Securing Communication in Internet of Vehicles using Collaborative Cryptography and Intelligent Reflecting Surfaces

Ahmed Aljumaili [1*], Hafedh Trabelsi [2], Wassim Jerbi [3], Rafal Hazim [4]
[1,4] Dept. College of Engineering Technology, Al-Kitab University - Iraq, Kirkuk 36015, Iraq
[2,3] Dept. CES LAB, ISET, University of Sfax – Tunisia, Sfax, Tunisia
Email: [1] ahmedh.ali@uoalkitab.edu.iq, [2] hafedh.trabelsi@enis.tn,
[3] Wassim.jerbi@isetn.run.tn, [4] rafal.alnassir@uoalkitab.edu.iq,
*Corresponding Author

Abstract—**The Internet of Vehicles (IoV) is revolutionizing transportation systems by enabling seamless communication and collaboration among vehicles, roadside units (RSUs), and cloud servers. However, the dynamic and diverse nature of IoV environments raises significant concerns regarding security vulnerabilities and operational efficiency. In response to these challenges, this study proposes an innovative approach that integrates collaborative cryptographic techniques with intelligent reflecting surfaces (IRS). Our approach leverages advanced encryption methods, such as the Advanced Encryption Standard (AES), to ensure secure data transmission, while intelligent reflecting surfaces dynamically adjust their reflective properties to enhance signal propagation and reception. We present a comprehensive network model and algorithmic framework for implementing our proposed strategy, with a specific emphasis on cryptographic protocols and the role of intelligent reflecting surfaces in enhancing both communication security and efficiency. Through theoretical analysis and discussion, we highlight the potential advantages of integrating intelligent reflecting surfaces into secure physical layer (PL), IoV networks, including expanded network coverage, reduced communication overhead, and enhanced energy efficiency. Moreover, we address security threats and vulnerabilities in IoV environments, including potential attacks such as eavesdropping, data tampering, and denial of service. We discuss strategies for mitigating these security risks through the combined use of cryptographic techniques and intelligent reflecting surfaces, thereby bolstering the resilience and robustness of IoV systems.**

Keywords*—*Internet of Vehicles (IoV), Intelligent Reflecting Surfaces (IRS), Advanced Encryption Standard (AES), Efficiency Enhancement, Cryptographic Techniques, Security Attacks, Denial of Service (DoS), Cybersecurity

I. INTRODUCTION

The emergence of the IoV heralds a transformative era in transportation systems, leveraging cutting-edge communication technologies to revolutionize the way vehicles interact and collaborate. Unlike traditional vehicular networks, where vehicles operate in isolation, IoV facilitates seamless communication and coordination among vehicles, roadside infrastructure, and central control systems. This interconnected ecosystem enables real-time data exchange, facilitating informed decision-making and enhancing overall system efficiency.

In IoV environments, vehicles serve as mobile data hubs, continuously exchanging information with one another and with RSUs equipped with sensors and communication devices. This constant flow of data enables various applications, including traffic management, collision avoidance, and navigation assistance, to operate with unprecedented accuracy and effectiveness. Moreover, IoV systems enable proactive maintenance and fleet management, leading to reduced downtime and optimized resource allocation.

However, the pervasive connectivity and dynamic nature of IoV environments introduce new challenges, particularly in terms of communication security and privacy. With vehicles exchanging sensitive information, such as location data and driver behavior, protecting against unauthorized access, interception, and tampering becomes paramount. Additionally, ensuring privacy-preserving communication is essential to safeguarding user information and maintaining trust in IoV systems.

In this study, we propose a collaborative cryptographic approach augmented by IRS to ensure secure communication for PL in IoV environments. Our innovative strategy addresses security and performance concerns by integrating symmetric cryptographic techniques like the AES with IRS technology. Unlike conventional cryptographic systems reliant solely on encryption algorithms, our approach harnesses IRS to enhance security, communication reliability, coverage, and energy efficiency.

Our study's key contributions lie in the development of a novel cryptographic technique tailored for IoV scenarios and the integration of IRS to augment communication capabilities and security. Through comprehensive simulations and analysis, we validate the efficacy of our strategy in mitigating security risks and improving communication performance within IoV environments.

