaults by investigating network conduct. IDS frameworks survey different boundaries on the CAN, arranged as time/recurrence based, actual framework qualities, determination based, and highlight based, using deviations from ordinary sensor conduct as interruption pointers.

# Time/Frequency-Based IDS :

•

With regards to auto wellbeing guidelines and the common utilization of occasional signs from Electronic Control Units (ECUs), any deviation in signal recurrence is viewed as unusual way of behaving, showing a possible interruption. One principal Interruption Recognition Framework (IDS) approach centers around dissecting the recurrence of CAN messages. Another technique, proposed by Lee et al., presents the offset proportion and time span based IDS, which surveys the reaction season of sent remote casings. This calculation really recognizes assaults and distinguishes their sorts, yet with the disadvantage of expanded transport traffic because of the infusion of remote casings for investigation.

While time/recurrence examination offers important experi- ences into CAN conduct, varieties in the vehicle’s state (e.g., inactive or running) and the Might’s need at any point plan can altogether change timing data, affecting the viability of

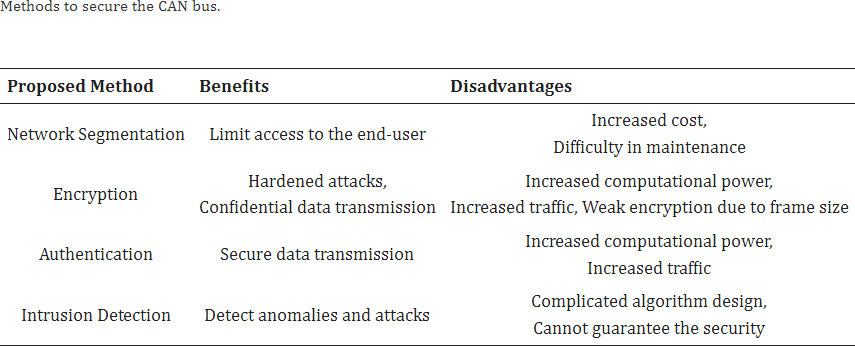


Fig. 18.

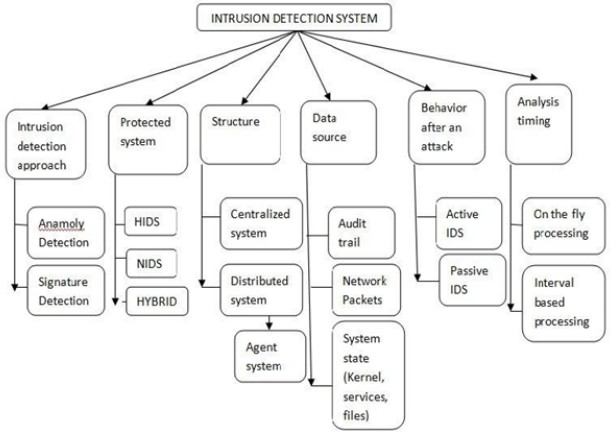


Fig. 19.

time/recurrence based IDS. Also, this strategy might battle to recognize assaults that don’t modify the recurrence, for example, disguise assaults..

# Physical Characteristic Based IDS :

The actual qualities of the Regulator Region Organization (CAN) network offer an extraordinary road for interruption discovery, as each handset displays a particular sign shape, impacted by assembling varieties, cabling, and maturing. An imaginative methodology, VoltageIDS, presented by Choi, use the electrical finger impression of CAN signals, taking into account factors like positive and negative incline values and voltage at a predominant level. While accomplishing a zero misleading positive rate and recognizing assaults and blunders, this strategy requires an oscilloscope for signal assortment and includes concentrated signal handling.

Clock slant arises as one more technique proposed by Cho and Shin, using the shortfall of a common expert clock in CAN. By fingerprinting the transmitter ECU through clock slant, irregularities can be identified, yet with constraints in appropriateness to occasional messages and weakness to mimicry. In spite of the fact that clock slant based discovery arrived at 97% exactness with a 0.55% misleading positive rate, it stays defenseless against specific assaults. While actual trademark based IDS offers important bits of knowledge into CAN security, ecological factors and maturing may affect its dependability, particularly despite programming layer assaults. In addition, the handling requests of such strategies might present dormancy or require expensive equipment.

# Specification Based IDS :

Larson presented a detail-based assault location technique by planning rules grounded in the CAN Open convention. Notwithstanding, this approach shows restricted assault loca- tion capacities, orders all ECUs to be furnished with finders, and misses the mark on solidarity to ruin convention agreeable assaults. In an alternate vein, Studnia proposed a language- based interruption location framework, characterizing the orga- nization’s language qualities from ECU particulars and creat- ing illegal successions. The location component triggers upon the event of any of these predetermined successions, actually recognizing interruptions in light of language deviations.

# Feature-Based IDS :

Include based framework examination investigates network boundaries like busload, recurrence, and the quantity of dropped messages, alongside factors like unusual messages and payload, normally utilizing computerized reasoning proce- dures. Search engine optimization presented a Generative Ill- disposed Nets (GAN)- based Interruption Identification Frame- work (IDS) using profound learning models, known for its versatility and strength against control by assailants, showing a black-box location trademark. Another methodology, pro- posed by Groza and Murvay, consolidates Sprout separating to examine periodicity and payload in CAN messages, offer- ing memory-effective information examination. Albeit every technique presents special qualities, there is a compromise included. An extensive IDS arrangement might include a cross breed framework that joins different strategies to address var- ious parts of the Could security at any point challenge. While

IDS can relieve security issues, complete security requires the joining of cryptography to guarantee secrecy..

# SECURE BOOT

•

Secure Boot is not an automotive industry exclusive idea, in fact, it’s supported by most BIOS in home PCs. It’s a Unified Extensible Firmware Interface (UEFI) mechanism which allows only software with valid signatures to be booted in the machine it’s working on. The manufacturer loads some databases of keys and signatures in the device in manufac- turing time. The firmware would then be signed and have its signature checked before booting. Secure booting is a very strong security mechanism that stops malicious firmware from being booted, but previously there have been vulnerabilities in specific implementations that allowed for bypasses in some occasions, which makes secure booting not a silver bullet.

# SECURE ACCESS SERVICE

•

The scientists dug into the diagnostics validation component while figuring out a 2010 Toyota Prius and a 2010 Portage Break, uncovering a Security Access system implanted inside the Bound together Diagnostics Administration (UDS) char- acterized in ISO 14229-1. UDS fills in as a standard diagnos- tics correspondence convention for Electronic Control Units (ECUs) in the auto domain, offering different administrations to gather data about a vehicle’s usefulness and state. The Secu- rity Access administration utilizes a Test Reaction convention, where the analyzer demands a "seed" from the ECU, which, upon age, is sent back. Both the analyzer and ECU share a cryptographically safe capability and a key to make a reaction. Notwithstanding, the free standard needs points of interest on the capability, keys, or seed age. Outstandingly, weaknesses were recognized, for example, unsurprising seeds and lacking reaction length, empowering assailants to utilize beast power or replay assaults. The specialists effectively separated keys through figuring out, uncovering shortcomings in the security of these auto frameworks.

