PROCEEDINGS OF

INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS AND NEW APPLICATIONS

https://proceedings.icisna.org/

2nd International Conference on Intelligent Systems and New Applications (ICISNA'24), Liverpool, April 26-28, 2024.

Enhancing the Internet of Vehicles through Collaborative Cryptographic Mechanisms with IRS

Ahmed Aljumaili[1], Hafedh Trabelsi[2], Wassim Jerbi[2], Rafal Hazim[1]

[1]College of Engineering Technology, Al-Kitab University, Kirkuk 36015, Iraq

[2]CES LAB, ENIS, University of Sfax, Sfax, Tunisia

ahmedh.ali@uoalkitab.edu.iq, ORCID: 0009-0000-0538-5470

hafedh.trabelsi@enis.tn, ORCID: 0000-0002-5268-506X

Wassim.jerbi@isetn.run.tn, ORCID: 0000-0002-1618-7469

rafal.alnassir@uoalkitab.edu.iq, ORCID: 0009-0000-0880-495X

***Abstract*— The Internet of Vehicles (IoV) is transforming transportation systems by allowing for seamless communication and collaboration between vehicles, roadside units (RSUs), and cloud servers. However, the dynamic and varied character of IoV settings raises serious security and efficiency concerns. This work suggests a novel strategy to addressing these issues by combining collaborative cryptographic processes and intelligent reflecting surfaces (IRS). Our method uses modern encryption techniques, such as the modern Encryption Standard (AES), to assure safe data delivery, while intelligent reflecting surfaces dynamically modify their reflection qualities to improve signal propagation and reception. We provide a detailed network model and algorithmic framework for implementing the suggested strategy, with a focus on cryptographic techniques and the role of intelligent reflecting surfaces in improving communication security and efficiency. Through theoretical analysis and debate, we emphasize the possible benefits of incorporating intelligent reflecting surfaces in IoV networks, such as improved network coverage, lower communication costs, and increased energy efficiency. Furthermore, we explore the implications of our strategy for IoV security and suggest future research areas in this area.**

***Keywords*—Internet of Vehicles, collaboration, security, efficiency, cryptographic techniques, intelligent reflecting surfaces (IRS), and communication.**

I. Introduction

IoV proposes a paradigm shift in transportation systems, utilizing cutting-edge communication technology to improve safety, efficiency, and convenience. IoV enables vehicles to interact with one another, with roadside infrastructure, and with centralized control systems, allowing for real-time data interchange and informed decision-making. As IoV systems become more widely used, protecting communication security and privacy becomes increasingly important.

This study describes a collaborative cryptographic approach that uses the IRS to ensure safe communication in IoV environments. Our proposed strategy to addressing security and performance concerns in IoV systems combines symmetric cryptographic approaches such as the AES with IRS. Unlike traditional cryptographic systems, which rely primarily on encryption algorithms, we use IRS to improve communication reliability, coverage, and energy efficiency.

The main contributions of this study are the invention of a unique cryptographic technique designed for IoV scenarios and the incorporation of IRS to improve communication capabilities. We demonstrate the usefulness of our strategy in reducing security risks and enhancing communication performance in IoV environments using thorough simulations and analysis.

The rest of the paper is organized as follows: Section 2 summarizes current research in the subject of IoV security and communication protocols. Section 3 describes the network model and computational framework used in our suggested approach. Section 4 describes the cryptographic mechanisms used to ensure safe communication in IoV environments. Section 5 discusses the integration of IRS and their function in improving communication within IoV systems. Section 6 examines the difficulties found during our research and identifies potential areas for further research and growth. Finally, Section 7 summarizes the article and discusses future research directions.

II. Related Work

The paper provides a comprehensive overview of authentication protocols in the IoV domain, as evidenced by Bagga et al. [1]. It delves into the taxonomy, analysis, and challenges surrounding these protocols, offering valuable insights into the security landscape of IoV systems.

In addition, the work explores the challenges and solutions in IoV presented by Fadhil and Sarhan [2]. This survey elucidates the various hurdles encountered in the IoV ecosystem and proposes potential solutions to address them, contributing to a deeper understanding of the field.

Furthermore, Storck and Duarte-Figueiredo [3] conduct a comprehensive survey on 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications in IoV. Their research sheds light on the advancements in communication technologies that underpin IoV systems, highlighting the importance of robust infrastructure for enabling seamless connectivity and communication among vehicles and their surroundings.