The precise organization of the paper's structure allows for a thorough investigation of security and communication inside the IoV ecosystem. To set the stage for the next topics, Section 2 provides a thorough summary of recent research on IoV security and communication protocols. The network model and computational framework used in our suggested method are described in Section 3, which also provides the technical background for our study. Section 4 delves into the topic of cybersecurity and describes the cryptographic techniques that are used to guarantee safe communication in Internet of Vehicles environments.Section 5 delves deeply into the integration of IRS and how they improve communication in IoV systems. Taking on difficulties head-on, Section 6 explores roadblocks and suggests possible directions for additional study and advancement. IoV algorithm-specific cybersecurity attacks are analyzed in Section 7, with a focus on vulnerabilities and suggested defenses. In Section 8, the report wraps up by providing an overview of the main conclusions and suggesting future research avenues to further the development of IoV technology.

II. Related Work

The paper offers a thorough examination of authentication protocols within the IoV domain, as demonstrated by Bagga et al. [1]. It explores the taxonomy, analysis, and challenges surrounding these protocols, providing valuable insights into the security landscape of IoV systems.

Furthermore, Fadhil and Sarhan [2] address the challenges and solutions within the IoV environment. Their survey identifies various hurdles within the IoV ecosystem and proposes potential solutions, contributing to a deeper understanding of the field.

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

Additionally, Chen et al. [4] introduce a secure authentication protocol tailored for IoV, focusing on maintaining 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 explores 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 tailored for IoV environments. This protocol prioritizes both efficiency and security, aiming to facilitate seamless communication among vehicles while ensuring the confidentiality and integrity of exchanged messages. By enhancing the overall reliability of IoV systems, Chaudhry's protocol contributes to the advancement of vehicular communication networks.

Vasudev et al. [7] introduce a lightweight mutual authentication protocol designed for vehicle-to-vehicle (V2V) communication within IoV frameworks. Emphasizing mutual authentication's importance in establishing trust among communicating vehicles, their protocol fosters a secure and resilient IoV ecosystem capable of withstanding various security threats and attacks.

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

Sharma and Mohan [9] investigate a cloud-based secured VANET with advanced resource management and IoV applications. Their research explores integrating cloud computing technologies to enhance VANET security and efficiency, particularly within IoV contexts. Leveraging cloud resources, their approach aims to improve VANET scalability, reliability, and performance in supporting various IoV services.

Elsagheer Mohamed and AlShalfan [10] propose an Intelligent Traffic Management System based on IoV principles. Focusing on leveraging IoV technology to develop intelligent traffic management systems, their work aims to enhance safety, reduce congestion, and optimize resource utilization in urban transportation networks.

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

Hakak et al. [12] offer a survey on autonomous vehicles (AVs) within the framework of 5G and beyond. Their study delves into the integration of AVs with advanced communication technologies, particularly focusing on the potential of 5G networks and beyond to support various autonomous driving applications. By assessing the current state of AV technology and its evolution alongside communication infrastructures, the authors provide valuable insights into the opportunities and challenges associated with deploying AVs in future transportation systems.

Agbaje et al. [13] conduct a survey on interoperability challenges within the IoV. Their research identifies and examines 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 underlying 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 enabling 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 understanding the technological landscape shaping the future of autonomous transportation.

Ji et al. [17] conduct 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] investigate the application of machine learning technologies to enhance the security of vehicular communication within the IoV. Their study explores recent advancements and applications of machine learning algorithms in detecting and mitigating security threats in connected vehicle environments. By analyzing the role of machine learning in IoV security, the authors provide valuable insights into leveraging these technologies to address cybersecurity challenges effectively.

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

Alaya and Sellami [20] present a clustering method and symmetric/asymmetric cryptography scheme customized for securing urban VANETs. Their work focuses on enhancing VANET security in urban settings by leveraging clustering techniques and cryptographic mechanisms. Through their approach, the authors aim to mitigate security threats and improve VANET resilience against malicious attacks.

Saleem et al. [21] offer insights on the Authenticated Key Management (AKM-IoV) protocol proposed for fog computing-based IoV deployments. Their commentary critically evaluates the design and implementation of the AKM-IoV protocol, highlighting its strengths and limitations. By contributing to the discourse on secure key management protocols for IoV environments, the authors provide valuable suggestions for protocol improvement and future research directions.

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

Jerbi et al. [24], [25] introduce Crypto-ECC, a rapid secure protocol tailored 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 IoT security by proposing a cryptographic protocol adapted to the resource constraints of wireless sensor networks. Leveraging elliptic curve cryptography (ECC), Crypto-ECC aims to provide efficient security solutions for IoT applications.

