World Journal of Engineering Research
Print ISSN: 2959-9865
Online ISSN: 2959-9873
DOI: https://doi.org/10.61784/wjer3049

A HYBRID IDENTITY AUTHENTICATION SYSTEM COMBINING PHYSICAL LAYER RECOGNITION AND CERTIFICATES FOR C-V2X IN HIGHWAY ENVIRONMENTS

YuanYuan Song[1*], Yitzhak Cohen[2]
[1]*Shandong Zhengchen Technology company limited, Jinan 250101, Shandong, China.*
[2]*SCOPE Strategic Management Ltd, Drech Begen 156, Tel Aviv-Jaffa, Israe.*
Corresponding Author: YuanYuan Song, E-mail: 245194050@qq.com

Abstract: With the rapid development of Cellular Vehicle-to-Everything (C-V2X) communication systems, ensuring the security and integrity of data exchanged between vehicles and infrastructure has become a significant challenge. Identity authentication plays a crucial role in safeguarding these communications against threats such as identity spoofing and data tampering. Traditional certificate-based authentication methods, while effective, often suffer from performance issues, especially in high-speed, dynamic environments such as highways. In this paper, we propose a hybrid identity authentication system that combines physical layer recognition with certificate-based methods to enhance security and improve real-time performance in C-V2X systems operating in highway environments. The physical layer authentication leverages channel state information (CSI), signal fingerprints, and other radio-frequency characteristics to authenticate vehicles, providing an additional layer of security. This is combined with certificate-based public key infrastructure (PKI) to offer a comprehensive and robust identity verification process. The hybrid approach addresses the shortcomings of traditional methods by enhancing security while minimizing computational overhead and ensuring low-latency authentication. We discuss the challenges and opportunities in integrating these two authentication methods and highlight the potential impact of emerging technologies, such as 5G and machine learning, in optimizing the hybrid authentication process for C-V2X systems. Finally, we propose future research directions to further improve the efficiency, scalability, and robustness of hybrid authentication schemes in vehicular networks.
Keywords: C-V2X; Vehicles; Public key infrastructure

1 INTRODUCTION

With the rapid development of intelligent transportation systems (ITS) and Vehicle-to-Everything (V2X) communication technologies, the exchange of information between vehicles and infrastructure has seen growing applications in traffic management, road safety, and real-time data transmission. Specifically. Cellular V2X (C-V2X) technology is gaining significant attention in highway environments due to its low latency and high reliability, which enable efficient traffic flow management and accident prevention [1]. However, this widespread deployment raises significant security concerns, particularly regarding identity authentication in an open wireless communication environment. Threats such as identity spoofing and data tampering compromise the integrity of the system and undermine the trustworthiness of V2X applications [2].

Traditional identity authentication methods, such as certificate-based public key infrastructure (PKI) systems, offer a level of security in vehicular networks [3]. However, they often face performance bottlenecks in high-speed, low-latency environments due to the computational complexity and communication overhead involved [4]. Additionally, although physical layer-based authentication techniques—such as recognition based on channel state information and radio frequency (RF) characteristics—have been widely studied in recent years, integrating these physical layer characteristics with high-level certificate-based authentication methods remains a challenging research topic. This hybrid approach could offer enhanced security and reliability for C-V2X systems, especially in high-speed environments like highways .

Highway environments present unique challenges for C-V2X systems, including high-speed vehicular mobility, complex interference patterns, and the need to support massive numbers of vehicles [5]. While certificate-based identity authentication methods can ensure a degree of security, they are not always sufficient to meet real-time performance requirements in high-speed highway scenarios. As a result, combining physical layer information with certificate-based methods could significantly improve both the efficiency and security of authentication processes in such environments. This paper presents a hybrid identity authentication system that integrates physical layer recognition with traditional certificate-based authentication, aiming to address the security challenges faced by C-V2X systems in highway environments. Figure 1 shows the working principle of the C-V2X communication hybrid identity authentication system.