# Secure Onboard Communications

•

To address the confirmation deficiencies in the Regu- lator Region Organization (CAN), the AUTOSAR people group proposed the Solid Locally available Correspondences (SecOC) module, which presents CAN approach verification by adding marks to in-vehicle correspondences. SecOC works with both even and unbalanced cryptography, expecting that vital administration and trade are as of now settled. The method includes annexing a mark, alongside a newness an incentive for uniqueness, to the safeguarded information unit (PDU) in the CAN outline. In balanced mode, for example, the shipper computes a Message Validation Code (Macintosh) over the info information and newness esteem utilizing a common key, annexing it to the message. The recipient confirms the newness esteem and recalculates the Macintosh, tolerating the message if right. Nonetheless, squeezing this framework into a normal CAN approach raises difficulties, for example, short- ening the 128-bit Macintosh into a 27-piece esteem, possibly powerless to beast force assaults. Another methodology, the Fitting and Secure Key Foundation (PnS), offers a minimal expense symmetric key foundation convention for CAN, using an actual property in the transport to characterize a key between two gadgets at whatever point they communicate a

piece all the while, upgrading security in the organization.

# Firewall Gateway

•

Improving in-vehicle correspondence security can include carrying out a firewall system inside network doors. In the event that message confirmation codes (Macintosh) or ad- vanced marks are used for verification and approval between Electronic Control Units (ECUs), firewall rules can be gotten from the approvals in each ECU’s declaration. At the point when Macintoshes or computerized marks are missing, firewall rules can be separately characterized in light of vehicular subnet approvals, permitting just messages from legitimate and valid ECUs to go through and be sent on the in-vehicle transport framework. Another methodology is to limit the entrance level of various organization types to explicit pieces of the transport framework, forestalling less basic organiza- tions, similar to LIN or MOST, from sending messages to higher wellbeing pertinent frameworks, for example, CAN or FlexRay. Moreover, utilizing Interruption Discovery Frame- works (IDS) in a focal entryway can additionally improve correspondence and framework security by examining and breaking down traded data to distinguish security-basic odd- ities. The IDS can then take proper countermeasures, from giving interruption advance notice messages to deactivating acting up ECUs, contingent upon the sort of correspondence bad conduct distinguished.

# Honeypots

•

Getting in-vehicle correspondence frameworks is vital be- cause of the weakness presented by remote correspondence entryways. Assailants can take advantage of remote admittance to send off digital goes after straightforwardly on the in-vehicle organization, which controls basic vehicle activities. Under- standing aggressor conduct is critical to creating successful se- curity arrangements. Honeypots, intended to show up as weak targets, act as instruments for avoidance and early discovery of pernicious assaults. In the car area, sensible honeypots can be executed to draw in genuine aggressors without disrupting typical vehicle activity. These honeypots gather information as the vehicle travels through unambiguous regions, recording data influencing the in-vehicle organization. Examination of this information distinguishes assault conduct, situations, and orders, helping with the improvement of vigorous safety efforts to shield in-vehicle correspondence frameworks in later plans and executions.

1. *Latest advancements in securing automotive networks*

# Quantum Key Distribution (QKD)

•

Quantum Key Age (QKG) and Quantum Key Dissemina- tion (QKD) are principal advancements for accomplishing quantum-safe security, fundamental for the up and coming age of secure Vehicle-to-Everything (V2X) correspondence orga- nizations. The security of cryptographic frameworks depends vigorously on the strength of their keys, affecting information secrecy, respectability, validation, non-disavowal, and access control in information trade. Keys should be extraordinary, really irregular, and safely put away or circulated for authentic security. QKD is especially helpful in safeguarding informa- tion trade inside the back-end framework, a practical objective

for assailants because of the likely burglary of huge mea- sures of touchy information. The mix of Quantum Irregular Number Age (QRNG) and QKD guarantees the age of high- entropy keys, safely disseminated across the organization. This encryption of vehicular interchanges gives flexibility against both flow and future assaults, and can flawlessly coordinate with quantum-safe calculations (QRAs) when they become accessible, limiting the requirement for critical programming or equipment adjustments.

# Quantum-Safe Security for Automotive Ecosystems

From an automotive ecosystem security perspective, vehicle systems, vehicle-to-vehicle networks, vehicle-to-infrastructure networks and back-end systems must be future-proofed by introducing quantum-safe cryptographic solutions as a priority. IDQ’s range of quantum-safe security solutions are specifi- cally designed to secure data in motion across V2X ecosystems

against existing and emerging threats.

# Quantum Random Number Generation (QRNG)

Strong key generation is key to ensure a third party cannot guess or deduce the security key. Therefore, the use of truly random numbers is crucial. Quantum Random Number Gener- ation (QRNG) serves this purpose well; instantly strengthening existing cryptographic mechanisms and ensuring new quantum resistant algorithms will remain robust.

* Instantly strengthen the encryption keys
* Protects communication to outside apps and hardware
* Protects communication in the cloud

IDQ’s Quantis QRNG chip is ideal for integration into automotive HSMs. It provides a clear and robust entropy generation mechanism with a security proof. It is AEC-Q100 certified, with integrated NIST 800-90A/B/C compliant DRBG post-processing.

Features and benefits:

* Provably random, highest value quantum enhanced keys
* Low cost, low power, environmentally robust
* Instant on

# Survey of Security Solutions Based on Cryptography Techniques:

Generally, there are two main components in the Cryptog- raphy approach.

First is known as Message Authentication Code (MAC) and another is called as cryptosystems having two fields sym- metric and asymmetric. Further, Integrity and Authentication is ensured by the MAC while confidentiality is provided by the symmetric and asymmetric cryptosystems. Additionally, session keys can be utilized for providing authentication. For vehicle safety, the load on the CAN bus and latency issue in response time should be within specified limit. Additionally, error detection in data frame transmission is provided by the Cyclic Redundancy Code (CRC) at CAN bus. ECUs are having their own limitations in terms of computational capacity thereby lightweight encryption is one of the solutions for handling this issue since ECUs are core components inside the vehicle handling various functions simultaneously. The bus may be heavily loaded during key exchange and pre-loaded keys in the ECUs can tackle this situation in key distribution environment.

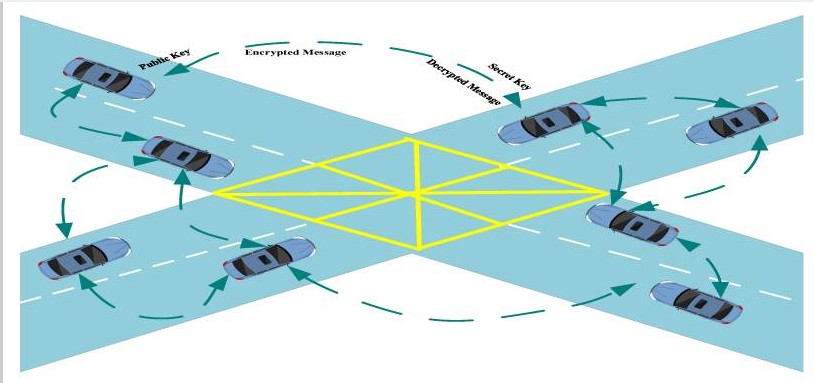


Fig. 20.