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

Jiang et al. [27] encompasses various authentication protocols and security mechanisms designed specifically for the IoV domain. Several research endeavors have focused on enhancing authentication methods and security measures to address the unique challenges posed by IoV environments.

Liu et al. [28] propose an access control mechanism based on risk prediction for the IoV. Their work focuses on managing access to IoV resources by predicting and mitigating security risks. By incorporating risk prediction techniques, the proposed mechanism aims to enhance security in IoV environments, contributing to effective access control strategies.

Babu et al. [29] conduct a survey on security challenges and protocols of electric vehicle dynamic charging systems. Their research explores the security aspects of dynamic charging systems for electric vehicles (EVs), addressing vulnerabilities and proposing protocols to mitigate potential threats. By examining security challenges specific to EV charging infrastructure, the authors contribute to the development of secure charging solutions in the IoV ecosystem.

Zhang et al. [30] propose a decentralized location privacy-preserving spatial crowdsourcing mechanism for the IoV. Their work focuses on preserving the location privacy of vehicles participating in spatial crowdsourcing tasks while ensuring the reliability and efficiency of data collection. By leveraging decentralized approaches, the proposed mechanism aims to protect the privacy of vehicle locations in IoV environments, contributing to enhanced privacy preservation strategies.

El-Rewini et al. [31] discuss cybersecurity challenges in vehicular communications. Their work examines the vulnerabilities and threats faced by vehicular communication systems and proposes strategies to address cybersecurity concerns. By identifying and analyzing cybersecurity challenges, the authors contribute to enhancing the security posture of vehicular communication networks.

Chaeikar et al. [32] propose an AI-enabled cryptographic key management model for secure communications in the IoV. Their research focuses on leveraging artificial intelligence (AI) techniques to enhance cryptographic key management processes in IoV environments, thereby strengthening the security of vehicular communication systems.

Aman et al. [33] present a privacy-preserving and scalable authentication protocol for the IoV. Their work addresses the privacy concerns associated with authentication processes in IoV systems by proposing a protocol that ensures privacy protection while maintaining scalability and efficiency. By incorporating privacy-preserving mechanisms, the protocol enhances the privacy of IoV users without compromising security.

Li et al. [34] propose RTED-SD, a real-time edge detection scheme for Sybil Distributed Denial of Service (DDoS) attacks on the IoV. Their research focuses on detecting and mitigating DDoS attacks targeting IoV systems by leveraging real-time edge detection techniques. By enhancing the resilience of IoV systems against DDoS attacks, the proposed scheme contributes to improving the overall security of vehicular communication networks.

Osibo et al. [35] discuss security and privacy issues in 5G IoV environments. Their research explores the unique security and privacy challenges posed by the integration of 5G technology into IoV systems, aiming to identify potential threats and vulnerabilities and propose solutions to mitigate them.

Bagga et al. [36] propose a mutual authentication and key agreement protocol for IoV-enabled Intelligent Transportation Systems (ITS). Their work focuses on designing a secure protocol that facilitates mutual authentication between vehicles and infrastructure elements in IoV-enabled ITS environments, ensuring the integrity and confidentiality of communication.

Wang et al. [37] present a secure and efficient multiserver authentication and key agreement protocol for the IoV. Their research aims to design a protocol that enables efficient authentication and key agreement between vehicles and multiple servers in IoV environments, enhancing the security and scalability of vehicular communication systems.

Bojjagani et al. [38] propose a secure authentication and key management protocol for the deployment of IoV in ITS. Their work focuses on developing a protocol that addresses the security and key management challenges associated with deploying IoV in ITS, ensuring secure and reliable communication among vehicles and infrastructure elements.

Nongthombam et al. [39] discuss the construction of an efficient authenticated key agreement protocol for ITS. Their research focuses on designing a protocol tailored to the specific requirements of ITS environments, considering factors such as efficiency, security, and scalability. By developing an efficient authenticated key agreement protocol, the authors aim to enhance the security and reliability of vehicular communication systems in ITS deployments.

Hazim et al. [40] investigate Orbital Angular Momentum (OAM) beam generation, steering, and limitations using an IRS. Their research, published in Progress in Electromagnetics Research M, explores the application of IRS technology to manipulate electromagnetic waves for beamforming, offering insights into the potential of IRS for enhancing wireless communication systems.