The paper first provides an overview of current research in C-V2X identity authentication, highlighting the limitations of existing methods and technologies in real-world applications. Next, the discussion focuses on the integration of physical layer authentication, exploring how it can enhance security and performance in highway environments. Finally,

the paper outlines future research directions and challenges in realizing a secure and efficient hybrid authentication system for C-V2X.

Figure 1 Hybrid Identity Authentication System for C-V2X Communication

2 CURRENT RESEARCH ON C-V2X IDENTITY AUTHENTICATION

Identity authentication plays a crucial role in ensuring the integrity, authenticity, and privacy of communication in C-V2X systems [6]. As C-V2X applications increasingly span across highway environments, ensuring secure communication between vehicles, roadside units, and infrastructure becomes a priority. Over the years, various authentication methods have been proposed and developed to address these challenges. These methods generally focus on public key infrastructures (PKI), certificate-based authentication, and more recently, physical layer-based authentication techniques, each offering distinct advantages and limitations.

2.1 Certificate-Based Authentication

Certificate-based authentication remains one of the most widely adopted methods for ensuring secure identity verification in C-V2X systems. By utilizing a public-key infrastructure (PKI), certificates are issued to vehicles and infrastructure devices, which are used to validate the identity of the communication entities [7]. This method guarantees the integrity and authenticity of messages exchanged over the network, as it relies on the encryption of data with public and private keys.

However, traditional certificate-based authentication methods suffer from significant performance issues, especially in high-speed highway environments. The computation and verification processes involved in issuing and validating certificates are resource-intensive and can lead to high latency, which is detrimental in real-time applications where low-latency communication is critical. Additionally, these systems are vulnerable to attacks such as certificate spoofing and unauthorized certificate revocation, which compromise the system's security [8].

2.2 Physical Layer Authentication

In contrast to certificate-based approaches, physical layer authentication techniques utilize unique physical characteristics of the communication channel or radio signals to verify the identity of communication entities [9]. These characteristics include channel state information (CSI), the unique multipath propagation of signals, and received signal strength. Physical layer authentication offers a promising alternative as it operates independently of higher-layer cryptographic mechanisms and can enhance system security by providing an additional layer of verification.

However, the integration of physical layer authentication with traditional certificate-based methods remains a challenge [10]. While physical layer methods can improve security, they are often sensitive to environmental factors such as noise, interference, and fading, which can degrade their effectiveness in real-world applications. Moreover, these methods require sophisticated hardware and signal processing techniques, which may introduce additional costs and complexity to the system.

2.3 Hybrid Authentication Approaches

Given the limitations of certificate-based and physical layer authentication methods when used independently, hybrid authentication schemes have been proposed to combine the strengths of both approaches [11]. By integrating physical layer features with certificate-based authentication, hybrid systems aim to provide more robust security while maintaining performance in high-speed and dynamic environments like highways.

Hybrid approaches offer several advantages over individual methods, including enhanced security, reduced risk of identity spoofing, and faster authentication processes [12]. However, these systems face challenges in terms of

computational complexity, real-time processing requirements, and hardware limitations. Future research is needed to address these challenges and optimize the integration of physical and certificate-based authentication in C-V2X systems.

3 CHALLENGES AND OPPORTUNITIES IN HYBRID IDENTITY AUTHENTICATION FOR C-V2X

While hybrid identity authentication systems combining physical layer recognition and certificate-based methods hold great promise for enhancing the security and reliability of C-V2X systems, several challenges remain to be addressed [13]. These challenges primarily stem from the need to integrate two fundamentally different approaches—physical layer characteristics and higher-layer cryptographic techniques—into a unified, efficient, and practical authentication framework. Despite these challenges, the hybrid approach offers substantial opportunities for improving the performance and security of C-V2X systems, especially in dynamic and high-speed highway environments.

