**Simran Kaur 40241517**

**Snehpreet Kaur 40254443**

1. **Gateway Framework for In-Vehicle Networks Based**

**on CAN, FlexRay, and Ethernet**

**Abstract:**

This paper introduces a comprehensive gateway framework for In-Vehicle Networks (IVNs) utilizing the Controller Area Network (CAN), FlexRay, and Ethernet protocols. The framework is meticulously designed for easy reuse and verification, aiming to reduce development costs and time. Notably, it offers a configurable architecture, and its verification environment is automatically generated through a program featuring a dedicated graphical user interface (GUI). The gateway framework boasts advanced functionalities, including parallel reprogramming, diagnostic routing, network management (NM), dynamic routing updates, multiple routing configurations, and robust security measures.

**Key Findings and Contributions:**

Platform Independence: The gateway framework is hardware/software platform-independent, enabling developers to easily create and verify gateways while significantly reducing development costs and time.

Reusability and Safety: Experimental verification demonstrates that the proposed gateway framework is reusable, safe, and effective. The evaluation includes theoretical analyses and experimental measurements focusing on end-to-end processing time.

Optimization Insights: The analysis underscores the importance of optimizing both the gateway framework and the network. While efforts are required to enhance the gateway's performance, optimizing the network is deemed crucial for overall improvement.

Applicability: The proposed gateway framework proves beneficial for current automotive systems with a central gateway and holds even more promise for future systems utilizing Domain Control Units (DCUs) as gateways.

Future Work: The authors outline plans to explore a security gateway addressing the separation of the unsafe network domain (V2X) from the safe network domain (IVN), with a focus on preventing security threats that could compromise vehicle safety.

**Conclusion:**

The gateway framework introduced in this paper represents a significant contribution to the development of In-Vehicle Networks. Its platform independence, reusability, and advanced functionalities position it as a valuable tool for current automotive systems and hold great promise for the evolving landscape of future automotive architectures. The insights gained from the analysis emphasize the need for ongoing efforts in both gateway and network optimization to ensure optimal performance. The proposed security gateway for segregating unsafe and safe network domains signals a proactive approach to addressing potential security threats in the automotive domain.

1. **LIN Bus Based Touchpad System for Smart Vehicle Cabin**

**Abstract:**

This paper introduces a LIN bus touchpad system (LBTS) as an innovative solution for creating a smart vehicle cabin, enhancing safety, comfort, and the overall driving experience. The LBTS utilizes a touchpad signal processor with the LIN Bus interface to facilitate efficient access and control of devices such as headlights, taillights, and the cooling fan. The system is designed with a LIN bus-based controller (CS8975) and a high-performance STM32 Nucleo-64 board, providing flexibility and innovation in the interior design of the human-centric cabin.

**Key Features and Implementation:**

LIN Bus Touchpad System (LBTS): The LBTS enables safe and efficient access to devices within the smart cabin, employing a touchpad signal processor and a LIN bus-based controller (CS8975).

Master-Slave Architecture: The STM32 Nucleo-64 CPU serves as the master ECU node, orchestrating the LIN message sequence. Slave ECU nodes control specific end devices, such as headlights, taillights, and the cooling fan, responding to instructions from the master node.

Cost-Effective and Reliable: The LBTS demonstrates the LIN bus's ability to manage cost-sensitive and high-reliable data transmission in automotive applications, particularly for human-centric interactions in next-generation vehicles.

Future Work and Cybersecurity Considerations: The paper highlights possibilities for future work, including exploring cybersecurity vulnerabilities like message spoofing, response collision attacks, header collision attacks, and potential countermeasures.

**Conclusion:**

The LIN Bus-Based Touchpad System (LBTS) proposed in this paper showcases a viable alternative for enhancing the smart vehicle cabin. With a focus on safety, comfort, and flexibility in interior design, the LBTS leverages LIN bus technology to efficiently control essential devices. The master-slave architecture, featuring the STM32 Nucleo-64 CPU, demonstrates effective communication and control within the system. Furthermore, the LBTS highlights the LIN bus's suitability for cost-sensitive and reliable data transmission in automotive applications. The paper concludes by identifying avenues for future research, particularly in exploring cybersecurity aspects and implementing countermeasures to ensure the robustness of the proposed system in next-generation vehicles.