Jerbi et al. [41] propose BSI (Blockchain to secure routing protocol in Internet of Things) in their paper published in Concurrency and Computation: Practice and Experience. The BSI protocol aims to enhance the security of routing protocols in the IoT by leveraging blockchain technology. By providing a secure and tamper-proof mechanism for routing protocol operations, BSI contributes to improving the resilience of IoT networks against various cyber threats.

Jerbi et al. [42]introduce a novel secure routing protocol for the generation and management of cryptographic keys in wireless sensor networks deployed in the IoT. Their work, published in the International Journal of High Performance Computing and Networking, presents a protocol design optimized for the resource-constrained environment of IoT deployments. By ensuring the secure establishment and management of cryptographic keys, their protocol enhances the security posture of IoT deployments, particularly in wireless sensor network applications.

The work by Naeem et al. [43] provides a comprehensive review of security and privacy considerations for reconfigurable intelligent surfaces (RIS) in 6G networks. The authors discuss prospective applications and challenges associated with RIS deployment, offering valuable insights into the evolving landscape of wireless communication security.

Kavaiya and Patel [44] address the issue of passive attacks in 6G vehicular networks from a physical layer security perspective in their study published in *Wireless Networks*. Their work sheds light on strategies to mitigate passive attacks in the context of emerging 6G network environments.

III. Background

In this section, we delve into the evolution and significance of the IoV, highlighting the key challenges faced in ensuring communication security and privacy. We also explore the role of collaborative cryptography and IRS in addressing these challenges, laying the groundwork for the proposed strategy.

A. Evolution and Significance of the Internet of Vehicles

The IoV represents a transformative shift in transportation systems, leveraging advanced communication technologies to enhance safety, efficiency, and convenience. Traditionally, vehicles operated independently with limited communication capabilities. However, the advent of IoV technology has facilitated seamless communication between vehicles, roadside infrastructure, and central control systems [45]–[47].

The evolution of IoV can be attributed to advancements in wireless communication, sensor technology, and cloud computing. These developments have enabled real-time data exchange, enabling applications such as intelligent traffic management, predictive maintenance, and autonomous driving. Consequently, IoV has the potential to revolutionize transportation systems by improving road safety, reducing traffic congestion, and minimizing environmental impact [48], [49].

B. Key Challenges in Ensuring Communication Security and Privacy

Despite its numerous benefits, IoV faces significant challenges in ensuring communication security and privacy. The dynamic and interconnected nature of IoV environments makes them susceptible to various security threats, including cyberattacks, data breaches, and privacy violations [50].

1) Cybersecurity Threats: One of the primary challenges is safeguarding the confidentiality, integrity, and availability of data exchanged within IoV networks. Malicious actors may attempt to intercept communication channels, manipulate transmitted data, or disrupt network operations, posing serious security risks [51].

2) Privacy Concerns: Furthermore, IoV raises concerns about privacy infringement, as sensitive information such as location data and personal identifiers is shared among vehicles and infrastructure. Unauthorized access to this information can lead to privacy breaches, identity theft, and unauthorized surveillance, undermining user trust and confidence in IoV systems [52].

C. Role of Collaborative Cryptography and Intelligent Reflecting Surfaces in Addressing IoV Challenges

To address the security and privacy challenges in IoV systems, innovative approaches such as collaborative cryptography and IRS have emerged as promising solutions [53].

1) Collaborative Cryptography: Collaborative cryptography harnesses the collective computational power of multiple entities to enhance security and resilience against cyber threats. By distributing cryptographic tasks across multiple nodes and leveraging consensus mechanisms, collaborative cryptography can mitigate single points of failure and improve the overall security posture of IoV networks [54].

2) Intelligent Reflecting Surfaces: IRS offer a unique solution for improving communication reliability and efficiency in IoV environments. By dynamically adjusting the reflection properties of surfaces, IRS can enhance signal propagation, extend coverage, and mitigate interference, thereby improving overall network performance [55].

IV. Security Attacks in Internet of Vehicles

A. Overview of Security Threats

The IoV ecosystem is susceptible to various security threats and attacks that can compromise the integrity, confidentiality, and availability of communication networks. These threats pose significant risks to the safety, privacy, and reliability of IoV systems, necessitating a comprehensive understanding and mitigation strategy [56].