Chen et al. [4] present a secure authentication protocol tailored for the IoV, focusing on ensuring the integrity and confidentiality of communication between vehicles and their surrounding infrastructure. Their work contributes to enhancing the security posture of IoV systems, addressing the unique challenges posed by the dynamic and interconnected nature of vehicular networks.

Garg et al. [5] conduct a comprehensive survey that delves into the myriad security and privacy issues prevalent in IoV ecosystems. By identifying and analyzing these challenges, their research provides valuable insights into the vulnerabilities inherent in IoV systems and lays the groundwork for developing robust security mechanisms to mitigate potential threats.

Chaudhry [6] proposes an efficient and secure message exchange protocol specifically designed for IoV environments. By prioritizing both efficiency and security, Chaudhry’s protocol aims to facilitate seamless communication among vehicles while ensuring the confidentiality and integrity of exchanged messages, thereby enhancing the overall reliability of IoV systems.

Vasudev et al. [7] introduce a lightweight mutual authenti protocol tailored for vehicle-to-vehicle (V2V) communication on within IoV frameworks. Their protocol emphasizes the importance of mutual authentication in establishing trust among communicating vehicles, thereby fostering a secure and resilient IoV ecosystem capable of withstanding various security threats and attacks.

Hakimi et al. [8] present a survey on the Internet of Vehicle (IoV), focusing on its applications and comparing various technologies such as Vehicular Ad-Hoc Network (VANET), IoV, and SDN-IoV. By examining the characteristics and capabilities of these technologies, the authors provide insights into the diverse applications and potential advantages of IoV systems in different contexts.

Sharma and Mohan [9] explore a cloud based secured VANET with advanced resource management and IoV applications. Their research investigates the integration of cloud computing technologies to enhance the security and efficiency of VANETs, particularly in the context of IoV applications. By leveraging cloud resources, their approach aims to improve the scalability, reliability, and performance of VANETs in supporting various IoV services.

Elsagheer Mohamed and AlShalfan [10] propose an Intelligent Traffic Management System based on the IoV. Their work focuses on leveraging IoV technology to develop intelligent systems for managing traffic flow and improving transportation efficiency. By integrating IoV capabilities into traffic management systems, the authors aim to enhance safety, reduce congestion, and optimize resource utilization in urban transportation networks.

Karim et al. [11] conduct a comprehensive analysis of the architecture, protocols, and security considerations in IoV systems. Their work presents a taxonomy of IoV architectures, analyzes various protocols used in IoV deployments, and discusses the challenges and solutions related to security in IoV environments. By addressing these key aspects, their research contributes to the understanding and advancement of IoV technology, paving the way for more secure and efficient deployments.

Hakak et al. [12] present a survey on autonomous vehicles (AVs) in the context of 5G and beyond. Their work investigates the integration of AVs with advanced communication technologies, focusing on the potential of 5G networks and beyond to enable various autonomous driving applications. By examining the current state of AV technology and its evolution alongside communication infrastructures, the authors provide insights into the opportunities and challenges associated with the deployment of AVs in future transportation systems.

Agbaje et al. [13] conducted a survey on interoperability challenges in the IoV. Their research identifies and analyzes the interoperability issues that arise in IoV environments, considering the integration of diverse vehicular communication technologies and standards. By addressing these challenges, the authors aim to facilitate seamless communication and collaboration among vehicles and infrastructure elements within IoV ecosystems.

Abbasi et al. [14] explore the architecture, services, and applications of the IoV. Their work provides an overview of IoV technology, highlighting its architecture components, the services it enables, and the diverse applications it supports. By examining the functionalities and potential use cases of IoV systems, the authors contribute to a better understanding of the IoV landscape and its implications for future transportation systems.

Mahmood [15] investigates connected vehicles in the IoV, focusing on the concepts, technologies, and architectures that underpin these systems. The research discusses the fundamental principles of connected vehicles, including communication protocols, network architectures, and architectural components. By examining the key concepts and technologies driving connected vehicles in the IoV, the author provides valuable insights into the design and deployment considerations for connected vehicle systems.

Ahangar et al. [16] present a survey of autonomous vehicles, focusing on the communication technologies that enable their operation and the challenges associated with their deployment. The research examines various communication technologies used in AVs, including sensors, wireless communication protocols, and networking architectures. By addressing the communication requirements and challenges of AVs, the authors contribute to the understanding of the technological landscape shaping the future of autonomous transportation.

Ji et al. [17] present a survey on the IoV, focusing on network architectures and applications. The authors investigate various network architectures employed in IoV systems and discuss their applications across different domains. By providing insights into the design principles and deployment scenarios of IoV networks, the survey contributes to a better understanding of the evolving landscape of vehicular communication systems.