The Hardware Security Module (HSM) in ECUs can be effectively utilized for performing encryption and decryption in optimal time and compensating the issue of resource con- strained ECUs.

# Survey of Security Solutions Based on Machine Learning Algorithms

In today’s world of wireless networks, machine learning (ML) approaches are considered as the most promising choice for handling security-related issues. Researchers are proposing solutions utilizing ML to deal with vehicle security issues. Ma- chine learning (ML) approaches have significant advantages as compared with other mechanisms, one of the main important features is to get optimal predictions about several types of attacks. The use of machine learning model in intrusion detection.

# Multi-Layered Security Framework

The developing scene of cutting edge vehicles, set apart by mind boggling in-vehicle design and delicate electronic parts, requires a vigorous and coordinated network safety system. This proposed system embraces a multifaceted methodology, fastidiously tending to both digital and actual dangers innate in present day in-vehicle correspondence organizations. Shown in Figure 13, the system contains six layers, each committed to explicit security perspectives: ECU-boot level security, ECU to ECU correspondence, areas/sub-spaces correspondence, ap- plication programming updates or form issues, passage se- curity regulator, and vehicle to outer administrations. These layers aggregately brace the online protection stance of the vehicle, accentuating the honesty of the whole organization. The choice of auto conventions for each layer depends on their viability and appropriateness in giving usefulness inside the mind boggling design of current in-vehicle frameworks. This coordinated methodology fills a basic hole in the space, offering a custom fitted and powerful protection against a

range of digital and actual interruptions, guaranteeing a far reaching security procedure for the unpredictable idea of contemporary auto frameworks.

The multi-layered security framework for modern vehicles is meticulously designed to address a spectrum of security challenges inherent in the intricate in-vehicle communication networks. Each layer serves a distinct purpose, collectively contributing to the overall cybersecurity posture of the vehicle.

1. CONTROL PLATFORM LAYER:

**Objective:** Enhance the security of the vehicle’s platform, focusing on protecting ECU firmware, improving boot-level security, and safeguarding hardware modules.

•

**Key Measures:** Interaction between OEM trusted server and TPM chip for secure firmware updates, regular updates with secure signing and flashing mechanisms.

•

1. SECURE ECU TO ECU COMMUNICATION LAYER:

**Objective:** Ensure integrity in message exchanges be- tween ECUs, safeguarding sensitive information from potential cyber threats.

•

**Key Measures:** Implementation of an HSM chip as a security controller, responsible for authentication, encryp- tion/decryption, and secure storage.

•

1. RELIABILITY AND PRIVACY OF COMMUNICATION BETWEEN DOMAINS/SUB-DOMAINS LAYER:

**Objective:** Maintain secure communication within dif- ferent vehicle domains and sub-domains, employing crypto- graphic certificates, encryption, intrusion detection, and ECU- level validation.

•

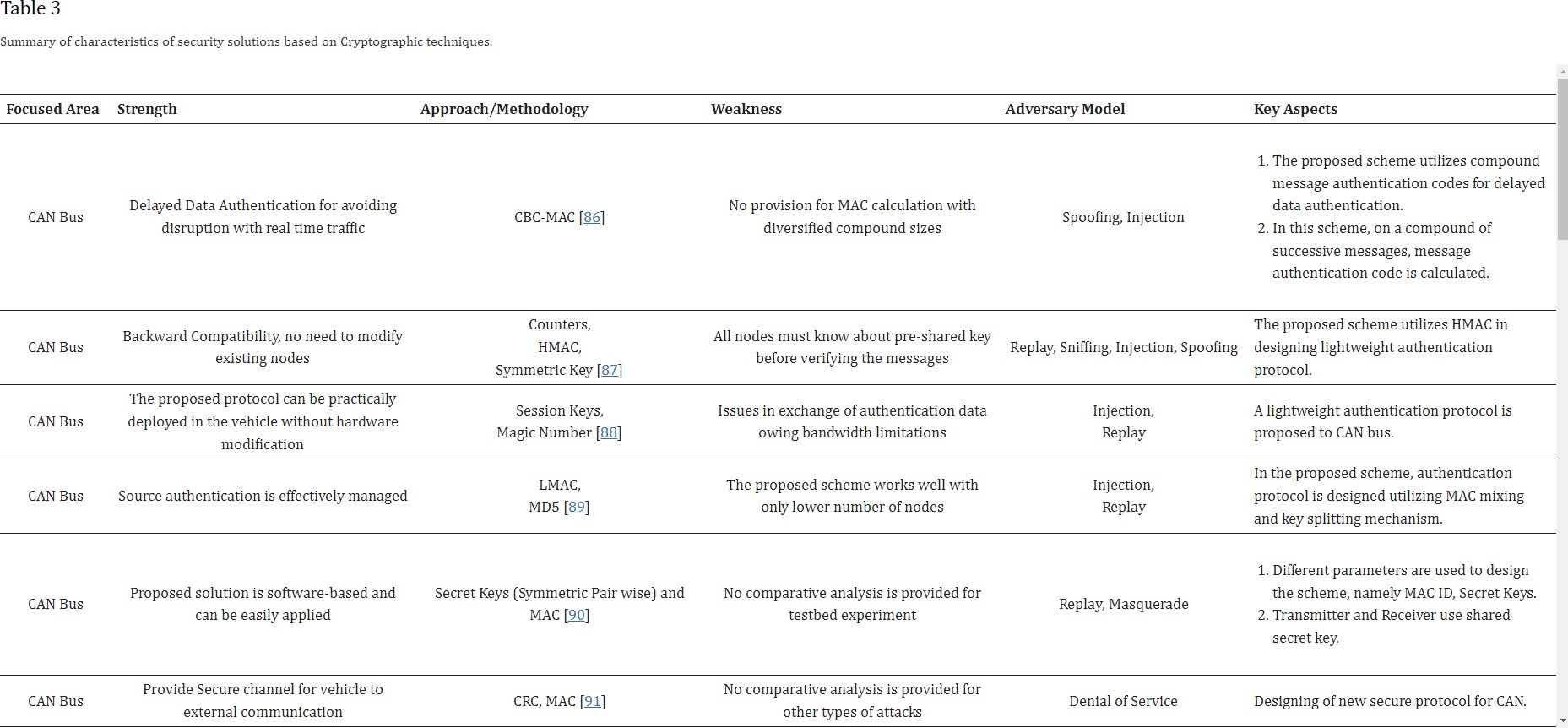


Fig. 21.

