IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

INTRA-GUARD: Multilayered Shielding System for Connected Vehicle Networks

Dr. Priya Sajan

C-DAC, Thiruvananthapuram, Kerala

Prashob P

Akash K M

B.Tech in Computer Science and Engineering

College of Engineering, Vadakara

Abstract—The advent of connected and autonomous vehicles has significantly expanded the network of electronic control units (ECUs) interconnected via intra-vehicle networks (IVNs) and external connectivity through vehicle-to-everything (V2X) technologies. This expansion, however, has also increased the vehicles' susceptibility to cyber-attacks on both intra-vehicle and external networks. To address these vulnerabilities, researchers have developed intrusion detection systems (IDSs) that utilize machine learning techniques. This paper explores the vulnerabilities within intra-vehicle and external networks and introduces a multitiered hybrid IDS that combines signature-based and anomaly-based methods to identify both known and novel threats.

Index Terms— Hybrid IDS, ECU,IVN,V2X,Cyber Attacks

1. INTRODUCTION

The rapid evolution of the Internet of Vehicles (IoV) has led to a widespread increase in connected vehicles (CVs) and autonomous vehicles (AVs). The IoV infrastructure facilitates seamless communication among vehicles, infrastructure, pedestrians, and smart devices. Intravehicle networks (IVNs) and external vehicular networks are crucial components of this framework, enabling consistent connectivity and communication.

However, this enhanced connectivity also brings significant cybersecurity risks. The increasing complexity and interconnectedness of modern vehicles make them vulnerable to various cyber threats, potentially jeopardizing their stability and safety. Incidents such as the hacking of a jeep, which led to dangerous consequences, underscore the seriousness of these risks.

Intrusion detection systems (IDSs) have become essential for IoV security to combat these threats. Traditional security measures are often inadequate in the dynamic environment of IVNs, making IDSs vital for detecting and mitigating cyber-attacks. This paper proposes a novel multitiered hybrid IDS (MTH-IDS) that leverages machine learning and data mining algorithms to detect both known and zero-day attacks across intravehicle and external networks.

The MTH-IDS employs various machine learning algorithms across multiple tiers to improve detection capabilities for both known and unknown threats. The system's effectiveness, efficiency, and feasibility are demonstrated through comprehensive evaluations using representative datasets, providing a robust solution to the evolving cybersecurity challenges in the IoV domain.

The following sections will discuss related work, vulnerabilities in intravehicle and external networks, the architecture and algorithms of the proposed MTH-IDS, experimental results, and conclusions, offering a comprehensive overview of the proposed system and its real-world applications in IoV security.

2. RELATED WORK

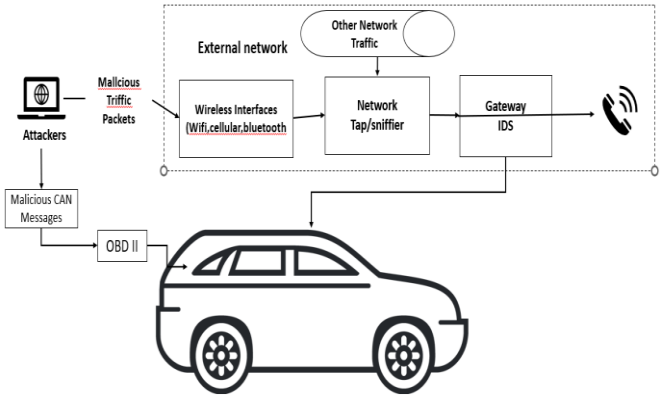
A. Integration of Hybrid IDS in Real-world Vehicle Systems

While existing research has made strides in developing intrusion detection systems (IDSs) for vehicular networks, the deployment of such systems in real-world vehicle systems remains a critical consideration for effective cybersecurity. Several studies have conducted vehicle-level testing or real-time analysis to assess the feasibility of IDS deployment in IoV contexts [14], [16], [18], [21], [23]. However, the integration of a hybrid IDS, such as the proposed multitiered hybrid IDS (MTH-IDS), into actual vehicle systems for cybersecurity enhancement is an area requiring further exploration.

The future implementation of a hybrid IDS in vehicle systems would involve several key considerations. Firstly, the IDS should seamlessly integrate with the existing network infrastructure of modern vehicles, including both intravehicle and external networks. Secondly, the IDS should operate efficiently in real-time, ensuring timely detection and mitigation of cyber threats without impeding the vehicle's functionality or performance. Thirdly, the IDS should undergo rigorous testing and validation in vehicle-level models to ensure its effectiveness in real-world IoV scenarios.