Ali et al. [18] explore machine learning technologies to secure vehicular communication in the IoV. Their work reviews recent advances and applications of machine learning in enhancing the security of vehicular communication systems. By examining the role of machine learning algorithms in detecting and mitigating security threats in the IoV, the authors provide valuable insights into the potential of these technologies to address cybersecurity challenges in connected vehicle environments.

Noura et al. [19] propose LoRCA, Lightweight Round Block and Stream Cipher Algorithms for IoV systems. The research introduces efficient encryption algorithms tailored to the resource-constrained environment of IoV systems. By developing lightweight cryptographic solutions, the authors aim to enhance the security of communication in IoV networks without imposing significant overhead on computational resources.

Alaya and Sellami [20] present a clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks. Their work focuses on enhancing the security of VANETs deployed in urban environments. By leveraging clustering techniques and cryptographic mechanisms, the authors aim to mitigate security threats and improve the resilience of VANETs against malicious attacks.

Saleem et al. [21] provide comments on the Authenticated Key Management (AKM-IoV) protocol proposed for fog computing-based IoV deployment. The authors offer insights and critiques on the design and implementation of the AKM-IoV protocol, highlighting its strengths and limitations. Through their analysis, they contribute to the ongoing discourse on secure key management protocols for IoV environments, offering suggestions for improvement and future research directions.

Eyadeh et al. [23] present a study on the modeling and simulation of performance limits in the IEEE 802.11-point coordination function. Their research, published in the International Journal of Recent Technology and Engineering, investigates the performance boundaries of the IEEE 802.11 standard's point-coordination function. Through modeling and simulation techniques, the authors analyze the factors influencing the performance limits of this function, providing valuable insights for optimizing wireless communication protocols.

Jerbi et al. [24], [25] introduce Crypto-ECC, a rapid secure protocol designed for large-scale wireless sensor networks deployed on the Internet of Things (IoT). Their work, published in the book" Theory and Applications of Dependable Computer Systems," focuses on enhancing the security of IoT deployments by proposing a cryptographic protocol tailored to the resource constraints of wireless sensor networks. By leveraging elliptic curve cryptography (ECC), Crypto-ECC aims to provide rapid and efficient security solutions for IoT applications.

Jerbi et al. [26] present CoopECC, a collaborative cryptographic mechanism specifically designed for the Internet of Things (IoT). Published in the Journal of Sensors, their research introduces a novel approach to cryptographic key management in IoT environments. CoopECC leverages collaboration among IoT devices to enhance the efficiency and security of cryptographic operations, offering a promising solution for securing IoT deployments against various cyber threats.

III. Proposed Architecture for IoV

The Internet of Vehicles architecture is a multi-layered, intricate system. As illustrated in Figure 1, the vehicle, network, RSU, infrastructure, Cloud Server (CS), trusted authority (TA), data analytics, applications, and security are the essential elements of an IoV architecture. The vehicle itself is the primary element of the IoV architecture. Smart sensors and other intelligent gadgets allow vehicles to talk to the environment and to other vehicles [27] – [29].

Cellular networks, Wi-Fi, and Dedicated Short Range Communications (DSRC) protocols are some of the communication technologies that allow connectivity between cars and the Internet at the network layer. The cloud layer provides data processing and storage capabilities for the Internet of Vehicles. Multiple vehicle data points can be combined and analyzed by CS to provide real-time insights about traffic patterns, road conditions, and other topics. The data analytics layer handles processing the massive amounts of data generated by the Internet of Vehicles [30].

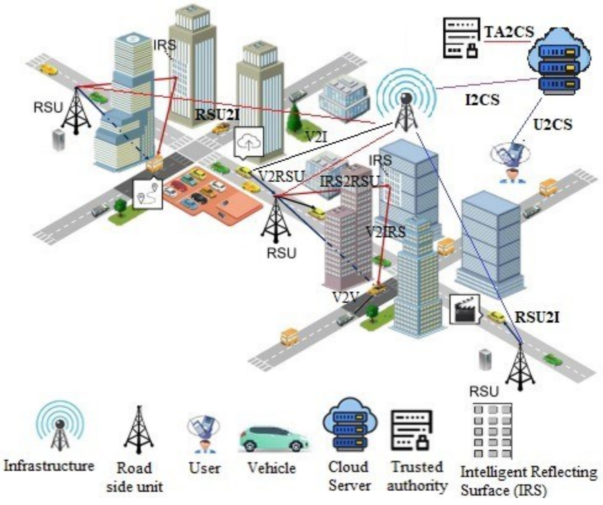

Fig. 1 A IoV system in a smart city environment

IV. NETWORK MODEL AND ALGORITHMIC FRAMEWORK

In this section, we describe the network model and the algorithmic framework utilized in our proposed approach for securing communication within the IoV environment.