3.1 Challenges in Integration

One of the primary challenges in implementing hybrid authentication for C-V2X systems is the complexity of integrating physical layer recognition techniques with certificate-based authentication [14]. Physical layer authentication methods, such as those based on channel state information (CSI) and signal fingerprints, require specialized hardware and signal processing algorithms to extract the relevant features. These methods rely on accurate measurements of the radio environment, which can be susceptible to factors such as interference, fading, and multi-path propagation. Integrating these features with traditional cryptographic operations used in certificate-based authentication introduces additional computational and communication overhead, which can impact the real-time performance of C-V2X systems in high-speed environments [15,16].

Moreover, the environmental conditions in highway scenarios, such as rapidly changing vehicle velocities and complex interference patterns, make it difficult to consistently obtain accurate and reliable physical layer features. The effectiveness of physical layer authentication methods may degrade due to factors such as signal noise, Doppler shifts, and vehicle mobility. These issues highlight the need for robust signal processing algorithms capable of accurately extracting features despite varying environmental conditions and high mobility [17,18].

3.2 Computational Complexity and Real-Time Processing

Another challenge in hybrid authentication systems is the computational complexity associated with processing physical layer features and verifying digital certificates in real time. Certificate-based authentication schemes, particularly those based on public-key cryptography, are computationally intensive, requiring significant processing power for key generation, signing, and verification. When combined with physical layer authentication, the system must process both signal characteristics and cryptographic data, further increasing the computational load.

In highway environments, where vehicles are moving at high speeds, the authentication process must be completed within a very short time frame to avoid delays in communication and ensure safe driving conditions. The need for low-latency communication and high throughput places a premium on the efficiency of the authentication process. As a result, the hybrid authentication system must be optimized to minimize computational overhead while maintaining a high level of security and reliability [19]. Figure 2 shows the C-V2X communication principle between the vehicle and the RSU.

Figure 2 C-V2X Communication between Vehicles and RSU

3.3 Opportunities for Improvement

Despite the challenges, the hybrid approach presents several opportunities to enhance the security and performance of C-V2X systems. One of the key advantages is the ability to provide multiple layers of security, making it more difficult for attackers to compromise the system. By combining the strengths of physical layer authentication, which is resistant to certain types of spoofing attacks, with the robust security guarantees of certificate-based methods, the hybrid system can offer enhanced protection against both physical and cryptographic threats.

Moreover, advancements in signal processing algorithms and hardware are opening up new opportunities for more efficient and accurate physical layer authentication. Machine learning and artificial intelligence (AI) techniques, in particular, have shown promise in improving the accuracy of physical layer authentication by automatically learning to recognize patterns in signal characteristics, even under noisy or variable conditions [20]. These techniques can significantly reduce the impact of environmental factors such as interference and fading, making physical layer authentication more reliable in real-world highway environments.

Additionally, emerging technologies such as 5G and beyond offer the potential to improve the performance of hybrid authentication systems. With higher bandwidth, lower latency, and better support for massive IoT devices, these next-generation networks could facilitate the real-time processing of both physical layer and certificate-based authentication, making hybrid systems more scalable and practical for large-scale deployment in C-V2X networks [21].

3.4 Future Directions

Looking ahead, there are several key areas where further research is needed to address the challenges and fully realize the potential of hybrid identity authentication systems for C-V2X. These include:

Robust Signal Processing: Developing advanced signal processing techniques that can extract reliable physical layer features under diverse environmental conditions, including high mobility and interference.

Lightweight Cryptographic Methods: Designing lightweight cryptographic protocols that can reduce the computational overhead associated with certificate-based authentication, ensuring real-time performance in high-speed environments.

Machine Learning Integration: Leveraging machine learning and AI to improve the accuracy and adaptability of physical layer authentication, enabling the system to learn and adapt to changing environmental factors.

Integration with 5G Networks: Exploring the synergies between hybrid authentication systems and 5G networks to enable seamless, scalable, and low-latency authentication processes for C-V2X communications.