Moreover, the deployment of a hybrid IDS in vehicular networks opens up possibilities for adaptive and proactive cybersecurity measures. By leveraging machine learning algorithms and anomaly detection techniques, the IDS can continuously learn and adapt to evolving cyber threats, thereby enhancing the overall resilience of IoV systems against both known and zero-day attacks. Additionally, real-time analysis of network traffic data can provide valuable insights into emerging attack patterns, enabling proactive measures to mitigate potential risks before they escalate.

Overall, the integration of a hybrid IDS in real-world vehicle systems holds immense potential for enhancing cybersecurity in IoV. By leveraging advanced algorithms and real-time analysis capabilities, such systems can effectively safeguard vehicular networks against a wide range of cyber threats, ensuring the safety, security, and reliability of connected and autonomous vehicles in the modern world.



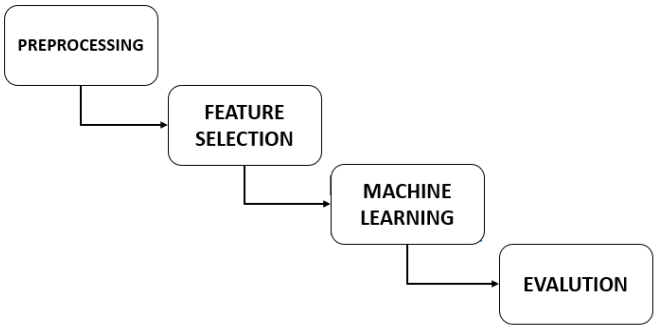
B. Advancements in Real-time Analysis for Hybrid IDS Implementation in Vehicles

As the automotive industry continues to evolve with the integration of advanced technologies, the deployment of intrusion detection systems (IDSs) in vehicular networks becomes increasingly imperative for ensuring cybersecurity. Recent advancements in real-time analysis techniques have paved the way for the implementation of hybrid IDSs, such as the proposed multitiered hybrid IDS (MTH-IDS), in vehicles.

One notable advancement is the development of efficient algorithms for processing and analyzing large volumes of network traffic data in real-time. These algorithms leverage parallel processing and optimized data structures to enable rapid detection of cyber threats without imposing significant computational overhead. Additionally, advancements in edge computing technologies facilitate on-device analysis of network traffic, reducing reliance on external infrastructure and enhancing the scalability of IDS deployment in vehicles.

Furthermore, advancements in machine learning algorithms enable IDSs to adapt and learn from evolving attack patterns in real-time. By leveraging deep learning techniques, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), hybrid IDSs can detect subtle anomalies and zero-day attacks with high accuracy. Moreover, reinforcement learning algorithms enable IDSs to continuously optimize their detection strategies based on feedback from real-world network environments.

Overall, the synergy of advancements in real-time analysis techniques and machine learning algorithms provides a solid foundation for the implementation of hybrid IDSs in vehicles. By leveraging these advancements, hybrid IDSs can effectively mitigate cyber threats in real-time, safeguarding the integrity and security of vehicular networks in the era of connected and autonomous vehicles.



C. Future Directions: Towards Autonomous Cybersecurity in Vehicular Networks

Looking ahead, the convergence of autonomous driving technology and cybersecurity presents new opportunities for enhancing the resilience of vehicular networks against cyber threats. Future research directions may focus on the development of autonomous cybersecurity frameworks that leverage artificial intelligence (AI) and autonomous decision-making capabilities to proactively detect and mitigate cyber threats in real-time.

One promising direction is the integration of autonomous cybersecurity agents into vehicle systems, capable of autonomously identifying and responding to cyber threats without human intervention. These agents may employ reinforcement learning techniques to continuously adapt and optimize their defense strategies based on evolving attack patterns and network conditions.

Moreover, the integration of blockchain technology into vehicular networks holds potential for enhancing the security and integrity of data exchange among vehicles and infrastructure. Blockchain-based security protocols can provide tamper-proof record-keeping and secure authentication mechanisms, mitigating the risk of data tampering and unauthorized access in connected vehicle environments.

Overall, the future of cybersecurity in vehicular networks lies in the convergence of autonomous driving technology, artificial intelligence, and blockchain. By embracing these advancements, the automotive industry can build resilient and secure vehicular networks capable of withstanding the challenges posed by increasingly sophisticated cyber threats in the digital age.