1. **Flexible Approach to the Controller Area Networks Test**

**and Evaluation**

**Abstract:**

The surge in Electronic Control Units (ECUs) within modern vehicles, coupled with increased communication traffic, has prompted car manufacturers to partition a single Controller Area Network (CAN) into dedicated sub-networks. While existing test and evaluation tools cater to scenarios with up to two CAN networks, their limitations include reliance on standard CAN hardware and a constrained test functionality. This paper introduces a groundbreaking solution—a set of IP functions comprising a CAN generator, CAN trigger unit, and time-triggered CAN controller. These IP functions, implemented in FPGA-based test tools, facilitate real-time testing across an unlimited number of CAN sub-networks.

**Key Features and Innovations:**

Multi-Network Testing Platform: The paper presents a flexible testing platform designed for CAN-based ECUs and systems, offering support for an arbitrary number of CAN sub-networks simultaneously.

IP Functions for Real-Time Testing: Three IP functions—CAN generator, CAN trigger unit, and time-triggered CAN controller—are introduced, enabling the development of multi-network test sites with ease and speed.

Low Host Service Requirements: Thanks to strong hardware support for inter-function synchronization and event time stamping, the real-time requirements for the host service are minimal.

FPGA Implementation for Configuration: Concrete configurations are implemented in the FPGA, providing the flexibility to add hardware support for additional features or other bus types like LIN or FlexRay.

Application Examples: The paper showcases the designed platform's application through examples, demonstrating its versatility in addressing the evolving testing needs of complex in-vehicle networks.

**Conclusion:**

This work pioneers a flexible approach to Controller Area Networks (CAN) test and evaluation, offering a solution to the challenges posed by the increasing number of Electronic Control Units and communication traffic in modern vehicles. The introduction of three IP functions—CAN generator, CAN trigger unit, and time-triggered CAN controller—proves instrumental in enabling real-time testing across numerous CAN sub-networks. With a focus on FPGA implementation, the platform not only meets current testing requirements but also provides a foundation for accommodating future features and diverse bus types. The presented examples underscore the platform's practical application, positioning it as a valuable tool for car manufacturers navigating the complexities of multi-network testing in contemporary automotive systems.

1. **A Hybrid Approach for Fast Anomaly Detection in**

**Controller Area Networks**

**Abstract:**

As in-vehicle networks and wireless communication technologies continue to advance, modern automobiles have evolved into sophisticated cyber-physical systems. This paper addresses the crucial need for securing Controller Area Networks (CAN) in vehicles by proposing a hybrid anomaly detection system. The system relies on identifying patterns of recurring messages and analyzing the time intervals between messages on the CAN bus. Unlike some existing methods, our approach requires no modifications to the CAN bus itself. The effectiveness of the proposed system is demonstrated through evaluation on real CAN bus traffic, including simulated attack scenarios, showcasing a robust detection rate with rapid response times.

**Key Features and Methodology:**

Hybrid Anomaly Detection Model: The proposed system leverages a hybrid approach, combining the analysis of recurring message patterns and timing intervals, to identify anomalies in the CAN bus.

Evaluation on Real CAN Bus Traffic: The system's performance is assessed using real CAN bus traffic and simulated attack scenarios, demonstrating its efficacy in achieving a high detection rate.

No CAN Bus Modifications Required: A notable advantage of the proposed method is its non-intrusive nature, requiring no modifications to the CAN bus infrastructure.

Feasibility and Fast Response Times: The paper establishes the feasibility of the proposed approach on embedded devices, emphasizing fast response times crucial for real-time anomaly detection.

Future Work: The authors acknowledge future work to address false positives, particularly when using large window sizes. Additionally, the intention is to explore additional features that can enhance overall accuracy without compromising response time.

**Conclusion:**

This work introduces a hybrid anomaly detection system for Controller Area Networks (CAN) in modern vehicles, contributing to the robust cybersecurity of automotive systems. By focusing on recurring message patterns and timing intervals, the proposed approach achieves a commendable detection rate without necessitating modifications to the CAN bus. The evaluation on real-world CAN bus traffic underscores the system's effectiveness, emphasizing rapid response times. Acknowledging areas for improvement, the paper outlines future work aimed at reducing false positives and enhancing accuracy, ensuring the ongoing relevance and reliability of the proposed anomaly detection system in securing the evolving landscape of in-vehicle networks.

**5)Development of a Controller Area Network Interface Unit and Its Application to a Fuel Cell Hybrid Electric Vehicle**

**Abstract:**

This paper introduces a Controller Area Network (CAN)-based network interface unit designed for studying power train control timing in fuel cell hybrid electric vehicles. With a focus on the communication needs of next-generation vehicles, especially fuel cell electric vehicles, the paper emphasizes the importance of efficient data exchange among subsystems or Electronic Control Units (ECUs) to enhance fuel economy and safety. Addressing the potential challenges of transmission delays on the data bus, a straightforward method is proposed, utilizing a holistic scheduling approach to adapt controller sampling periods. The application of this interface unit in an experimental setup for a fuel cell hybrid electric vehicle demonstrates its effectiveness in resolving transmission delay issues caused by task prioritization.