4 CONCLUSION AND FUTURE OUTLOOK

In this paper, we have discussed the challenges and opportunities associated with hybrid identity authentication systems combining physical layer recognition and certificate-based methods for C-V2X communication in highway environments. The security of C-V2X systems is paramount to ensure reliable and safe communication between vehicles and infrastructure, especially in high-speed, dynamic environments like highways. Traditional certificate-based authentication methods, although effective in many scenarios, face limitations in high-speed vehicular networks due to performance bottlenecks and vulnerability to certain types of attacks. On the other hand, physical layer authentication provides an additional layer of security by leveraging the unique characteristics of the communication channel, but it also faces challenges related to environmental variability, signal noise, and hardware requirements.

By combining the strengths of both approaches, hybrid identity authentication systems offer a promising solution to the security challenges faced by C-V2X networks. The integration of physical layer authentication with certificate-based methods can enhance both the security and efficiency of the authentication process, providing a more robust defense against identity spoofing and other malicious attacks. However, significant challenges remain, including the need for effective integration of physical and cryptographic methods, the computational complexity of real-time processing, and the reliability of physical layer authentication under varying environmental conditions.

Despite these challenges, the potential for hybrid authentication systems to revolutionize the security landscape of C-V2X systems is immense. Advances in machine learning, signal processing, and next-generation networks such as 5G will likely play a pivotal role in addressing these challenges and improving the overall performance of hybrid authentication systems. Future research efforts should focus on optimizing the integration of physical and certificate-based authentication, reducing computational overhead, and developing more robust signal processing techniques that can adapt to the highly dynamic nature of highway environments.

Looking forward, several key areas warrant further exploration:

Optimization of Hybrid Systems: Further research should aim to refine hybrid authentication techniques to ensure that they can be efficiently implemented in real-time C-V2X systems without compromising security or performance.

Advanced Machine Learning Algorithms: The application of machine learning and AI to improve the accuracy and robustness of physical layer authentication, particularly in noisy and highly dynamic environments, holds great potential.

5G Integration: With the advent of 5G networks, new opportunities emerge for supporting hybrid authentication systems at scale, with the potential to handle high-speed vehicular communication with lower latency and higher throughput.

Scalability and Robustness: Future studies should focus on ensuring that hybrid authentication systems can scale to large numbers of vehicles and infrastructure elements while maintaining reliability under a wide range of operational conditions.

In conclusion, while hybrid identity authentication systems for C-V2X communications face several technical challenges, they represent a promising direction for enhancing the security of vehicular networks in highway environments. As research continues to evolve and technologies such as 5G and machine learning mature, the potential for these systems to provide secure, low-latency, and reliable authentication for C-V2X networks is becoming increasingly achievable.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

FUNDING

This work was supported in part by Key R&D Program of Shandong Province (2022KJHZ002).

REFERENCES

[1] Hu H, Chai R, Chen ML, et al. System-level simulation platform of C-V2X mode 4: Integrating CarMaker and NS-3. IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2021. DOI: 10.1109/PIMRC50174.2021.9569386.

[2] Eckermann F, Wietfeld C. SDR-based open-source C-V2X traffic generator for stress testing vehicular communication. IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), 2021. DOI: 10.1109/VTC2021-Spring51267.2021.9449043.

[3] Peters S, Sivrikaya F, Dang XT. SEP4CAM – a simulative/emulative platform for C-V2X application development in cross-border and cross-domain environments. IEEE/ACM 25th International Symposium on Distributed Simulation and Real Time Applications (DS-RT 2021), 2021. DOI: 10.1109/DS-RT52167.2021.9576134.

[4] Abbasi HI, Gholmieh R, Nguyen TV, et al. LTE-V2X (C-V2X) performance in congested highway scenarios. IEEE International Conference on Communications (ICC 2022), 2022: 303-308. DOI: 10.1109/ICC45855.2022.9838706.

[5] Miao LL, Virtusio JJ, Hua KL. PC5-based cellular-V2X evolution and deployment. Sensors, 2021, 21(3): 843. DOI: 10.3390/s21030843.