B. Types of Security Attacks

In IoV environments, attackers exploit vulnerabilities in communication protocols, hardware components, and software systems to launch various types of security attacks:

- **DoS Attacks:** Attackers flood network resources or services with malicious traffic, rendering them unavailable to legitimate users. DoS attacks disrupt IoV communication channels, leading to service degradation or complete downtime [57].

- **Man-in-the-Middle (MitM) Attacks:** Attackers intercept and modify communication between vehicles or between vehicles and infrastructure elements. MitM attacks enable attackers to eavesdrop on sensitive data, inject malicious content, or impersonate legitimate entities [58].
- **Sybil Attacks:** Attackers create multiple fake identities or nodes to manipulate network behavior and disrupt communication. Sybil attacks compromise the integrity of IoV systems by generating false information, distorting network topology, or overwhelming network resources [59].
- **Eavesdropping and Sniffing Attacks:** Attackers passively monitor wireless communication channels to intercept and capture sensitive information exchanged between vehicles or between vehicles and roadside units. Eavesdropping attacks compromise the confidentiality of data transmitted over IoV networks [60].
- **Spoofing and Impersonation Attacks:** Attackers forge or spoof network identities to impersonate legitimate vehicles or infrastructure elements. Spoofing attacks deceive IoV systems into accepting false messages or commands, leading to unauthorized access or control [61].
- **Tampering and Modification Attacks:** Attackers alter or tamper with data packets, control messages, or sensor readings transmitted over IoV networks. Tampering attacks manipulate the integrity of data, leading to false readings, inaccurate navigation, or unsafe driving conditions [62].

C. Case Studies of Security Breaches

Several real-world incidents highlight the severity and impact of security breaches in IoV systems [63]–[65]:

- **Tesla Model S Hacking Incident:** In 2016, researchers remotely hacked into a Tesla Model S vehicle's infotainment system, demonstrating the vulnerability of connected vehicles to remote attacks.
- **Jeep Cherokee Remote Control Attack:** In 2015, security researchers remotely hijacked a Jeep Cherokee's control systems, demonstrating the potential for attackers to take over vehicle functions such as steering and braking.
- **University of Michigan IoV Experiment:** Researchers at the University of Michigan conducted a large-scale experiment in 2018, revealing vulnerabilities in connected vehicle systems that could be exploited by malicious actors to disrupt traffic flow or cause accidents.

D. Vulnerable Components and Attack Surfaces

IoV systems are vulnerable to various components and attack surfaces, which can be exploited by malicious actors to compromise the integrity and security of the system. Some of the key vulnerable components and attack surfaces in IoV systems include:

- **Insecure Communication Channels:** IoV systems rely on communication channels for exchanging data between vehicles, infrastructure, and backend servers. If these channels are not properly secured, they can be susceptible to interception, eavesdropping, and tampering by unauthorized entities [66].
- **Weak Authentication and Access Control Mechanisms:** Inadequate authentication and access control mechanisms can allow unauthorized users to gain access to sensitive resources and functionalities within IoV systems. Weak passwords, lack of multi-factor authentication, and improper user authorization can lead to unauthorized access and misuse of system resources [67].
- **Unprotected Data Transmission and Storage:** Data transmitted and stored within IoV systems may be vulnerable to interception, manipulation, or theft if proper encryption and data protection mechanisms are not implemented. Unencrypted data packets and storage vulnerabilities can expose sensitive information to unauthorized access and exploitation.
- **Lack of Encryption and Integrity Verification:** Without robust encryption and integrity verification mechanisms, data integrity and confidentiality within IoV systems can be compromised. Attackers may tamper with data packets, inject malicious content, or impersonate legitimate entities, leading to data corruption and unauthorized system access [68].
- **Exploitable Hardware and Software Vulnerabilities:** Vulnerabilities in hardware components and software systems used in IoV devices and infrastructure can be exploited by attackers to gain unauthorized access, execute malicious code, or disrupt system operations. Unpatched software vulnerabilities, insecure firmware, and hardware backdoors pose significant risks to the security of IoV systems.