Network Model

Our network model comprises several key entities [31], [32]:

- *Trusted Authority (TA):* Responsible for securely distributing keys between communicating entities.
- *CS:* Stores and manages data exchanged between entities.
- *Users (U):* End-users interacting with IoV services.
- *Vehicles:* Modeled as mobile nodes equipped with communication devices.
- *Roadside Units (RSUs):* Fixed infrastructure units deployed along roadways to facilitate communication with vehicles.
- *IRS:* Modeled as intelligent surfaces capable of dynamically adjusting their reflection properties to enhance communication between vehicles and RSUs.

Algorithmic Framework

In the context of the IoV, Algorithmic 1 offers an organized method for implementing cryptographic mechanisms and session establishment protocols. This allows for secure communication between entities and makes it easier to integrate IRS for improved network performance [33], [34].

Algorithm 1: Algorithmic Framework

Initialization:

1. Generate public/private key pairs for communicating entities.
2. Securely exchange public keys.
3. Generate a shared secret key using a secure key exchange mechanism.

Session Establishment:

1. Exchange nonces between entities.
2. Compute session keys using AES-Key-Derivation.

Nominal Scenario:

1. Generate a random nonce.
2. Compute the session key using AES-Key-Derivation.
3. Encrypt the message using AES-GCM encryption.
4. Sign the message with the sender's private key.
5. Include the signature in the message header.
6. Transmit the encrypted and authenticated message.
7. On the receiving end, verify the signature using the sender's public key.
8. Derive the session key.
9. Decrypt the message.

Alternative Scenario (Key Update):

1. When a key update is required, generate new nonces N'A$ and N'B.
2. Compute the updated session key $K'S = AES-Key-Derivation (N'A, N'B, Shared Secret).
3. Use the updated session key for encryption and authentication.

Error Scenarios:

1. **Signature Verification Failure**: If the signature verification fails, discard the message and log the incident.
2. **Decryption Failure**: If the decryption fails, consider the message as corrupted or malicious and log the incident.
3. **Invalid Nonce**: If the nonce is not valid (e.g., repeated or out of sequence), reject the message and log the incident.
4. **Key Exchange Failure:** If the key exchange process fails, terminate the communication and log the incident.
5. **IRS Integration Failure**: If the integration of IRS fails, fallback to traditional communication or terminate the connection.

Intelligent Reflecting Surface (IRS) Integration:

1. Implement IRS functionality for secure communication.
2. Evaluate the impact of IRS on network coverage, cost reduction, and energy efficiency.

Algorithm Explanation

The network model and algorithmic framework for the IoV consist of the following components [35]– [37]:

1) Trusted Authority (TA): Responsible for securely distributing public and private keys between communicating entities in the IoV network.

2) CS: Serves as a centralized data repository for managing information exchanged between entities in the IoV network.

3) Users (U): Represent various stakeholders in the IoV ecosystem, including vehicle operators, administrators, passengers, and pedestrians.

4) Vehicles: Modeled as mobile nodes equipped with communication devices capable of securely transmitting and receiving data.

5) Roadside Units (RSUs): Fixed infrastructure units deployed along roadways to facilitate communication with vehicles.

6) IRS: Modeled as intelligent surfaces deployed in the environment to enhance communication between vehicles and RSUs.

The algorithmic framework comprises the following steps:

1) Initialization:

- Generate public/private key pairs for communicating entities.
- Securely exchange public keys between entities.
- Generate a shared secret key using a secure key exchange mechanism.

2) Session Establishment:

- Entities exchange nonces (random values) to establish a session key.
- Compute the session key using the exchanged nonces and the shared secret key.

3) Nominal Scenario:

- Generate a random nonce for each message transmission.
- Compute the session key for encryption and decryption.
- Encrypt the message using the AES-GCM encryption algorithm.
- Sign the message with the sender's private key to ensure authenticity.
- Transmit the encrypted and authenticated message along with the signature.
- On the receiving end, verify the signature and decrypt the message using the session key.

4) Intelligent Reflecting Surface (IRS) Integration:

- Implement IRS functionality to enhance communication between vehicles and RSUs.
- Evaluate the impact of IRS on network coverage, cost reduction, and energy efficiency through simulation and analysis.