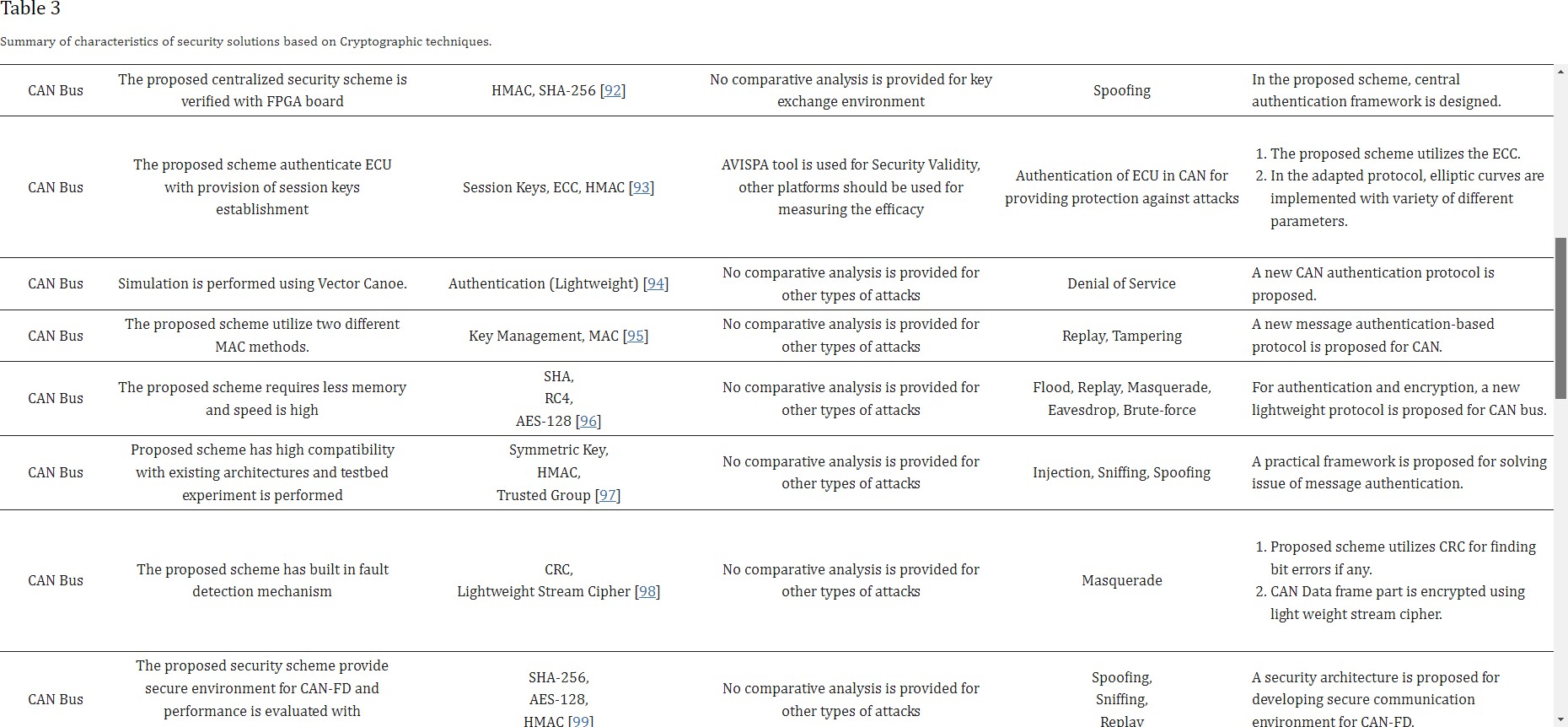


Fig. 22.

1. APPLICATION SOFTWARE RELIABILITY AND

AUTHENTICITY LAYER:

1. SECURE GATEWAY/DOMAIN CONTROLLER LAYER:

**Objective:** Address the security of software updates and downloads, ensuring immediate updating of vehicle software upon detecting vulnerabilities.

•

**Key Measures:** Verification and uploading of third-party developed application software by the OEM’s trusted server, secure storage, and communication channel security.

•

**Objective:** Protect the vehicle’s gateway and domain controller, incorporating advanced security mechanisms like key management, firewalls, and intrusion detection systems.

**Key Measures:** Context-aware routing for message vali- dation, Secure Hardware Extension (SHE) chip, and protection of cryptographic credentials managed by PKI.

•

•

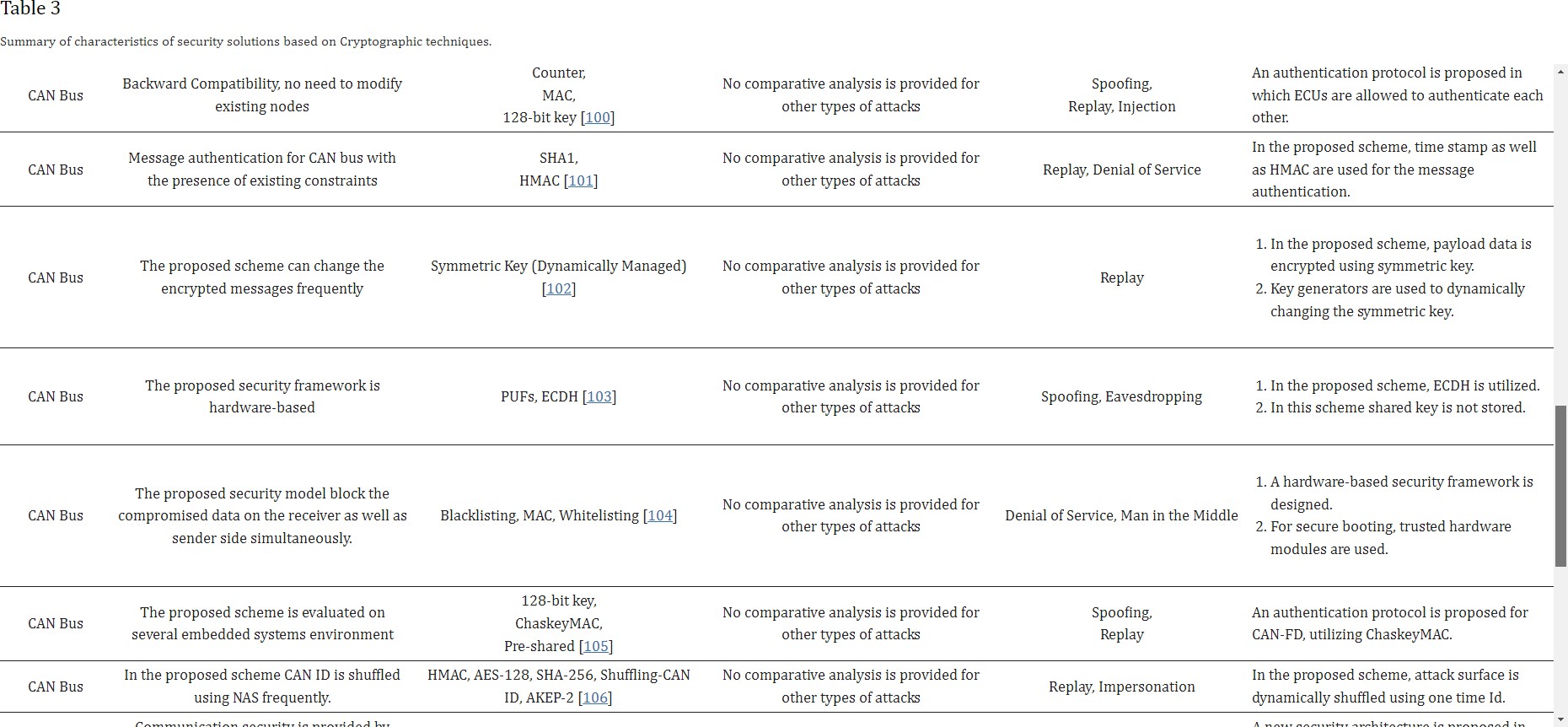


Fig. 23.

