Enhancing Communication Security an In-Vehicle Wireless Sensor Network

Subjects: Computer Science, Information Systems

Contributor: Algimantas Venčkauskas, Marius Taparauskas, Šarūnas Grigaliūnas, Rasa Brūzgienė

The adoption of wireless sensor networks (WSNs) in vehicle systems represents a transformative development in the automotive sector, broadening the scope of functionalities from simple monitoring and control to facilitating sophisticated driver assistance and self-driving features. Secure in-vehicle communication systems are integral to the realization of fully connected and automated urban environments, where vehicles and city systems operate in harmony to optimize city life.

Keywords: in-vehicle WSN ; communication security ; wireless sensor networks

1. Introduction

Today's emphasis on cybersecurity in the realm of vehicles cannot be overstated. As we witness the rapid evolution and integration of computer technologies into vehicles, we are also seeing the creation of complex networks that manage crucial systems. These systems, which include aspects like braking [1], lighting [2], and engine control [3], rely heavily on data from various sensors. The threat of compromising these in-vehicle technologies is not just a theoretical risk; it has real-world implications for the safety of both those inside the vehicle and pedestrians alike. Moreover, the advent of wireless sensors [4] has opened new doors for hackers, making our vehicles more vulnerable to cyber-attacks. Adding to this complexity is the ability of smart devices to connect to a vehicle's network, which introduces yet another risk for potential breaches, endangering the privacy of users.

The adoption of wireless sensor networks (WSNs) in vehicle systems represents a transformative development in the automotive sector, broadening the scope of functionalities from simple monitoring and control to facilitating sophisticated driver assistance and self-driving features. Yet, this fusion of technology introduces significant security concerns that demand thorough attention to safeguard the systems' safety, privacy, and dependability. The critical role of encryption in automotive WSNs is highlighted by the imperative to guard sensitive data, uphold the integrity of the data being exchanged, and secure communication across networked devices [5][6].

In the context of smart cities, such vehicles play a pivotal role in enhancing urban mobility, reducing traffic congestion, and improving environmental sustainability [7]. Secure communication within these vehicle systems and their interaction with the urban infrastructure is paramount, as it not only ensures the efficient operation of transportation networks but also underpins the safety and privacy of the city's inhabitants. Secure in-vehicle communication systems are integral to the realization of fully connected and automated urban environments, where vehicles and city systems operate in harmony to optimize city life [8].

Securing data through encryption is essential. As vehicles constantly collect and share sensitive information, including their location [9], speed, and the driver's habits, it is imperative to implement strict protocols to protect these data from falling into the wrong hands. Moreover, keeping the data intact as they are transmitted is critical for the smooth operation of vehicle systems. Employing encryption and digital signatures plays a key role in ensuring the data are not altered during their journey, protecting against attacks aimed at tampering with the data, which could put vehicle safety at risk. The complexity and scalability of networks, particularly with the emergence of Vehicle-to-Everything (V2X) systems, compound the difficulty of managing encryption keys and protocols [10]. Additionally, the real-time data transmission required by many automotive applications necessitates efficient encryption processes that do not introduce undue latency.

Nevertheless, integrating encryption within automotive wireless sensor networks presents significant challenges. The computational capabilities and resources of sensor nodes in these networks are often limited, making it difficult to implement strong encryption techniques without negatively impacting system performance. The sensor nodes must endure harsher conditions than typical stationary or portable computers, including higher temperatures and vibrations, with the added constraint of vehicles having relatively modest computing systems and power supplies. These compact

and power-limited components constrain processing capabilities, increasing the vulnerability of vehicle security systems. In environments where resources are scarce, employing long cryptographic keys or sophisticated algorithms can significantly slow down system operations, potentially to a detrimental extent. Moreover, vehicle networks can be compromised through various means, such as wireless communications or internal vehicle hardware, posing a risk to user safety. The manipulation of data or signals by compromised sensors can interfere with vehicle functionality, endangering both passengers and pedestrians [11].