Intelligent Reflecting Surface (IRS) Integration

IRS represents a revolutionary technology poised to transform communication paradigms within the IoV ecosystem. This section delves into the intricacies of seamlessly integrating IRS into existing vehicular communication architectures. By strategically deploying IRS along roadways and within urban environments, we aim to harness their reflective properties to enhance signal propagation, mitigate interference, and bolster the reliability of wireless communication between vehicles and RSUs. The integration of IRS not only holds the promise of extending network coverage to previously inaccessible areas but also opens avenues for optimizing spectrum utilization and reducing energy consumption in IoV deployments [38].

Leveraging advanced beam forming techniques and reconfigurable surface designs, IRS can actively manipulate electromagnetic waves to steer signals towards intended recipients, overcome signal attenuation, and mitigate multipath fading effects. Moreover, the deployment of IRS necessitates careful consideration of factors such as placement optimization, beam forming algorithms, and coordination mechanisms to maximize their efficacy in real-world scenarios.

By integrating IRS seamlessly into the IoV infrastructure, we aim to establish robust communication links that exhibit resilience to dynamic environmental conditions and vehicular mobility patterns. Considering recent advancements in wireless communication technologies, the integration of IRS emerges as a promising avenue for enhancing both the reliability and security of vehicular communication systems within the IoV.

IRS, equipped with reconfigurable reflective elements, can dynamically manipulate the propagation environment of wireless signals, enabling tailored signal focusing, beam forming, and interference mitigation. Beyond their conventional role in optimizing signal coverage and quality, IRS can be strategically deployed to fortify the security posture of IoV ecosystems. By leveraging their ability to create secure communication zones and thwart eavesdropping attempts, the IRS serves as a formidable line of defence against malicious actors seeking to compromise the confidentiality and integrity of vehicular data transmissions. Furthermore, through the integration of advanced signal processing algorithms and anomaly detection techniques, the IRS can actively monitor and mitigate potential cyber threats, thereby augmenting the overall cybersecurity resilience of IoV deployments. This section explores the multifaceted role of IRS in bolstering the security infrastructure of vehicular networks and highlights their potential to mitigate emerging cybersecurity challenges within IoV environments [39], [40].

V. Mechanisms For Secure Communication

In this section, we delve into the cryptographic mechanisms employed to ensure secure communication within the IoV ecosystem.

A. AES Encryption

Symmetric encryption uses AES, which provides robust cryptographic protection. AES provides key lengths of 128 bits, 192 bits, or 256 bits and operates on set block sizes. To maintain secrecy during transmission, we encrypt message payloads using AES [42].

B. AES-GCM Mode

Authenticated encryption uses AES in Galois/Counter Mode (AES-GCM), which protects both integrity and confidentiality. The authentication offered by Galois/Counter Mode is combined with the encryption capabilities of AES in AES-GCM. This guarantees that the communication is encrypted and that, upon decryption, its legitimacy is confirmed.

C. Key Exchange Mechanisms

Establishing shared secret keys between communication entities requires a secure key exchange. To securely negotiate session keys, we use reliable key exchange protocols like the Diffie-Hellman key exchange protocol. Message payloads are then encrypted and decrypted using these session keys symmetrically.

D. Digital Signatures

Digital signatures are used to ensure the authenticity and non-repudiation of messages. Using their respective public keys, recipient entities validate the signatures on communications that sender entities have signed using their private keys. By doing this, the IoV network's message exchanges are guaranteed to be legitimate and authentic.

E. Secure Hash Functions

SHA-256 and other secure hash algorithms are used to create fingerprints and message digests. During transmission, these digests are utilized to confirm the integrity of message payloads. Any message tampering can be identified by comparing the computed digest at the recipient's end with the transmitted digest [41].

VI. Integration of IRS

This section covers how IRS are incorporated into the IoV communication framework and how this affects communication efficiency and reliability.

A. IRS Functionality

Passive structures with reconfigurable reflecting elements that can change their properties to control electromagnetic waves are known as IRS. These surfaces can be integrated inside automobiles or positioned strategically along roadways to improve signal coverage and reduce propagation obstructions.

B. Dynamic Reflection Adjustment

Based on the traffic density, real-time ambient circumstances, and communication requirements, IRS dynamically modifies the reflection qualities of its elements. IRS enhances the communication reliability between automobiles and roadside units by strategically adjusting the phase and amplitude of reflected signals.

C. Collaborative Signal Optimization

IRS works in tandem with nearby cars and roadside apparatuses to maximize signal propagation routes. IRS eliminates interference among communication channels and maximizes the overall network throughput by coordinating reflection modifications and communicating signaling information.