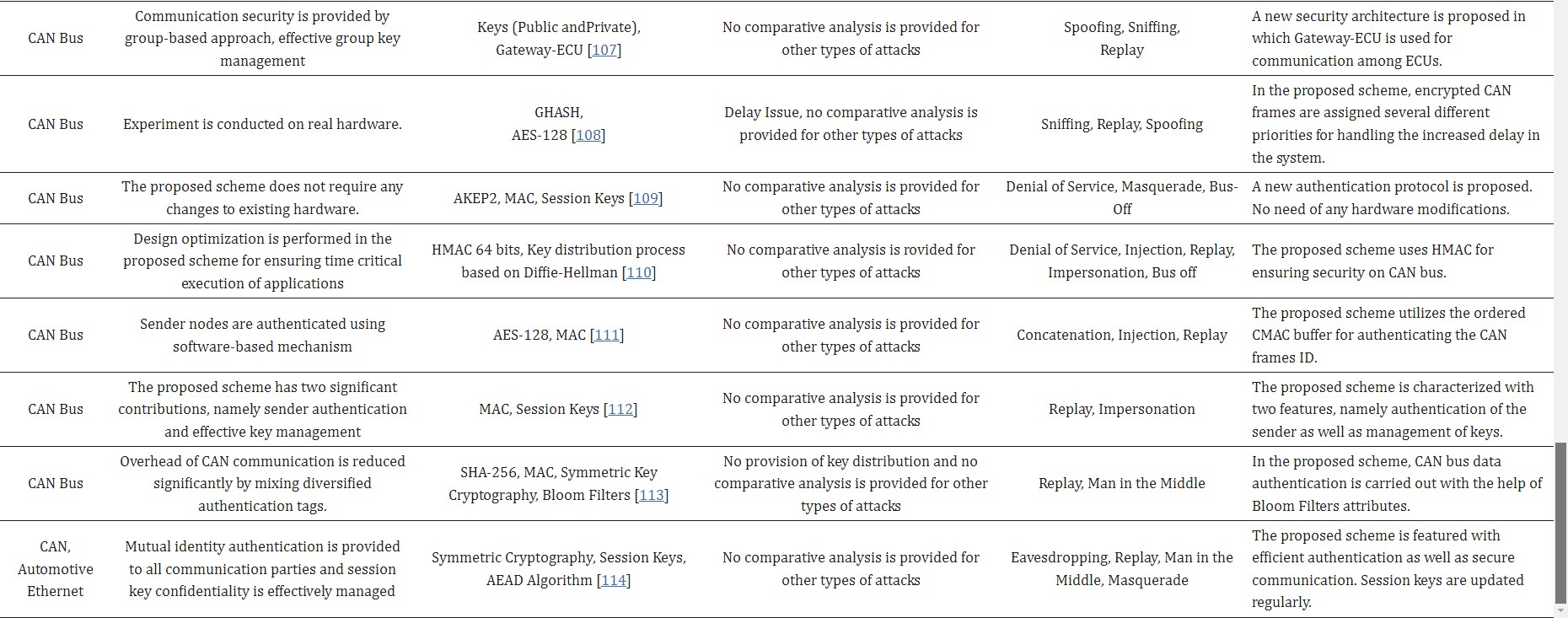


Fig. 24.

1. SECURE EXTERNAL COMMUNICATION LAYER:

**Objective:** Ensure the security of communications from the in-vehicle network to external services, implementing crucial authentication and message validation functions.

•

**Key Measures:** Trusted communication authority (TCA) for securing communication channels to external services, frequent certificate updates, and digital signatures.

•

# Open Issues and Future Directions :

In the previous section, we review malware detection ap- proaches that have been proposed in the last decade based on the method used, the analysis method used, the target operating system, the detection and the response times, the data source, the main benefits and drawbacks of each method. In this section, we first discuss the limitations of applying these

approaches in securing and protecting the intelligent vehicles against malware. Second, we discuss the security requirements that are needed in order to provide a successful and secure intelligent vehicle system. Finally, we summarize and discuss open research problems for the scientific community to address in order to meet the security requirements that are needed for a successful and secure intelligent vehicle system, and offer some recommendations for developing a more successful detection schema against malware for intelligent vehicles.

# Existing Techniques Limitations in Securing Intelligent Vehicles Against Malware :

•

Despite the fact that malware detection techniques are improving day over day, the following limitations of applying these malware detection techniques to intelligent vehicles

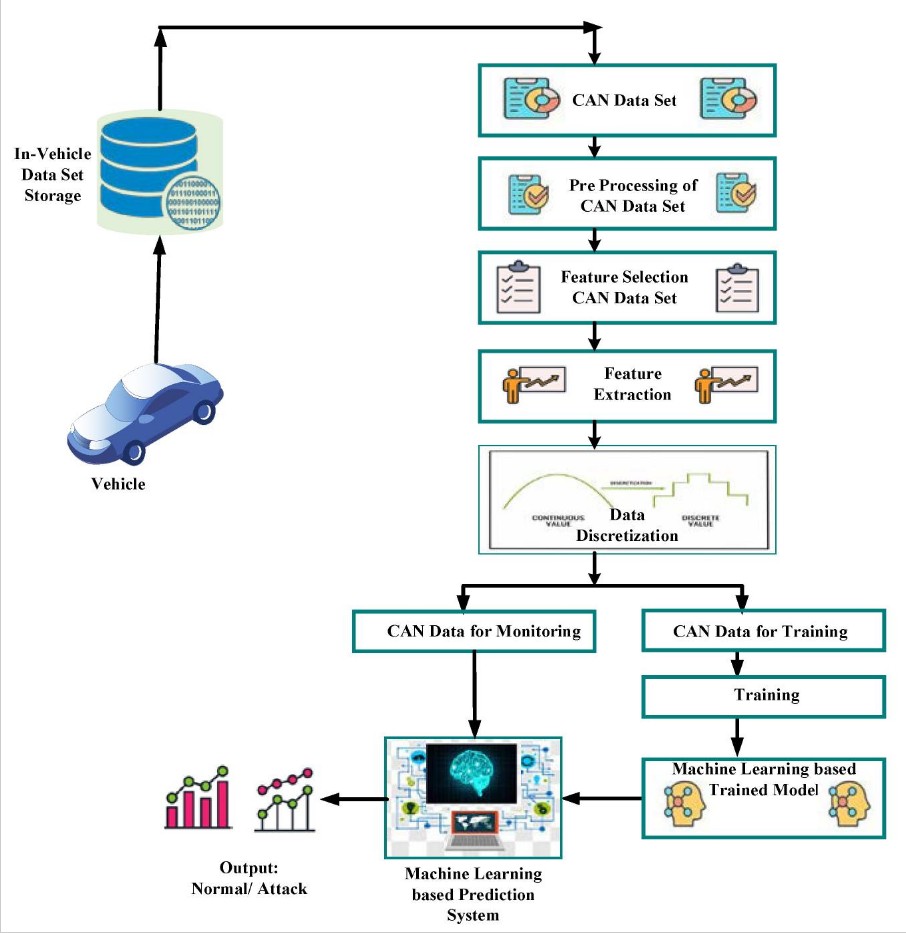


Fig. 25. 4 Intrusion Detection) General Flow Diagram reflecting series of steps for intrusion detection using machine learning model.

remain an unresolved issue.