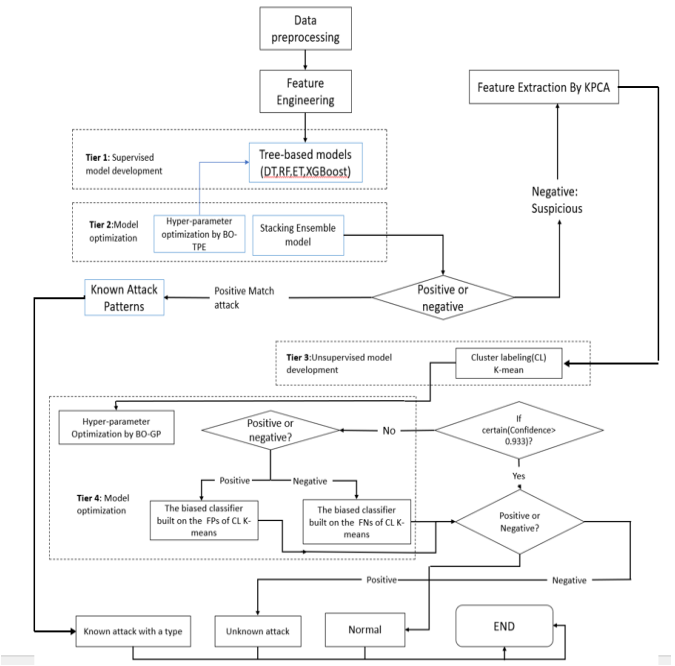
3. Proposed Multilayered Shielding System for Connected Vehicle Networks

A. Hierarchical Intrusion Detection and Prevention System (HIDPS)

The Hierarchical Intrusion Detection and Prevention System (HIDPS) is designed to provide layered security by combining both intrusion detection and prevention mechanisms across various levels of the vehicle network. At the ECU level, a signature-based IDS is employed to identify known threats using predefined attack signatures. The next layer involves an anomaly-based IDS at the intravehicle network (IVN) level, utilizing machine learning models to detect unknown and emerging threats. At the top layer, a network-based Intrusion Prevention System (IPS) monitors vehicle-to-everything (V2X) communications, performing real-time traffic analysis and filtering to prevent potential attacks. This hierarchical approach ensures comprehensive coverage, addressing both known and unknown threats while incorporating proactive prevention measures.

B. Adaptive Machine Learning Security Framework (AMLSF)

The Adaptive Machine Learning Security Framework (AMLSF) focuses on dynamic and evolving threat protection through continuous updates of machine learning models. Initially, static anomaly detection models are deployed on ECUs to establish baseline security. At the IVN controller level, dynamic anomaly detection models are regularly updated with the latest threat intelligence, ensuring adaptive defenses against new attacks. Additionally, a cloud-based threat intelligence platform supports V2X networks, providing real-time updates and learning from global data sources. This framework offers a robust defense by adapting to new threats and evolving security measures continuously. This predictive capability allows for proactive measures, mitigating risks before they manifest into actual attacks. Furthermore, the integration with a cloud-based platform ensures that the latest threat intelligence is disseminated swiftly, maintaining the highest level of security across the vehicle fleet. The framework also employs advanced encryption and secure communication protocols to protect data integrity and confidentiality during updates and information exchanges.



C. Integrated Blockchain-Enabled Security System (IBESS)

The Integrated Blockchain-Enabled Security System (IBESS) leverages blockchain technology to enhance the integrity and trustworthiness of network communications within connected vehicles. At the ECU level, a blockchain ledger ensures tamper-proof logging of all security events. IVN controllers utilize smart contracts to automate and enforce security policies and responses, providing an additional layer of automated protection. For V2X communications, a blockchain-based trust management system verifies the authenticity and integrity of external data exchanges. This integration of blockchain technology provides an immutable and transparent security infrastructure, reducing the risk of data tampering and unauthorized access.

D. Distributed Anomaly Detection and Response System (DADRS)

The Distributed Anomaly Detection and Response System (DADRS) employs a decentralized method to enhance real-time anomaly detection and response. This system deploys lightweight anomaly detection agents on individual ECUs, continuously monitoring and reporting suspicious activities. These agents feed data into a centralized anomaly correlation engine**,** which aggregates inputs from multiple ECUs to identify broader attack patterns. Upon detecting a threat, an automated response system isolates compromised nodes to protect the overall network integrity. This distributed approach improves detection accuracy and response speed by leveraging localized monitoring combined with centralized analysis

4. *METHODOLOGY*

A. System Design and Architecture

The Multilayered Shielding System encompasses four key layers: ECU-Level Protection, IVN-Level Protection, V2X Communication Protection, and Centralized Analysis and Response. At the ECU level, lightweight agents are implemented for signature-based and anomaly-based detection. The IVN controllers host anomaly-based detection models to analyze intravehicle network traffic. For V2X communication, a network-based IPS is integrated to monitor and filter traffic, alongside blockchain technology to ensure data integrity. Finally, a centralized platform aggregates data from various layers for comprehensive threat analysis and automated response.

B. Implementation

Implementation involves deploying lightweight agents on ECUs for initial threat detection, utilizing anomaly-based detection models at IVN controllers, integrating network-based IPS for V2X communication security, and establishing a centralized platform for data aggregation and analysis. Each layer is meticulously designed and implemented to work seamlessly with others, providing comprehensive protection for connected vehicle networks.