**Key Contributions and Findings:**

Communication Efficiency for Next-Gen Vehicles: The paper underscores the necessity of robust communication between subsystems or ECUs in advanced vehicles, such as fuel cell electric vehicles, to optimize fuel economy and safety.

Transmission Delay Mitigation: A method for dynamically adjusting controller sampling periods is proposed, offering a solution to unexpected transmission delays that could lead to unstable vehicle operation.

Experimental Application: The presented CAN-based interface unit is applied to an experimental setup for a fuel cell hybrid electric vehicle, showcasing its capability to resolve transmission delay problems associated with task prioritization.

Timing Analysis Method: The paper introduces a simple yet effective timing analysis method, employing a PCI-CAN board and a Windows platform-based monitoring program to calculate computation and communication times for each task.

Worst Case Response Time: The study determines the worst-case response time for stable vehicle operation, providing insights into establishing appropriate sampling periods.

**Conclusion:**

This work contributes a CAN-based network interface unit designed to address critical timing issues in the power train control of fuel cell hybrid electric vehicles. By presenting a straightforward method for adapting controller sampling periods based on holistic scheduling, the paper tackles transmission delay challenges that could compromise vehicle stability. The experimental application of the interface unit in a fuel cell hybrid electric vehicle setup validates its effectiveness in resolving transmission delay problems caused by task prioritization. The introduced timing analysis method, along with insights into worst-case response times, enhances our understanding of establishing optimal sampling periods for stable vehicle operation in the context of evolving automotive technologies.

**6) Controller Area Network Modeling and Its Application in Cyber-Physical Power System Co-Simulation**

**Abstract:**

This paper presents a comprehensive exploration of Controller Area Network (CAN) modeling and its application in power system control, focusing on the development of a simulation model within the OPNET network simulator. The model encompasses the node, process, packet, and link components, establishing a hierarchical structure for effective representation. Through simulations, the paper validates the effectiveness of the CAN model. Furthermore, the study proposes a cyber-physical power system co-simulation platform, integrating OPNET and PSCAD. Detailed illustrations of the interfaces between these simulators and the time synchronization method are provided. The CAN model is adapted with the OPNET ESYS module to seamlessly integrate it into the co-simulation platform.

**Key Contributions and Findings:**

OPNET Simulation Model: The paper meticulously designs and builds an OPNET simulation model for the CAN bus, delineating the hierarchical structure that includes node, process, packet, and link models.

Functionalities Implementation: The CAN bus LLC (Logical Link Control) and MAC (Media Access Control) sublayer functionalities are implemented within the model, covering packet sending and receiving, bus state monitoring, and arbitration.

Validation through Simulation: The effectiveness of the designed CAN model is rigorously validated through simulations, ensuring its accuracy and reliability in representing CAN bus dynamics.

Cyber-Physical Co-Simulation Platform: A cyber-physical power system co-simulation platform is proposed, leveraging OPNET and PSCAD. The study details the design of data interfaces and a synchronization method crucial for successful integration.

Applicability in Power System Co-Simulation: Both the CAN bus model and the co-simulation platform are deemed applicable in the context of cyber-physical power system co-simulation, enhancing the understanding of power system dynamics.

**Conclusion:**

This work contributes a detailed simulation model of the Controller Area Network (CAN) within the OPNET network simulator, offering insights into the hierarchical structure and functionalities of the CAN bus. The validation of the CAN model through simulations establishes its accuracy and reliability. The paper further proposes a cyber-physical power system co-simulation platform based on OPNET and PSCAD, presenting interfaces and synchronization methods for effective integration. The adapted CAN model, equipped with the OPNET ESYS module, seamlessly integrates into the co-simulation platform, demonstrating its applicability in cyber-physical power system co-simulation scenarios. Overall, this study advances the understanding and application of CAN modeling in the context of power system control and co-simulation.