Existing ways to deal with malware identification face huge weaknesses because of the assorted jumbling and avoid- ance procedures utilized by arising malware ages. Different avoidance procedures are used to mask malware, making it trying for regular discovery techniques. For example, particular sorts of malware embrace choked execution to get away from identification, a procedure that can be applied in vehicles to dial back movement across various Electronic Control Units (ECUs). Also, malware takes advantage of cutting

•

edge equipment elements, for example, multi-center processors and hyper-stringing to spread its exercises across centers, intending to outperform preventive measures. In the auto setting, this means spreading malware across different ECU strings. Furthermore, malware may present sham directions, use guidance replacement, code interpretation, or subroutine reordering to modify its appearance and hinder appropriate examination. The versatile idea of these avoidance methods renders current methodologies unacceptable for wise vehicles, where guaranteeing traveler security requests powerful and

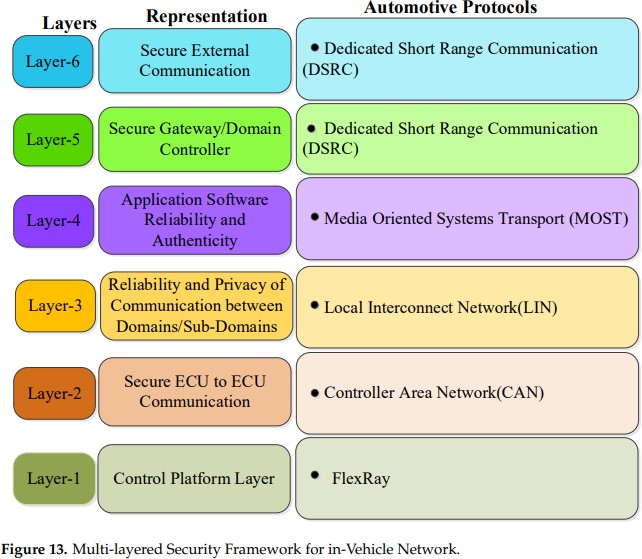


Fig. 26.

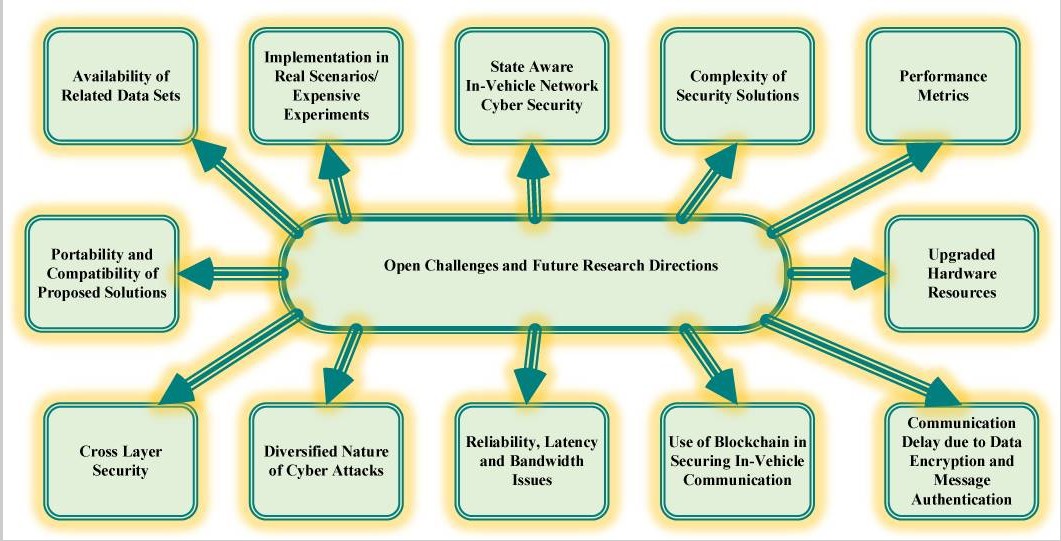


Fig. 27.

modern answers for successfully counter advancing malware dangers..

All of the current approaches might fail to detect new malware generations, as well as sophisticated malware. As a result, these approaches are inappropriate for use in intel- ligent vehicles due to concerns regarding driver safety and passengers as well. Furthermore, with the exception of cloud- based approaches, all approaches cannot be used for intelligent vehicles since they need to be updated regularly in order to handle any potential new malware during the vehicle’s long lifespan. Besides, updating them on a regular basis on millions of vehicles would be difficult to handle and can be costly for both vehicle owners and automakers. Cloud-based approaches have an edge over other approaches since all installations and configurations are updated on a regular basis in the cloud. Therefore, we believe cloud-based malware detection will be a feasible solution for safeguarding intelligent vehicles against malware attacks in the future especially with the advent of high speed 5G technology.

•

Malware detection in real-time is really challenge. The majority of malware detection approaches in the last decade have been proposed and validated to detect malware using datasets and are not suitable for real-time detection. The issue with these non-real-time approaches is that they are unsuitable for intelligent vehicles because if the vehicle is infected with malware, the malware must be detected in real- time in order to ensure the safety of the drivers and passengers.

•

There is no well-known and widely recognized dataset that can be used to assess the effectiveness of malware de- tection methods. Despite the fact that each malware detection technique has its own set of advantages and disadvantages, however, it is difficult to say that one is more effective than the other. This is due to the fact that each malware detection technique uses different malware and dataset.

•

According to our findings, we observe that there are only two malware detection methods that can detect malware in real time. However, these methods need a lot of computational resources, which make them infeasible for intelligent vehicles due to the limited computational resources of the ECUs and CAN bus. Furthermore, these methods are not cost-efficient and are not adaptable for intelligent vehicles since they need a sophisticated hardware modification. As a result, these meth- ods may not be suitable for resource-constrained in-vehicle devices that also need to be lightweight.

•

All present IDS approaches cannot identify malware attacks at the application level, but they may detect malware attacks at the data link layer or physical layer after the actual damage has likely happened. As a result, in addition to the need for an effective IDS for intelligent vehicles at the data link and physical layers, modern cars also require an effective defense system at the application layer in order to safeguard them against malware.

•

**:** • **Security Requirements to Securing Intelligent Vehicles** In this section, we discuss four essential requirements for securing intelligent vehicles. These are critical security criteria for every communication system. These requirements

are authentication, integrity, privacy, and availability. Each requirement is presented below along with its description.

**Authentication: -** It means that the access to any infor- mation or vehicle’s data must be given to the only authorized users and parties. By giving authorization to specific users and parties to access any information or vehicle’s data, malware attacks and unauthorized manipulations can be prevented from happening. In this way, vehicle’s network system can be more protected by only giving authorization to a certain users and parties. The key management and distribution must be efficient and accurate in order to meet this requirement.