D. Coverage Enhancement

Through the rerouting of signals around obstructions and dead zones, the integration of IRS increases the coverage range of current communication infrastructures. This increases communication link dependability and connectivity in tricky situations, particularly in crowded or obstructed regions.

E. Cost-Effective Deployment

With IRS deployment, you can increase network coverage and enhance communication quality at a lower cost without having to add more active equipment. Compared to conventional active relay stations, IRS uses less energy and minimizes infrastructure development costs by utilizing passive reflecting surfaces.

F. Energy Efficiency

By minimizing signal attenuation and improving signal transmission pathways, IRS promotes energy efficiency. IRS contributes to energy conservation in automobiles and roadside devices, which reduces signal losses and optimizes communication paths, resulting in overall network energy savings.

VII. Challenges and Future Research

Although the combination of IRS and cryptographic techniques has the potential to improve security and communication in the IoV, there are still several obstacles to overcome and directions for further study.

A. Security Challenges

Ensuring strong security measures against new and developing cyber threats and attacks is one of the main problems. IoV systems are susceptible to a range of security threats, such as data breaches, cyber-attacks, and privacy violations, as they get more networked and data intensive. It will take ongoing improvements in intrusion prevention systems, threat detection methods, and cryptographic techniques to address these issues.

B. Scalability and Compatibility

Concerns of scalability and compatibility emerge when IoV networks grow to support an increasing number of cars and devices. Maintaining network efficiency and dependability requires ensuring smooth interoperability between various hardware platforms, software applications, and communication protocols. The development of standardized protocols and architectures that provide scalable and interoperable Internet of vehicles should be the main goal of future research projects.

C. Reliability and Resilience

There are many obstacles in the way of achieving high communication dependability and resilience in dynamic vehicle situations. Degradation of communication quality and disruption of network connectivity can be caused by numerous factors, including environmental conditions, network congestion, and signal interference. To lessen the effects of unfavorable circumstances and guarantee continuous service delivery, future research should investigate fault-tolerant techniques, robust network topologies, and adaptive communication systems.

D. Regulatory Compliance and Privacy

Ensuring user privacy and adhering to legal regulations are crucial factors to consider while implementing IoV. Complying with data protection laws like the CCPA and GDPR presents ethical and legal difficulties while gathering, keeping, and using vehicle data. Subsequent investigations must focus on privacy-maintaining methods, anonymization procedures, and regulatory frameworks to guarantee conscientious data handling methods within IoV ecosystems.

E. Energy Efficiency and Sustainability

When designing and operating IoVs, energy consumption and environmental sustainability are becoming increasingly crucial factors to consider. Significant energy demands are imposed by the expansion of linked infrastructure and cars, which can put a strain on resources and increase carbon emissions. To reduce the environmental impact of IoV systems, future research should concentrate on improving energy-efficient communication protocols, power management techniques, and integration of renewable energy sources.

F. Adoption and User Acceptance

To fully realize the promise of IoV technologies, user acceptance and adoption must be encouraged. Gaining the public's trust and support requires overcoming user skepticism, addressing safety issues, and highlighting the concrete advantages of IoV solutions. To encourage favorable views toward IoV adoption, future research should prioritize user- centric design concepts, human factors engineering, and user education programs.

VIII. Conclusions

Our collaborative cryptography technique, which we have integrated with IRS to improve security and communication in the IoV environment, is given in this work. Our suggested method seeks to overcome the difficulties of safe and dependable communication in dynamic vehicular networks by utilizing modern encryption techniques like AES and incorporating IRS technology. We have outlined the main elements of our approach through the creation of an algorithmic framework and network model. These elements include the cloud server for data management, the trusted authority for key distribution, and the roles that users, cars, RSUs, and IRS play in enabling secure communication. We have covered in depth the cryptographic techniques used for secure communication, emphasizing the significance of key management and authentication in guaranteeing data integrity and secrecy. These techniques include session setup, encryption, decryption, and signature verification. In addition, we have talked about how IRS fit into the IoV architecture and how they might improve energy efficiency, lower costs, and increase communication coverage.

References

[1] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, “Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges,” IEEE Access, vol. 8, pp. 54314–54344, 2020.

[2] J. A. Fadhil and Q. I. Sarhan, “Internet of vehicles (IoV): A survey of challenges and solutions,” in 2020 21st International Arab Conference on Information Technology (ACIT), 2020.