**7) Controller Area Network With Flexible Data**

**Rate Transmitter Design With Low**

**Electromagnetic Emission**

**Abstract:**

This paper addresses the design of a Controller Area Network with Flexible Data Rate (CAN-FD) transmitter that emphasizes low electromagnetic emission (EME) and improved voltage symmetry on the CAN bus. The introduction of CAN-FD for higher data rates in automotive systems necessitates robust electronic functions, and this study proposes a novel transmitter design to achieve these goals. The design incorporates a "Ping-Pong" driving scheme for precise turn-on/off timing without the need for complex circuits or post-calibration processes. Fabricated using a 0.18 μm automotive Bipolar-CMOS-DMOS process, the proposed CAN-FD transmitter demonstrates enhanced voltage symmetry at 5 Mbps, resulting in reduced EME.

**Key Contributions and Findings:**

Low EME CAN-FD Transmitter: The paper introduces a CAN-FD transmitter design focused on minimizing electromagnetic emission (EME), crucial for ensuring the robustness of electronic systems in intelligent automotive applications.

Ping-Pong Driving Scheme: A unique "Ping-Pong" driving scheme is implemented in the transmitter to precisely match turn-on/off timing of power driver states and improve voltage symmetry on the CAN bus signals.

Fabrication and Process: The proposed CAN-FD transmitter is fabricated using a 0.18 μm automotive Bipolar-CMOS-DMOS process, ensuring compatibility with automotive electronic systems.

Measurement Results: Evaluation through common mode FFT and conducted EME tests demonstrates that the proposed transmitter outperforms conventional switch transmitters in matching voltage symmetry at a 5 Mbps data rate.

Successful Verification: The proposed CAN-FD transmitter is successfully verified to enhance voltage symmetry on the CAN bus and reduce electromagnetic emission, contributing to the robustness of electronic functions.

**Conclusion:**

This work presents a novel CAN-FD transmitter design with a focus on minimizing electromagnetic emission and improving voltage symmetry on the CAN bus. The introduction of a "Ping-Pong" driving scheme provides a simple yet effective method for accurate turn-on/off timing without the need for complex circuits or post-calibration processes. Fabricated using a 0.18 μm automotive Bipolar-CMOS-DMOS process, the transmitter demonstrates improved voltage symmetry at 5 Mbps, leading to reduced electromagnetic emission. The measurement results affirm the efficacy of the proposed design in outperforming conventional switch transmitters. This study contributes to advancing the robustness of electronic functions in automotive systems relying on CAN-FD technology.

**8)Research on the Time Delay of Controller Area**

**Network for Vehicle**

**Abstract:**

This research delves into the critical aspect of time delay within the Controller Area Network (CAN) – a pivotal component in the evolution of vehicle networks towards connectivity and intellectualization. As vehicles become more reliant on networked systems, challenges related to reliability and real-time performance arise, especially with the escalating network load. The study focuses on the urgency of addressing the time delay issue, considering its direct impact on vehicle safety, particularly in high-speed and driverless scenarios. The paper reviews the CAN bus mechanism, analyzes various types of time delays, establishes a model for on-bus message delay under Electromagnetic Interference (EMI) conditions, and conducts simulations. Given the formidable challenge of eliminating time delay entirely, the study emphasizes the need for diverse strategies to meet these rigorous challenges.

**Key Contributions and Findings:**

Importance of Time Delay: The paper underscores the significance of time delay in the context of CAN bus, especially concerning vehicle safety during high-speed and driverless operations.

Analysis of Time Delay Types: Different types of time delays, such as queueing delay and transmission delay, are thoroughly analyzed, providing insights into the mechanisms influencing delay occurrences.

Modeling On-Bus Message Delay: A model for on-bus message delay is established, considering the impact of Electromagnetic Interference (EMI) on delay characteristics.

Simulation and Research: The study includes simulations to further understand and analyze the time delay scenarios, acknowledging the inherent challenges in eliminating delays entirely.

Average Delay Applicability: Emphasizing the practicality of average delay over maximum delay, the research advocates for new scheduling algorithms to reduce delay in CAN bus communication.

**Conclusion:**

This research delves into the complexities of time delay within the Controller Area Network (CAN) and its profound implications for vehicle safety and performance. Analyzing various types of time delays, establishing models for on-bus message delay under challenging environments like EMI, and conducting simulations contribute to a comprehensive understanding of the delay mechanisms. As complete elimination of time delay proves challenging, the study advocates for the development of new scheduling algorithms in CAN bus communication. The practical focus on average delay over maximum delay ensures relevance to real-world scenarios, and the paper calls for extensive future experiments to address the ongoing challenges in mitigating time delay effectively within the CAN bus framework.