•

**Integrity: -** It is referred to the validity of data between the sender and the recipient of a communication system. The most basic criterion of communication system integrity is that the data received is correct and not tampered with intention- ally. It is important to check the honesty of the message that is being sent in the vehicle’s network system. The message has to get validated to make sure that it hasn’t been manipulated or corrupted by a malware, or some other factors such as noise and fading. Error detection and correction codes must be developed to ensure the integrity of any communication system.

•

**Privacy: -** Intelligent vehicles tend to share informa- tion with each other (such as Vehicle-to-Vehicle communi- cation) and between the surrounding infrastructure (Vehicle- to-Infrastructure communication). Therefore, privacy plays a big factor in this role to protect vehicle’s information from being used to do unauthorized behaviors such as using the information to spy on vehicles and access its private data.

•

**Availability: -** It is referred to the fact that authorized users have access to the systems and resources they need. Improving the chances of all targeted vehicles receiving in- formation is critical in vehicular networks. Continuous avail- ability is tough to accomplish under normal working settings, and it gets more and more challenging when updates and patches are required at various points. It is critical that network activities continue and that the cars remain unaffected. The availability of services at all times is critical. As a result, the needed redundancy for this purpose must be appropriately implemented.

•

*A. Recommendations and potential future directions for en- hanced security*

One of the biggest challenges that automakers face is finding solutions against malware attacks and creating a full immunity system to combat this threat. Although the existing defenses are some of the most effective approaches of building structural defenses against malware attacks, there are still some challenges and issues that need further investigation and study. There are additional potential solutions that could be implemented to provide a great protection and immunity against malware attacks. Some additional potential solutions and directions that will enhance intelligent vehicles’ security that need to be addressed to meet the security requirements to securing intelligent vehicles are presented below.

1. AUTHENTICATION SYSTEM USING LI-FI TECHNOLOGY: -

Carrying out a lightweight cryptographic validation frame- work is critical for upgrading security in keen vehicles. This framework guarantees a safe, proficient, and versatile way to deal with address complex transportation situations. Key headways in key extraction through remote blurring chan- nels, key foundation utilizing keyless cryptography, and key circulation by means of Li-Fi innovation grandstand huge advancement. Li-Fi, with its capacity to accomplish rapid remote correspondence surpassing 3 Gb/s and giving upgraded security by forestalling capture, stands apart as a promising part for canny vehicle confirmation. Coordinating Li-Fi into vehicle configuration can add to a solid and productive ver- ification framework, meeting fundamental security rules for hearty insurance.

1. FIREWALL SYSTEM: -

Although malware attacks can be destructive to intelligent vehicles with its different entry points, there are many ways that can be implemented to defend against malware attacks. Intelligent vehicle’s system tends to receive updates more often. Therefore, the liability of the source that is sending that information must be checked to make sure malware doesn’t get injected in the intelligent vehicle’s network. A network security device such as firewall should be implemented to monitor and block unwanted data. The firewall’s main purpose is to filter any data that enters the system and rejects malware attack vectors that have been recognized as a threat. Alongside with applying a network security device, security requirements need to be satisfied in order to provide a successful and secure protection to the vehicle’s system.

1. DEEP LEARNING USING OFFLOADING COMPUTATION MECHANISM: -

Intelligent deep learning such as neural networks technol- ogy is a great way to detect vulnerabilities and eliminate malware attacks in intelligent vehicle systems. Because the fact that this technology is more accurate and performs better than machine learning technology in malware detection, it is worth considering this advanced technological approach for intelligent vehicle systems. Deep learning, on the other hand, requires a lot of computing resources and capabilities in the vehicle’s ECUs, which leads to memory overloading for deep learning implementation in ECUs owing to the vehicle’s ECUs’ limited computation resources. However, the offloading computation mechanism was found to be a possible solution to solve the limited computation resources of the vehicle’s ECUs by transferring the resource intensive computational tasks to a separate processor such as an external platform, a hardware accelerator, a cluster, grid, or cloud server at the network edge. The future of intelligent vehicles is quite promising with deep learning using offloading computation mechanism towards faster and secure vehicle system.

1. SOFTWARE DEFINED SECURITY: -

Intelligent vehicles need to be able to detect malware attacks efficiently and effectively. Therefore, the software defined security system can be a reliable solution to detect and elimi- nate malware threats and further improves network security for intelligent vehicles by forwarding the security threats characteristics and traffic parameters for forensic analysis. The software defined security is referred to the use of software defined platforms to automate threat detection and mitigation. This can be accomplished by adopting an open flow protocol, Network Function Virtualization (NFV) and Software-Defined Networking (SDN) that uses multi-layered open virtual switch with programmatic extension principle that allows automation of threat detection and elimination on a bigger scale. This form of dynamic solution to threats will provide security for intelligent vehicles against malware attacks.

1. CLOUD-BASED SOLUTION USING 5G TECHNOLOGY: -

The combination of cloud arrangements with headways in quick 5G innovation presents a promising future for savvy vehicles, offering benefits like consistent access, on-request capacity, and cost-viability. This approach smoothes out re- freshes for establishments, settings, and arrangements, up- grading the effectiveness of savvy vehicle frameworks. The cloud turns into a critical asset in addressing difficulties connected with malware discovery, utilizing broad datasets and hearty figuring assets. Furthermore, distributed storage settle asset assignment issues, permitting information from each Electronic Control Unit (ECU) to be put away and handled in the cloud. The fast reception of 5G changes the reasonability of cloud-based arrangements, empowering quick and secure correspondence for information capacity and handling. The eventual fate of savvy vehicles shows up splendid, with cloud arrangements and 5G innovation improving framework speed and security. Looking forward, the vision of completely mechanized driving, pushed by self-driving frameworks and profound learning calculations, addresses a historic objective, promising a groundbreaking change in the car scene and a connecting with transportation experience in our day to day routines.

**Trained Model Errors:** - Self-driving vehicles rely on a deep learning model-based perception system to identify objects and drive autonomously on their own. However, due to algorithm bugs or model errors, the perception system in a self-driving vehicle may misclassify objects and lead to fatal car incidents. One recent example is the Uber self driving vehicle incident a self-driving vehicle misclassified a pedestrian as other objects and failed to break in time to prevent the collision. Therefore, the first new threat in fully automated self-driving vehicles would be the errors in the implemented in the trained deep learning model. In such a safety-critical system, it is crucial to make sure that the trained model for object identification and classification is robust and bug-free.

•

**Adversarial Examples:** - Besides the errors in the trained deep learning models, misclassification can also be triggered

•

by specially crafted adversarial inputs. This new threat is much more serious than inherent model bugs/errors because an outside attacker can trick the self-driving vehicle to actively deviate from the correct actions by inputting adversarial. For example, as demonstrated in a recent work, an attacker can deceive a self-driving vehicle by deliberately generating toxic signs alongside the road, causing the trained deep learning model to misclassify signs and drive recklessly. Consequen- tially, such a severe threat from adversarial examples, if not carefully addressed, would lead to potentially life-threatening consequences.