Moreover, it is important to note that the network within a vehicle does not undergo regular updates like standard computer systems do. Consequently, if new threats emerge or existing vulnerabilities are discovered, addressing these issues through software updates may not be feasible. Additionally, the in-vehicle network's complexity, composed of numerous subsystems each with their own security flaws, further complicates the situation. With the increasing prevalence of consumers' smart devices, there is a potential for these gadgets to connect to the vehicle's internal network, thus introducing new security challenges [12]. Inadequate security measures for communications between user devices and the vehicle's network can lead to breaches, either externally or through the user's own device. Such access does not limit itself to specific functionalities but might extend over the entire in-vehicle network. This poses a risk not only to the user's private information but also to their physical well-being, should control over the vehicle's sensor-controlled systems be compromised.

The use of wireless sensor networks for in-vehicle communication introduces various security issues. The data from sensors are transmitted omnidirectionally, meaning that with the right equipment and proximity, an unauthorized individual could intercept this information. This risk escalates if the sensor data are unencrypted, as reverse engineering could then be employed to disrupt the system's operations by injecting false data masquerading as legitimate sensor input. Furthermore, if the network's subsystems are interconnected without adequate segregation, compromising one part could lead to a breach of the entire system. Additionally, a system that connects to any device without verifying its authenticity is vulnerable to intrusion by external devices, posing a significant threat to the network's integrity.

Confronting these challenges demands innovative solutions. With vehicles increasingly becoming interconnected, ensuring the security of WSN communications through effective encryption is not merely a technical requirement but a scientific problem in ensuring automotive safety and reliability.

2. Enhancing Communication Security an In-Vehicle Wireless Sensor Network

Given the importance of wireless sensor networks in the automotive industry, particularly in facilitating communication between a number of sensors and control units within a vehicle, safety issues are paramount.

Researchers have explored numerous innovative approaches to address the intricate challenges of achieving robust, efficient, and flexible security in wireless sensor networks. One significant advancement is the integration of blockchain technology into WSNs, as detailed in [13]. This method leverages blockchain's decentralized nature and resistance to tampering to enhance data security and integrity within WSNs. The research combines blockchain technology with data transmission to create a very secure network architecture for small-scale wireless sensor networks. Each network has a central node for gathering data, known as a "mobile database", which relies on embedded microcontrollers for data handling. By incorporating the decentralized and secure features of blockchain, the study aims to enhance the protection of communications within these networks. Nevertheless, this approach faces challenges related to high computational and energy demands, especially in settings with limited resources, potentially affecting the system's practical efficiency and scalability.

A research article featured in [14] delves into improving how smart solar power systems are managed and connected by applying physical layer security within WSNs. The study highlights the crucial role of protecting the physical layer from unauthorized access and eavesdropping, suggesting that robust security can be achieved through the use of specialized equipment and methods. However, the complexity and the need for particular hardware present significant challenges to the widespread adoption of these systems.

The study referenced as [15] introduces a self-adjusting approach for optimizing the coverage of wireless sensor networks. This technique dynamically adapts to enhance intrusion tolerance by factoring in trust metrics. Its natural capacity to adjust to varying circumstances helps maintain its integrity, guaranteeing secure and reliable network coverage even under malicious attacks. Nonetheless, its reliance on trust metrics introduces a vulnerability to attacks aimed at manipulating these values, indicating areas that require further refinement.

The research documented in [16] introduces a specialized technique in symmetric cryptography aimed at bolstering security within wireless sensor networks. This form of cryptography is noted for its high efficiency and simplicity, making it particularly well-suited for use in WSN nodes that operate with limited resources. Despite its advantages, the technique faces challenges related to the complexity of key management and distribution, especially when deployed on a large scale.