**9)Implementation of Data Reduction Technique in**

**Adaptive Fault Diagnosis Algorithm for Controller**

**Area Network**

**Abstract:**

This paper addresses the crucial domain of fault diagnosis in distributed computer networks, with a specific focus on the Controller Area Network (CAN) protocol used in industrial and automotive applications. Unlike some network protocols, CAN lacks redundancy support for its channels or media, necessitating a network-level approach to fault handling. The authors propose and implement the Adaptive Fault Diagnosis algorithm for Controller Area Network (AFDCAN) and introduce a novel Data Reduction (DR) technique into its framework. The results demonstrate a significant reduction of 50% in fault diagnostic data and an average improvement of 31.3% in busload, showcasing the efficacy of the DR technique within AFDCAN.

**Key Contributions and Findings:**

Introduction of AFDCAN: The paper introduces the Adaptive Fault Diagnosis algorithm for Controller Area Network (AFDCAN) as a specialized approach for fault diagnosis in CAN-based industrial and automotive networks.

Data Reduction Technique: A unique Data Reduction (DR) technique is implemented in AFDCAN, resulting in a 50% reduction in fault diagnostic data and a noteworthy 31.3% average improvement in busload.

Comparison of AFDCAN Versions: AFDCAN-II demonstrates superior performance over AFDCAN-I, achieving a 50% compression in the data frame's data field and a 31.3% average reduction in busload, making the CAN bus available for additional application-related messages.

Scalability: AFDCAN-II facilitates the expansion of the system to accommodate more nodes, with up to twenty-two nodes being connectable to the CAN bus, allowing for increased network scalability.

Code Patch Integration: The paper highlights the seamless integration of code patches in AFDCAN-II, expanding the algorithm's functionality without compromising its performance due to the small memory footprint of the added code.

Unique DR Technique: The DR technique implemented in AFDCAN is specially designed for reducing fault diagnosis data, contributing to bandwidth efficiency and making the CAN bus available for a broader range of application-related messages.

**Conclusion:**

This research introduces an enhanced fault diagnosis algorithm, AFDCAN, tailored for Controller Area Network (CAN) environments in industrial and automotive applications. The incorporation of a unique Data Reduction (DR) technique proves instrumental, achieving significant reductions in fault diagnostic data and improving overall busload efficiency. The scalability of AFDCAN-II, coupled with its ability to handle more nodes, positions it as an advanced solution for fault diagnosis in CAN-based distributed systems. The integration of code patches showcases the algorithm's flexibility without compromising performance. The presented DR technique contributes to bandwidth efficiency, making AFDCAN and similar algorithms more advantageous for diverse application-related messages on the CAN bus.

**10) LIN-MM: Multiplexed Message Authentication**

**Code for Local Interconnect Network message**

**authentication in road vehicles**

**Abstract:**

The increasing interconnectivity of vehicles in the automotive market raises cybersecurity concerns, making Electronic Control Units (ECUs) susceptible to cyberattacks. The Local Interconnect Network (LIN) protocol, widely used in automotive communication, lacks robust security mechanisms. This paper introduces LIN Multiplexed MAC (LIN-MM), an innovative approach leveraging signal modulation to integrate Message Authentication Code (MAC) data seamlessly with standard LIN communication. LIN-MM enhances security while ensuring compatibility with existing LIN protocols, contributing to cost-effective and flexible solutions for cybersecurity in vehicles.

**Key Contributions and Findings:**

Automotive Cybersecurity Landscape: The paper emphasizes the vulnerability of Electronic Control Units (ECUs) in vehicles to cyberattacks and the need for enhanced security measures in the face of increasing interconnectedness.

LIN Multiplexed MAC (LIN-MM): LIN-MM introduces a novel approach to augment the security of LIN networks by integrating Message Authentication Code (MAC) data through signal modulation, ensuring compatibility with all versions of the standard LIN protocol.

Back-Compatibility and Flexibility: LIN-MM is designed to be back-compatible with existing LIN devices, allowing it to function seamlessly in hybrid networks that include both LIN and LIN-MM devices. This ensures a flexible and cost-effective solution for upgrading the cybersecurity of the current vehicle fleet.

Cost-Effective Security Upgrade: LIN-MM addresses the challenges posed by evolving security regulations while minimizing associated costs. The solution is presented as an economical and practical alternative for enhancing the security of LIN networks.

Security Analysis: The conducted security analysis reveals a notable improvement, particularly in mitigating the first three types of attacks. However, challenges related to Header collision attacks are acknowledged, prompting ongoing work on an enhanced version, referred to as (Type-B), aimed at addressing this specific vulnerability.