**Model Training Privacy:** - Training an accurate deep learning model for self-driving vehicles requires a very large dataset of road images or real driving videos as learning inputs. Thus, continuously contributing learning inputs collected from self-driving vehicles is essential to make the deep learning model robust and accurate in real deployments. However, most current model training infrastructures are centrally structured, which means that the input data from self-driving vehicles are transferred to a centralized server transparently. Since the contributed learning dataset is closely related to daily lives, it might reveal sensitive information of people, e.g., routine, locations, etc. Besides, according to a recent study, the trained deep learning models can also leak sensitive information of the data contributors.

•

**Model Execution Threats:** - In the implementation of fully automated self-driving systems, many new designs of hardware like TPU (Tensor Processing Unit), GPU, ASIC (Application-specific Integrated Circuit) and FPGA (Field Programmable Gate Array), are incorporated inside the au- tonomous vehicles for achieving lightweight and efficient deep learning. Existing systems construct a new central operating component inside the self-driving vehicle for controlling the hardware to work seamlessly without mutual intervention. However, similar to in-vehicle systems, such a central op- erating component might subject to malicious attacks, e.g., malware injections, and thus can hardly guarantee the cor- rectness of model executions. Therefore, such an operating system should be modeled as an untrusted environment whose attack surface may be easily leveraged by the attackers, and advanced defense mechanisms should be deployed for ensuring execution integrity in self-driving vehicles.

•

# Defense Strategies

•

We briefly discuss the strategies for defending against the aforementioned security threats in fully automated self-driving vehicles.

1. **DNN Robustness Improvement:** In order to improve the robustness and reduce errors of deep learning models, we could conduct comprehensive testing on those trained models. Existing testing of trained models for self-driving vehicles is mostly based on either
2. measuring and analyzing the recognition error over a newly-inputted learning dataset, or running real driving tests on the road and giving attention to disengagements, i.e., the incidents where the self-driving vehicle cannot decide. In the future, the testing procedures of deep learning models could be more automatic. When an error is detected, the system can automatically retrain the model for improving accuracy.

Also, the testing can be extended to real-time, so that errors can be continuously monitored during model execution, and automatically patched to further enhance driving safety.

1. **Adversarial Example Defense:** To address adversarial examples that can trick the deep learning model into behaving what the attacker wants, the first possible defense strategy is to pre-process or filter of input data so as to detect and eliminate the adversarial examples before executing. For example, we can use standard blurring techniques, e.g., Gaussian blur, to let our trained model “escape” from adversarial examples. Another useful defense strategy is to generate adversarial examples or detect potential adversarial examples using data mining methods, and then re-train the model with these generated adversarial examples to make the deep learning model more robust. Lastly, we can also try to enhance the interpretability of underlying deep learning models. In this way, we can closely monitor the model execution procedures and detect incorrect driving decisions in time to prevent fatal accidents.
2. **Data Privacy Preservation:** To provide privacy of the contributed training data, one possible strategy is to leverage the emerging federated learning architecture to train and update the deep learning model. With this privacy-enhanced architecture, the sensitive inputs for model training never leave the self-driving vehicles, and only model parameter updates are sent to the server for model converging and updating. As a result, the private training data from all self-driving vehicles can be protected during the model training and updating process. Specific configurations could be set to minimize mem- orization during training to prevent data leakage. In particular, one potential strategy for defending against memorization is by adding the chosen noise carefully to each gradient update during learning, so as to make the trained models differentially private. In this way, we can effectively hide the occurrence of some private information in the trained models and can thus prevent an attacker from extracting them by abusing model memorization.
3. **Execution Integrity Enhancement:** To enhance the exe- cution integrity inside the self-driving vehicle, we can leverage Trusted Execution Enclave (TEE) to construct a secure and isolated environment for executing integrity-critical driving decisions and learning. Currently, available TEE constructions are implemented in CPUs manufactured by Intel and. In the near future, we can further design enclaves for new hardware, from GPUs to ASIC circuits, so that both performance and execution integrity are guaranteed at the same time in a self- driving vehicle.

XL. CONCLUSION

1. *Key Takeaways from the Surveyed Literature:*

**Vulnerability to Evasion Techniques:** A significant issue with existing malware detection methods is their suscepti- bility to evasion. Modern malware uses various obfuscation techniques, like throttling execution across multiple Electronic Control Units (ECUs) or leveraging multi-core processors to spread activities and avoid detection. These methods can make malware difficult to analyze and, consequently, evade existing

•

detection systems. This vulnerability is particularly concerning in the context of intelligent vehicles, where passenger safety is paramount.

**Challenges in Detecting New Malware:** The current approaches struggle to identify new, sophisticated malware forms, posing a risk to driver and passenger safety in intel- ligent vehicles. Most traditional detection methods also face challenges in staying updated over a vehicle’s lifespan, making them impractical due to the high costs and logistical complex- ities involved in updating millions of vehicles regularly. In contrast, cloud-based approaches, which update configurations regularly in the cloud, are seen as more viable, especially with the emergence of high-speed 5G technology, offering a more adaptable and up-to-date defense against malware.

•

1. *Areas for Future Research and Development:*

Security Requirements for Intelligent Vehicles: To secure in- telligent vehicles effectively, four critical security criteria need to be met: authentication, integrity, privacy, and availability. Authentication ensures that only authorized users can access vehicle data, thereby preventing unauthorized manipulations. Integrity involves the validation of data exchanged within the vehicle’s network to ensure it has not been tampered with. Privacy is crucial in protecting the information shared between vehicles and infrastructure from unauthorized use, such as spying. Lastly, availability refers to ensuring consistent access to systems and resources, a challenging but essential aspect in vehicular networks.

Proposed Solutions for Enhanced Security:

**Li-Fi Technology for Authentication:** Implementing a lightweight cryptographic authentication system using Li-Fi technology can provide secure, efficient, and flexible secu- rity, suitable for complex transportation contexts. Li-Fi offers advantages in speed and security over Wi-Fi, making it an attractive option for intelligent vehicle design.

•

**Firewall Implementation:** Integrating firewalls in intel- ligent vehicle systems can help in monitoring and blocking potentially harmful data. Given that vehicles often receive frequent updates, it’s crucial to ensure the reliability of the source of these updates to prevent malware injection.

•

**Deep Learning with Computational Offloading:** Neural networks and deep learning technologies, known for their ac- curacy in detecting vulnerabilities, can be utilized in intelligent vehicle systems. Given the limited computational resources of vehicle ECUs, offloading computational tasks to external platforms or cloud servers can be an effective solution to implement resource-intensive deep learning algorithms.

•

**Software-Defined Security Systems**: Adopting software- defined security, which automates threat detection and mitiga- tion, can significantly improve network security. This approach involves using software-defined networking (SDN) and net- work function virtualization (NFV) technologies to create a dynamic and scalable defense against threats.

•

**Cloud-Based Solutions with 5G Technology:** Using cloud-based solutions, coupled with the advancements in 5G technology, can offer numerous benefits, including regular updates, on-demand storage, and lower costs. It can also

•

enhance malware detection performance with extensive data sets and robust computing resources