Additionally, another study in [17] discusses a secure and energy-efficient authentication strategy for WSNs, grounded in symmetric cryptography. This strategy skillfully balances the demands of security and energy conservation. It underscores the inherent challenges in securing WSNs, such as their susceptibility to physical attacks and the complexities of wireless communication. The study proposes a lightweight authentication protocol that efficiently conserves energy while ensuring secure communication between nodes.

Another noteworthy contribution comes from research published in [18], which delves into the characteristics and detection methods of Distributed Denial of Service (DDoS) attacks on WSNs, with a focus on vehicular networks. This study sheds light on the evolving nature of cyber threats and underscores the necessity for flexible and strong security measures to protect against these risks.

Lastly, the research in [19] investigates the practical challenges and solutions in deploying monitoring systems based on WSNs. It offers insight into the limitations and hurdles faced by WSNs, such as limited resources and susceptibility to external factors, providing valuable perspectives on the practical considerations for implementing secure sensor networks. The authors of the study in [20] conducted a statistical analysis on the network security issues faced by IT organisations, providing concrete evidence of the broader impact that security challenges in wireless sensor networks have on the business world.

In another piece of research [21] the optimization of access strategies for security in C-V2X (Cellular Vehicle-to-Everything) compute offloading networks was explored. This study highlights the difficulties arising from incomplete channel state information (CSI), which plays a crucial role in understanding how to ensure secure and efficient offloading in vehicular networks. Such advancements are critical for supporting the real-time data exchange and processing demands of modern vehicular systems.

Furthermore, the application of Artificial Intelligence (AI) in enhancing security is examined in the study [22], where the use of deep Q-learning to bolster the security of cellular V2X communications is investigated. This research marks a significant step forward in employing AI to bolster defence mechanisms against sophisticated cyber threats, thereby ensuring the integrity and reliability of vehicular communication systems.

Enhancing communication security in in-vehicle WSNs calls for interdisciplinary research efforts that span automotive engineering, cybersecurity, and information technology. A comprehensive approach that considers the technical, functional, safety, and privacy aspects of security is essential for developing effective solutions. Addressing the challenges of enhancing communication security for in-vehicle WSNs demands a proactive, adaptive research technique that anticipates future challenges, explores the integration of novel technologies, and promotes interdisciplinary collaboration. Traditional security frameworks need to be changed and improved to work with the changing and limited environment of in-vehicle WSNs. One way to do this could be to create lightweight encryption methods and effective key management systems.

While existing research, such as the integration of blockchain technology and physical layer security, aims to enhance data security and network integrity, these methods often face challenges related to high computational and energy demands, limiting their practical application in resource-constrained environments like vehicles. In contrast, the proposed framework focuses on the efficient management of cryptographic keys and network segmentation to ensure secure communication between subsystems without imposing significant resource overheads.

References

1. Murshed, A.; Anowar, S.S. Automatic Braking System and Smart Safety Features to Avoid and Reduce Road Accident. Ph.D. Thesis, BRAC University, Dhaka, Bangladesh, 2021.
2. Wang, Y.; Cui, Y.; Chen, F.; Ren, R. An “illumination moving with the vehicle” intelligent control system of road tunnel lighting. Sustainability 2020, 12, 7314.