**Conclusion:**

LIN-MM emerges as a forward-looking solution to fortify the security of LIN networks in vehicles, offering an innovative approach to seamlessly integrate Message Authentication Code (MAC) data through signal modulation. By maintaining compatibility with existing LIN protocols, LIN-MM presents a cost-effective and flexible cybersecurity upgrade for the current vehicle fleet. While demonstrating improvements in security against various attack types, the paper acknowledges ongoing efforts to enhance LIN-MM's architecture, specifically targeting Header collision attacks. LIN-MM stands as a promising advancement in the pursuit of robust cybersecurity for interconnected vehicles, aligning with evolving security regulations and requirements.

**11)Probabilistic Delay Model of Dynamic Message Frame**

**in FlexRay Protocol**

**Abstract:**

With the increasing complexity of safety and multimedia functions in automobiles, in-vehicle networks play a crucial role. Despite FlexRay emerging as the standard, the challenge of message delay analysis persists. This paper introduces a probabilistic delay model for message transmission in the FlexRay dynamic segment, specifically addressing variable-length messages sharing the same Frame Identifier (ID). The proposed model provides insights into frame delay probability, empty minislot distribution, and transmission probabilities for different frame lengths, offering valuable metrics for FlexRay network design.

**Key Contributions and Findings:**

Importance of In-Vehicle Networks: As automotive functions become more intricate, in-vehicle networks, particularly FlexRay, are integral. The paper underscores the significance of addressing the message delay analysis challenge in FlexRay networks.

Probabilistic Delay Model: The paper presents a novel probabilistic delay model for the FlexRay dynamic segment, accounting for variable-length messages with shared Frame IDs. This model serves as a valuable tool during the design phase of FlexRay networks.

Performance Metrics: Frame delay probability and empty minislot distribution are introduced as performance metrics derived from the probabilistic delay model. These metrics aid system designers in assessing the performance and efficiency of a FlexRay network.

Comparison with Previous Models: A comparative analysis is conducted between the proposed variable frame length model and a previous fixed frame length model. The results reveal that the fixed frame length model yields more pessimistic outcomes.

Transmission Probabilities: Utilizing the empty minislot probability, the paper explores transmission probabilities for frames of different lengths. This analysis assists FlexRay system designers in determining suitable parameters for optimal network performance.

Simulation Experiments: The proposed models are validated through simulation experiments, demonstrating their effectiveness in providing realistic predictions for message transmission in various system designs.

Future Research: The paper suggests future research avenues, including exploring new performance metrics for FlexRay using the introduced probabilistic delay model.

**Conclusion:**

This paper introduces a significant advancement in FlexRay protocol by proposing a probabilistic delay model tailored for the dynamic segment. The model considers variable-length messages sharing the same Frame ID, providing valuable insights into frame delay probability, empty minislot distribution, and transmission probabilities for different frame lengths. Comparative analysis reveals the superiority of the proposed model over a fixed frame length model, emphasizing its practicality for FlexRay system designers. Simulation experiments validate the models, and future research directions are outlined to further enhance performance metrics for FlexRay networks. The probabilistic approach presented in this paper contributes to the optimization of in-vehicle networks, aligning with the evolving landscape of automotive technologies.

**12) TCE-IDS: Time Interval Conditional Entropy-**

**Based Intrusion Detection System for**

**Automotive Controller Area Networks**

**Abstract:**

The proliferation of intelligent connected vehicles, driven by 5G technology, has expanded the functional interfaces, amplifying the susceptibility of automotive Controller Area Networks (CAN) to cyberthreats. Recognizing the direct impact of CAN network attacks on traffic safety, this study addresses the need for robust intrusion detection systems. While existing technologies struggle against sophisticated attacks, we introduce a novel Time Interval Conditional Entropy-based Intrusion Detection System (TCE-IDS) specifically tailored for automotive CAN networks. TCE-IDS exhibits resilience against interference, demonstrating efficacy in detecting a diverse range of attacks. Through experiments on our CAN-BUS network platform, we evaluate and validate TCE-IDS, highlighting its superior detection accuracy and deployment ease compared to existing intrusion detection methods.

**Key Contributions and Findings:**

Evolution of Intelligent Connected Vehicles: As intelligent and connected vehicles become integral to daily life, the vulnerability of these vehicles to network attacks rises. The study emphasizes the deployment of Intrusion Detection Systems (IDS) in automotive in-vehicle networks as a critical countermeasure.

Challenges in IDS Deployment: Considerations for IDS deployment include stability, reliability, real-time detection efficiency, and low power consumption. TCE-IDS addresses these factors while maintaining flexibility and cost-effectiveness.