[3] C. R. Storck and F. Duarte-Figueiredo, “A survey 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles,” IEEE Access, vol. 8, pp. 117593–117614, 2020.

[4] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, “A secure authentication protocol for internet of vehicles,” IEEE Access, vol. 7, pp. 1–1, 2019.

[5] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, “A survey on security and privacy issues in IoV,” Int. J. Electr. Comput. Eng. (IJECE), vol. 10, no. 5, p. 5409, 2020.

[6] S. A. Chaudhry, “Designing an efficient and secure message exchange protocol for Internet of vehicles,” Secur. Commun. Netw., vol. 2021, pp.1–9, 2021.

[7] H. Vasudev, V. V. Deshpande, D. Das, and S. K. Das, “A lightweight mutual authentication protocol for V2V communication in internet of vehicles,” IEEE Transaction on Vehicular Technology, vol. 69, no. 6, pp. 6709–6717, Jun. 2020.

[8] A. Hakimi, K. Mohamad Yusof, M. A. Azizan, M. A. A. Azman, and S. M. Hussain, “A Survey on Internet of Vehicle (IoV): Applications & Comparison of VANETs, IoV and SDN-IoV,” J. Elektr., vol. 20, no. 3, pp. 26–31, 2021.

[9] S. Sharma and S. Mohan, “Cloud-based secured VANET with advanced resource management and IoV applications,” in Connected Vehicles in the Internet of Things, Cham: Springer International Publishing, 2020, pp. 309–325.

[10] S. A. Elsagheer Mohamed and K. A. AlShalfan, “Intelligent Traffic Management System based on the Internet of vehicles (IoV),” J. Adv. Transp., vol. 2021, pp. 1–23, 2021.

[11] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, “Architecture, protocols, and security in IoV: Taxonomy, analysis, challenges, and solutions,” Security and Communication Networks, 2022.

[12] S. Hakak et al., “Autonomous Vehicles in 5G and beyond: A Survey,” Vehicular Communications, 2022.

[13] P. Agbaje, A. Anjum, A. Mitra, E. Oseghale, G. Bloom, and H.Olufowobi, “Survey of interoperability challenges in the internet of vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 12, pp. 22838–22861, 2022.

[14] S. Abbasi, A. M. Rahmani, A. Balador, and A. Sahafi, “Internet of Vehicles: Architecture, services, and applications,” Int. J. Commun. Syst., vol. 34, no. 10, 2021.

[15] Z. Mahmood, “Connected vehicles in the IoV: Concepts, technologies and architectures,” in Connected Vehicles in the Internet of Things, Cham: Springer International Publishing, 2020, pp. 3–18.

[16] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, “A survey of autonomous vehicles: Enabling communication technologies and challenges,” Sensors (Basel), vol. 21, no. 3, p. 706, 2021.

[17] B. Ji et al., “Survey on the internet of vehicles: Network architectures and applications,” IEEE Commun. Stand. Mag., vol. 4, no. 1, pp. 34–41,2020.

[18] E. S. Ali et al., “Machine learning technologies for secure vehicular communication in Internet of vehicles: Recent advances and applications,” Secur. Commun. Netw., vol. 2021, pp. 1–23, 2021.

[19] H. N. Noura, O. Salman, R. Couturier, and A. Chehab, “LoRCA: Lightweight round block and stream cipher algorithms for IoV systems,” Veh. Commun., vol. 34, no. 100416, p. 100416, 2022.

[20] B. Alaya and L. Sellami, “Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban vanet networks,” Journal of Information Security and Applications, vol. 58, 2021.

[21] M. A. Saleem, K. Mahmood, and S. Kumari, “Comments on ‘AKM-IoV: Authenticated key management protocol in fog computing-based internet of vehicles deployment,”' IEEE Internet Things J., vol. 7, no.5, pp. 4671–4675, 2020.

[22] A. Aljumaili, H. Trabelsi, and W. Jerbi, “A Review on Secure Authentication Protocols in IoV: Algorithms, Protocols, and Comparisons,” in 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), October 2023, pp. 1–11, IEEE.

[23] A. Eyadeh, M. Jarrah, and A. Aljumaili, “Modeling and simulation of performance limits in IEEE 802.11 point-coordination function,” International Journal of Recent Technology and Engineering, vol. 8, no. 4, pp. 5575–5580, 2019.

[24] W. Jerbi, A. Guermazi, and H. Trabelsi, “Crypto-ECC: A rapid secure protocol for large-scale wireless sensor networks deployed in internet of things,” in Theory and Applications of Dependable Computer Systems, Cham: Springer International Publishing, 2020, pp. 293–303.