3. Gautam, A.; Verma, G.; Qamar, S.; Shekhar, S. Vehicle pollution monitoring, control and challan system using MQ2 sensor based on Internet of things. Wirel. Pers. Commun. 2021, 116, 1071–1085.
4. Bharati, S.; Podder, P.; Mondal, M.; Robel, M.R.A. Threats and countermeasures of cyber security in direct and remote vehicle communication systems. arXiv 2020, arXiv:2006.08723.
5. Choudhary, D.; Pahuja, R. Deep learning approach for encryption techniques in vehicular networks. Wirel. Pers. Commun. 2022, 125, 1–27.
6. Olaniyi, O.O.; Okunleye, O.J.; Olabanji, S.O.; Asonze, C.U. IoT security in the era of ubiquitous computing: A multidisciplinary approach to addressing vulnerabilities and promoting resilience. Asian J. Res. Comput. Sci. 2023, 16, 354–371.
7. Menon, V.G.; Jacob, S.; Joseph, S.; Sehdev, P.; Khosravi, M.R.; Al-Turjman, F. An IoT-enabled intelligent automobile system for smart cities. Internet Things 2022, 18, 100213.
8. Olufowobi, H.; Bloom, G. Connected cars: Automotive cybersecurity and privacy for smart cities. In Smart Cities Cybersecurity and Privacy; Elsevier: Amsterdam, The Nerthlands, 2019; pp. 227–240.
9. Xiong, Z.; Cai, Z.; Han, Q.; Alrawais, A.; Li, W. ADGAN: Protect your location privacy in camera data of auto-driving vehicles. IEEE Trans. Ind. Inform. 2020, 17, 6200–6210.
10. Ghosal, A.; Conti, M. Security issues and challenges in V2X: A survey. Comput. Netw. 2020, 169, 107093.
11. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. Veh. Commun. 2020, 23, 100214.
12. Rathore, R.S.; Hewage, C.; Kaiwartya, O.; Lloret, J. In-vehicle communication cyber security: Challenges and solutions. Sensors 2022, 22, 6679.
13. Hsiao, S.J.; Sung, W.T. Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks. IEEE Access 2021, 9, 72326–72341.
14. Xiao, X.; Li, Y.; He, X.; Cai, Y.; Xiao, Y.; Huang, B.; Jin, X. Optimal Topology Control of Monitoring Sensor Network Based on Physical Layer Security for Smart Photovoltaic Power System. Front. Energy Res. 2023, 11, 1124700.
15. Chen, Z.; Li, X.; Yang, B.; Zhang, Q. A Self-Adaptive Wireless Sensor Network Coverage Method for Intrusion Tolerance Based on Trust Value. J. Sens. 2015, 2015, 430456.
16. Li, J. A Symmetric Cryptography Algorithm in Wireless Sensor Network Security. Int. J. Online Eng. (IJOE) 2017, 13, 102.
17. Delgado-Mohatar, O.; Sierra, J.M.; Brankovic, L.; Fúster-Sabater, A. An energy-efficient symmetric cryptography based authentication scheme for wireless sensor networks. In Proceedings of the Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices: 4th IFIP WG 11.2 International Workshop, WISTP 2010, Passau, Germany, 12–14 April 2010; Proceedings 4. Springer: Berlin/Heidelberg, Germany, 2010; pp. 332–339.
18. Fang, X.; Fang, K.; Li, G.; Jin, X.; Zheng, L. Research on the Characteristics and Detection Methods of DDoS Attacks on Wireless Sensor Networks for Vehicle Networking. Eng. Adv. 2022, 2, 175–181.
19. Miptahudin, A.; Suryani, T.; Wirawan, W. Wireless Sensor Network Based Monitoring System: Implementation, Constraints, and Solution. JOIV Int. J. Inform. Vis. 2022, 6, 778–783.
20. Tetteh, A.; Essah, R.; Badhon, A.J.; Asante, Y.A.; Patrick, A.B. A Statistical Study Into Network Security Issues of IT Companies in Accra. Asian J. Res. Comput. Sci. 2021, 12, 1–13.
21. Qiu, B.; Xiao, H.; Chronopoulos, A.T.; Zhou, D.; Ouyang, S. Optimal Access Scheme for Security Provisioning of C-V2x Computation Offloading Network With Imperfect CSI. IEEE Access 2020, 8, 9680–9691.
22. Jameel, F.; Javed, M.A.; Zeadally, S.; Jantti, R. Secure Transmission in Cellular V2X Communications Using Deep Q-Learning. IEEE Trans. Intell. Transp. Syst. 2022, 23, 17167–17176.