TCE-IDS Architecture: TCE-IDS employs a Time Interval Conditional Entropy-based approach, demonstrating flexibility, low cost, resistance to interference, and adaptability to various attack scenarios. The system reduces data transformation complexity and places minimal demands on computational resources.

Experimental Validation: Extensive experiments conducted on a real CAN network platform validate TCE-IDS's effectiveness. Results indicate rapid response, high accuracy, low resource requirements, and ease of deployment, positioning it as a viable solution for automotive network security.

Versatility Against Attacks: TCE-IDS proves its capability to detect various forms of attacks, showcasing its adaptability to the evolving landscape of cyber threats targeting intelligent connected vehicles.

Future Deployment Considerations: The study outlines plans for future deployment and verification of TCE-IDS in existing vehicle networks and intelligent networked vehicles, emphasizing its practicality and utility.

**Conclusion:**

TCE-IDS emerges as a promising solution for fortifying automotive Controller Area Networks against cyberthreats. Its Time Interval Conditional Entropy-based approach, combined with flexibility, low cost, and resistance to interference, positions it as an effective and deployable intrusion detection system. Through rigorous experimental validation, TCE-IDS demonstrates superior detection accuracy and ease of integration, laying the groundwork for enhanced security in intelligent connected vehicles. Future deployment considerations highlight the potential of TCE-IDS to contribute to the evolving landscape of vehicle network cybersecurity.

**13 Rapid, Multi-vehicle and Feed-forward Neural**

**Network based Intrusion Detection System for**

**Controller Area Network Bus**

**Abstract:**

This paper introduces NESLIDS, a Neural Network-based Intrusion Detection System designed for the Controller Area Network (CAN) bus within modern vehicles. NESLIDS employs a supervised Deep Neural Network (DNN) architecture to effectively counteract three critical attack categories: Denial-of-Service (DoS), fuzzy, and impersonation attacks. Through an iterative process, DNN parameters such as hidden layer neurons, batch size, and activation functions are optimized to maximize detection accuracy and minimize false positive rates (FPR). Extensive experimentation, utilizing both online and real-time CAN Bus data, demonstrates NESLIDS's superiority in terms of accuracy, scalability, and low false alarm rates compared to existing approaches.

**Key Contributions and Findings:**

NESLIDS Architecture: NESLIDS is presented as a rapid, multi-vehicle, and feed-forward neural network-based Intrusion Detection System for CAN Bus communication. The system efficiently detects malicious behavior without the need for repeated re-training.

Research Methodology: The research involves collecting CAN Bus data both online and through a data logger, followed by the injection of attack data, preprocessing in Python, training the DNN, and comprehensive testing using diverse datasets.

Attack Categories Addressed: NESLIDS is specifically designed to counter three critical attack categories: Denial-of-Service (DoS), fuzzy, and impersonation attacks, providing a comprehensive defense mechanism against varied intrusion attempts.

Optimization of DNN Parameters: The paper highlights the iterative optimization of DNN parameters, including hidden layer neurons, batch size, and activation functions, to achieve maximum detection accuracy and minimize false positive rates across different attack types.

Dataset Testing and Superior Performance: NESLIDS is tested on two datasets, HCRL and ML350, showcasing its ability to successfully detect DoS, fuzzy, and impersonation attacks with high accuracy and minimal false positives, surpassing existing DNN-based techniques.

Scalability and Real-time Implementation: NESLIDS demonstrates scalability and practicality by being trained on a given dataset and fine-tuned, eliminating the need for repeated training. Future work is proposed for real-time implementation in automotive intrusions.

**Conclusion:**

NESLIDS emerges as a robust and efficient solution for securing Controller Area Network Bus communication in modern vehicles. Leveraging a DNN-based FFNN structure, NESLIDS excels in detecting diverse attack categories, exhibiting high accuracy and minimal false positives. The iterative optimization of DNN parameters enhances its performance, making it superior to existing techniques. The scalability and adaptability of NESLIDS position it as a viable choice for real-time automotive intrusion detection. Future endeavors will focus on the practical implementation of NESLIDS in real-time automotive security scenarios.

**14)A New Delay-Compensation Scheme for**

**Networked Control Systems in Controller**

**Area Networks**

**Abstract:**

This paper introduces a new delay-compensation algorithm tailored for Networked Control Systems (NCSs) connected through Controller Area Networks (CAN). By analyzing CAN bus properties and identifying sources of delays induced by the network, we formulate the controlled system within the framework of NCSs. Departing from conventional state or output feedback control schemes, our approach incorporates a time-domain Smith predictor in the feedback control law. Leveraging augmentation techniques, we derive a closed-loop system with delayed states, establishing the asymptotical stability through a bilinear matrix inequality (BMI). The BMI is further converted into a linear matrix inequality (LMI), and the feedback gain in the proposed control law is computed by solving the LMI condition. Two application examples showcase the effectiveness and advantages of the proposed controller design method.