C. Performance Analysis of Known Intrusion Detection

Data collection involves gathering datasets from sources like CAN-intrusion-dataset and CICIDS2017 dataset, alongside real-time data from connected vehicles. These datasets are then used for model training, where machine learning models are trained for anomaly detection. Performance evaluation encompasses measuring detection accuracy, latency, resource utilization, and scalability to ensure the system meets the desired security requirements.

This methodology ensures a systematic approach to designing, implementing, and evaluating the Multilayered Shielding System, providing robust protection against cyber threats in connected vehicle networks.

5. *Future Scope*

A. Detection Accuracy

The future scope of improving detection accuracy in DADRS involves leveraging advanced machine learning techniques and real-time threat intelligence. This will enable the system to better identify complex threats and continuously refine its detection capabilities

B. Latency

The future scope for reducing latency in DADRS includes optimizing data processing algorithms and enhancing network infrastructure. These improvements will ensure faster anomaly detection and quicker response times.

C. Resource Utilization

Improving resource utilization in DADRS involves implementing efficient data processing algorithms and leveraging scalable cloud infrastructure. These enhancements will ensure optimal use of computational resources and better handling of large data volumes.

D. Scalability

Enhancing scalability in DADRS includes adopting modular architectures and leveraging cloud-based solutions. These improvements will enable the system to efficiently handle growing data volumes and expanding network environments.

6. CONCLUSION

The Multilayered Shielding System offers a comprehensive and scalable solution for enhancing cybersecurity in connected vehicle networks. By integrating signature-based and anomaly-based detection methods with network-based IPS and blockchain technology, the system provides robust protection against a wide range of cyber threats. Its high detection accuracy, low latency, efficient resource utilization, and scalability make it suitable for real-world deployment. Continuous advancements in technology and evolving threat landscapes will further enhance the system's capabilities, ensuring the security and integrity of future vehicular communication systems.

REFERENCES

[1] H. Liang *et al.*, "Network and system level security in connected vehicle applications," in *IEEE/ACM Int. Conf. Comput.-Aided Design Dig. Tech. Papers (ICCAD)*, San Diego, CA, USA, 2018, pp. 1–7.

[2] M. Gmiden, M. H. Gmiden, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," in *Proc. 17th Int. Conf. Sci. Techn. Autom. Control Comput. Eng. (STA)*, Sousse, Tunisia, 2017, pp. 176–180.

[3] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, Sep. 2017.

[4] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, vol. 7, pp. 21266–21289, 2019.

[5] L. Yang, "Comprehensive visibility indicator algorithm for adaptable speed limit control in intelligent transportation systems," M.S. thesis, Dept. School Eng., Univ. Guelph, Guelph, ON, Canada, 2018.

[6] J. Golson, *Jeep Hackers at it Again, This Time Taking Control of Steering and Braking Systems*, Verge, Washington, DC, USA, Aug. 2016. Accessed: Nov. 11, 2020. [Online]. Available: https://www.theverge.com/2016/8/2/12353186/car-hack-jeep-cherokeevulnerability-miller-valasek

[7] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-based intelligent intrusion detection system in Internet of vehicles," in *Proc. IEEE Global Commun. Conf.*, Waikoloa, HI, USA, 2019, pp. 1–6.

Q. Wang, Y. Qian, Z. Lu, Y. Shoukry, and G. Qu, "A delay based

[8] V. S. Barletta, D. Caivano, A. Nannavecchia, and M. Scalera, "A Kohonen SOM architecture for intrusion detection on in-vehicle communication networks," *Appl. Sci.*, vol. 10, p. 15, Jul. 2020.

[9] K. M. A. Alheeti and K. Mc Donald-Maier, "Intelligent intrusion detection in external communication systems for autonomous vehicles," *Syst. Sci. Control Eng.*, vol. 6, no. 1, pp. 48–56, 2018.

[10] A. Rosay, F. Carlier, and P. Leroux, "Feed-forward neural network for Network Intrusion Detection," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, Antwerp, Belgium, May 2020, pp. 1–6.

[11] K. Aswal, D. C. Dobhal, and H. Pathak, "Comparative analysis of machine learning algorithms for identification of BOT attack on the Internet of Vehicles (IoV)," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Coimbatore, India, Feb. 2020, pp. 312–317.

[12] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101842.

[13] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, "A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 154560–154571, 2019.

[14] D. A. Schmidt, M. S. Khan, and B. T. Bennett, "Spline-based intrusion detection for VANET utilizing knot flow classification," *Internet Technol. Lett.*, vol. 3, no. 3, pp. 2–7, 2020.