[6] Wang DL, Sattiraju RR, Qiu AJ, et al. Effect of retransmissions on the performance of C-V2X communication for 5G. IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), 2020. DOI: 10.1109/VTC2020-Fall49728.2020.9348560.

[7] Liu Q, Liang P, Xia JJ, et al. A highly accurate positioning solution for C-V2X systems. Sensors, 2021, 21(4): 1175. DOI: 10.3390/s21041175.

[8] Molina-Masegosa R, Gozalvez J, Sepulcre M. Configuration of the C-V2X mode 4 sidelink PC5 interface for vehicular communications. 14th International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2018), 2018: 43-48. DOI: 10.1109/MSN.2018.00014.

[9] Yoshioka S, Nagata S. Cellular V2X standardization in 4G and 5G. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2022, E105A(5): 754-762. DOI: 10.1587/transfun.2021WBI0001.

[10] Park J, Kavathekar V, Bhuduri S, et al. A co-operative perception system for collision avoidance using C-V2X and client-server-based object detection. Sensors, 2025, 25(17): 5544. DOI: 10.3390/s25175544.

[11] Ficzere D, Varga P, Wippelhauser A, Hejazi H, Csernyava O, Kovács A, Hegedus C. Large-scale cellular vehicle-to-everything deployments based on 5G – critical challenges, solutions, and vision towards 6G: A survey. Sensors, 2023, 23(16): 7031. DOI: 10.3390/s23167031.

[12] Chen SZ, Hu JL, Shi Y, et al. A vision of C-V2X: Technologies, field testing, and challenges with Chinese development. IEEE Internet of Things Journal, 2020, 7(5): 3872-3881. DOI: 10.1109/JIOT.2020.2974823.

[13] Chen ML, Chai R, Hu H, et al. Performance evaluation of C-V2X mode 4 communications. IEEE Wireless Communications and Networking Conference (WCNC), 2021. DOI: 10.1109/WCNC49053.2021.9417517.

[14] Li P, Wu K, Cheng Y, et al. How does C-V2X perform in urban environments? Results from real-world experiments on urban arterials. IEEE Transactions on Intelligent Vehicles, 2024, 9(1): 2520-2530. DOI: 10.1109/TIV.2023.3326735.

[15] Ning RR, Zhang XK, Feng WY, et al. Performance analysis of vehicle platoon communication in C-V2X autonomous mode. IEEE 23rd International Conference on High Performance Switching and Routing (HPSR), 2022: 41-46. DOI: 10.1109/HPSR54439.2022.9831348.

[16] Kumar RD, Rammohan A. Revolutionizing intelligent transportation systems with cellular vehicle-to-everything (C-V2X) technology: Current trends, use cases, emerging technologies, standardization bodies, industry analytics and future directions. Vehicular Communications, 2023, 43: 100638. DOI: 10.1016/j.vehcom.2023.100638.

[17] Hua QZ, Yu KP, Wen Z, Sato T. A novel base-station selection strategy for cellular vehicle-to-everything (C-V2X) communications. Applied Sciences-Basel, 2019, 9(3): 556. DOI: 10.3390/app9030556.

[18] Twardokus G, Rahbari H. Vehicle-to-nothing? Securing C-V2X against protocol-aware DoS attacks. IEEE Conference on Computer Communications (INFOCOM), 2022: 1629-1638. DOI: 10.1109/INFOCOM48880.2022.9796667.
[19] Chen SZ, Li Q, Wang Y, et al. C-V2X equipment identification management and authentication mechanism. China Communications, 2021, 18(8): 297-306.
[20] Flowers B, Ku YJ, Baidya S, et al. Utilizing reinforcement learning for adaptive sensor data sharing over C-V2X communications. IEEE Transactions on Vehicular Technology, 2024, 73(3): 4051-4066. DOI: 10.1109/TVT.2023.3322068.
[21] Brady C, Cao L, Roy S. Modeling of NR C-V2X mode 2 throughput. IEEE International Workshop on Communications Quality and Reliability (CQR), 2022: 19-24. DOI: 10.1109/CQR54764.2022.9918559.