[25] W. Jerbi, O. Cheikhrouhou, A. Guermazi, and H. Trabelsi, “MSU-TSCH: A Mobile Scheduling Updated Algorithm for TSCH in the Internet of Things,” IEEE Transactions on Industrial Informatics, vol. 19, no. 7, pp. 7978–7985, July 2023, doi: 10.1109/TII.2022.3215990.

[26] W. Jerbi, A. Guermazi, O. Cheikhrouhou, and H. Trabelsi, “CoopECC: A collaborative cryptographic mechanism for the internet of things,” J. Sens., vol. 2021, pp. 1–8, 2021.

[27] Q. Jiang, X. Zhang, N. Zhang, Y. Tian, X. Ma, and J. Ma, “Three-factor authentication protocol using physical unclonable function for IoV,” Computers Communication, vol. 173, pp. 45–55, May 2021.

[28] Y. Liu et al., “An access control mechanism based on risk prediction for the IoV,” in 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 2020.

[29] P. R. Babu, B. Palaniswamy, A. G. Reddy, V. Odelu, and H. S. Kim, “A survey on security challenges and protocols of electric vehicle dynamic charging system,” Secur. Priv., vol. 5, no. 3, 2022.

[30] J. Zhang, F. Yang, Z. Ma, Z. Wang, X. Liu, and J. Ma, “A decentralized location privacy-preserving spatial crowdsourcing for internet of vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 4, pp. 2299–2313,2021.

[31] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P.Ranganathan, “Cybersecurity challenges in vehicular communications,”Veh. Commun., vol. 23, no. 100214, p. 100214, 2020.

[32] S. S. Chaeikar, A. Jolfaei, and N. Mohammad, “AI-enabled cryptographic key management model for secure communications in the internet of vehicles,” IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 4, pp. 4589–4598, 2022.

[33] M. N. Aman, U. Javaid, and B. Sikdar, “A privacy-preserving and scalable authentication protocol for the internet of vehicles,” IEEE Internet Things J., vol. 8, no. 2, pp. 1123–1139, 2021.

[34] J. Li, Z. Xue, C. Li, and M. Liu, “RTED-SD: A real-time edge detection scheme for Sybil DDoS in the internet of vehicles,” IEEE Access, vol.9, pp. 11296–11305, 2021.

[35] B. K. Osibo, C. Zhang, C. Xia, G. Zhao, and Z. Jin, “Security and privacy in 5G internet of vehicles (IoV) environment,” Journal on Internet of Things, vol. 3, no. 2, 2021.

[36] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, K.-K. R. Choo, and Y. Park, “On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system,” IEEE Trans. Veh. Technol., vol. 70, no. 2, pp. 1736–1751, 2021.

[37] J. Wang, L. Wu, H. Wang, K.-K. R. Choo, L. Wang, and D. He, “A secure and efficient multiserver authentication and key agreement protocol for internet of vehicles,” IEEE Internet Things J., vol. 9, no. 23, pp. 24398–24416, 2022.

[38] S. Bojjagani, Y. C. A. P. Reddy, T. Anuradha, P. V. V. Rao, B. R. Reddy, and M. K. Khan, “Secure authentication and key management protocol for deployment of internet of vehicles (IoV) concerning intelligent transport systems,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 12, pp. 24698–24713, 2022.

[39] K. Nongthombam, S. Rana, M. S. Obaidat, D. Chhikara, and D. Mishra, “Construction of Efficient Authenticated Key Agreement Protocol for Intelligent Transportation System,” in 2022 2nd International Conference on Electronic Information Technology and Smart Agriculture (ICEITSA), IEEE, pp. 62–6, 2022.

[40] R. Hazim, N. Qasem, and A. Alamayreh, “OAM Beam Generation, Steering, and Limitations Using an Intelligent Reflecting Surface,” Progress in Electromagnetics Research M, vol. 118, 2023.

[41] W. Jerbi, O. Cheikhrouhou, A. Guermazi, M. Baz, and H. Trabelsi, “BSI: Blockchain to secure routing protocol in Internet of Things,” Concurrency and Computation: Practice and Experience, vol. 33, no.24, 2021, doi: 10.1002/cpe.6794.

[42] W. Jerbi, A. Guermazi, and H. Trabelsi, “A novel secure routing protocol of generation and management cryptographic keys for wireless sensor networks deployed in Internet of Things,” International Journal of High-Performance Computing and Networking, vol. 16, no. 2-3, pp. 87-94, January 12, 2021, doi: 10.1504/IJHPCN.2020.112693.