**Key Contributions and Findings:**

Background and Problem Definition: The study addresses the challenges of delay compensation in NCSs operating over CAN networks, identifying key sources of delays induced by the CAN bus.

Proposed Delay-Compensation Algorithm: The paper introduces a novel delay-compensation algorithm employing a time-domain Smith predictor for forecasting future states, providing a robust feedback control law.

Closed-Loop System Formulation: Utilizing augmentation techniques, the closed-loop system is derived, encompassing both delayed and nondelayed states, showcasing the uniqueness of the proposed approach.

Stability Analysis: Asymptotical stability of the closed-loop system is rigorously analyzed. A sufficient stability condition, expressed as a bilinear matrix inequality (BMI), is derived.

Conversion to LMI and Feedback Gain Calculation: The obtained BMI is efficiently converted into a linear matrix inequality (LMI), facilitating a streamlined calculation of the feedback gain in the proposed control law.

Simulation Examples: Two simulation examples are presented, demonstrating the advantages of the proposed delay-compensation algorithm over existing state-feedback control methods, with specific applications in electronic throttle control over a CAN bus.

Future Research Directions: The paper outlines future research directions, including the exploration of alternative control methods such as sliding mode control and T–S fuzzy control.

**Conclusion:**

This work introduces a novel delay-compensation scheme for NCSs in CAN environments, demonstrating advantages over traditional control schemes. The proposed algorithm, leveraging a time-domain Smith predictor, proves effective in mitigating delays and ensuring stability. Simulation examples validate the superiority of the approach, particularly in electronic throttle control applications. Future research will explore additional control methods to further enhance the robustness of delay compensation in NCSs.

**15)FlexRay Network Parameter Optimization Method**

**for Automotive Applications**

**Abstract:**

This paper presents a novel FlexRay Network Parameter Optimization (NPO) method designed to streamline the configuration process for FlexRay networks in automotive applications. The NPO method involves two essential steps: optimizing the static (ST) slot length and determining the communication cycle length. The first step formulates an optimal problem, considering bandwidth limitations as a criterion for efficient network usage. The optimal ST slot length is derived by exploring the design space within FlexRay specifications. Subsequently, an algorithm is proposed for analyzing worst-case response times (WCRTs) for both ST and dynamic frames in the second step, leading to the determination of the optimal communication-cycle length. The NPO method simplifies the FlexRay network configuration process, ensuring efficient utilization with minimal WCRT. The paper concludes with the application of the proposed method to a vehicle chassis control system, verifying its effectiveness.

**Key Contributions and Findings:**

Optimization Objective: The paper introduces an optimization objective for the FlexRay network, focusing on bandwidth utilization and minimizing worst-case response times (WCRT) for frames.

Two-Step NPO Method: The proposed NPO method comprises two straightforward steps: determining the optimal ST slot length and subsequently deriving the optimal communication-cycle length based on WCRT analysis.

ST Slot Length Optimization: An optimal problem is formulated for designing the ST slot length, considering protocol overhead and unused network resources. The method efficiently explores the design space within FlexRay specifications to determine the optimal ST slot length.

Communication-Cycle Length Determination: The paper proposes an algorithm for analyzing WCRTs for both ST and dynamic frames, leading to the derivation of the optimal communication-cycle length with minimal network delays.

Method Application: The NPO method is applied to a vehicle chassis control system as a practical example, verifying the effectiveness of the parameter-optimization algorithm.

Straightforward Process: The NPO method is defined in a straightforward manner, facilitating its application to various network design applications in the automotive, avionic, and industrial fieldbus systems.

Emerging Field and Future Work: Designing FlexRay configurations is identified as an emerging field, suggesting possibilities for future work such as supporting signal-based frame construction and addressing multirate communication with cycle-filtering and in-cycle repetition functionalities.

**Conclusion:**

The paper introduces a comprehensive FlexRay Network Parameter Optimization (NPO) method, emphasizing bandwidth utilization and minimizing worst-case response times. The two-step process simplifies the design of FlexRay configurations, showcasing applications in automotive, avionic, and industrial fieldbus systems. The NPO method is deemed effective, with potential avenues for future work identified in the emerging field of FlexRay configuration design.