E. Impact of Security Attacks

Security attacks targeting IoV systems can have severe consequences, impacting various aspects of system functionality, safety, and privacy. Some of the potential impacts of security attacks in IoV systems include:

- **Disruption of Communication and Service Availability:** DoS attacks or network congestion caused by malicious activities can disrupt communication channels and render essential services unavailable to users, leading to service outages and operational disruptions.
- **Compromise of Vehicle Safety and Control Systems:** Attacks targeting vehicle control systems or safety-critical components can compromise the safety and integrity of vehicles, leading to accidents, collisions, or loss of vehicle control. Malicious actors may tamper with braking

systems, steering mechanisms, or engine controls, endangering the lives of passengers and pedestrians.
- **Breach of User Privacy and Sensitive Data Exposure:** Unauthorized access to sensitive user data, such as location information, personal identifiers, or biometric data, can result in privacy violations and identity theft. Breaches of user privacy may also lead to stalking, surveillance, or targeted attacks against individuals or organizations.
- **Financial Losses and Reputational Damage:** Security breaches and data breaches in IoV systems can result in financial losses, legal liabilities, and reputational damage for businesses, manufacturers, and service providers. The costs associated with data breaches, regulatory fines, and litigation can have long-lasting repercussions for affected organizations and individuals.

V. Proposed Architecture for IoV

The architecture of the Internet of Vehicles is a complex, multi-layered system. The vehicle, network, RSU, infrastructure, Cloud Server (CS), trusted authority (TA), data analytics, apps, and security are the fundamental components of an IoV architecture, as shown in Fig. 1. The main component of the IoV architecture is the vehicle itself. Vehicles can communicate with each other and the environment thanks to smart sensors and other smart devices [27]–[29].

Dedicated Short Range Communications (DSRC) protocols, Wi-Fi networks, and cellular networks are a few of the communication technologies that enable network-layer access between automobiles and the Internet. The Internet of Vehicles uses the cloud layer for data processing and storage. CS can aggregate and evaluate several vehicle data points to deliver real-time insights about various issues such as road conditions and traffic patterns. The Internet of Vehicles generates enormous volumes of data, which are processed by the data analytics layer [30].

VI. 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.

A. Network Model

Several important entities make up our network model [31], [32]:

- **TA**: In charge of transferring keys safely between entities that communicate with one other.
- **CS**: Maintains and stores information transferred between entities.
- **Users (U)** : End-users interacting with IoV services.
- Vehicles are modeled as mobile nodes that are outfitted with communication gear.
- RSUs: These are fixed infrastructure units placed beside roads to help with vehicle communication.
- **IRS**: Designed to be intelligent surfaces that may modify their reflection characteristics dynamically to improve communication between automobiles and RSUs.

B. Algorithmic Framework

The Algorithmic 1 provides a structured approach to cryptographic mechanism and session establishment protocol implementation in the context of the IoVs. This facilitates the integration of IRS for enhanced network performance and permits secure communication between entities [33], [34].

C. Algorithm Explanation

The algorithmic framework provided can be broken down into several key steps:

1) Initialization:

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

2) Session Establishment:

- Exchange nonces (random values) between communicating entities.
- Compute session keys using the AES-Key-Derivation algorithm.

3) Nominal Scenario:

- Generate a random nonce for each message transmission.
- Compute the session key using AES-Key-Derivation.
- Encrypt the message using AES-GCM encryption algorithm to ensure confidentiality.
- Sign the message with the sender's private key to ensure authenticity.
- Include the signature in the message header.
- Transmit the encrypted and authenticated message.
- On the receiving end, verify the signature using the sender's public key.
- Derive the session key.
- Decrypt the message.

4) Alternative Scenario (Key Update):

- When a key update is required, generate new nonces N'_A and N'_B.
- Compute the updated session key K'_{session} using AES-Key-Derivation.
- Use the updated session key for encryption and authentication.

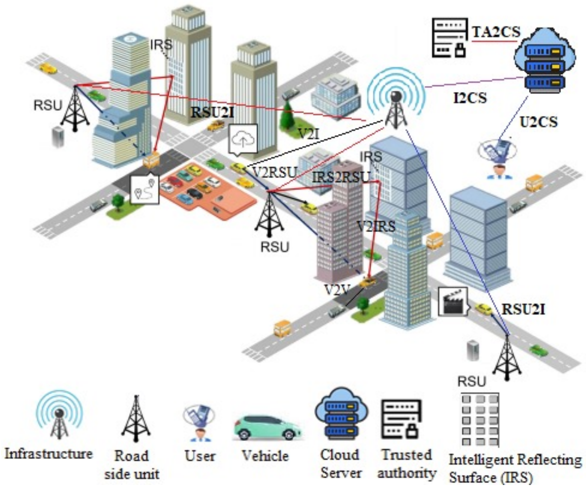

Fig. 1. A IoV system in a smart city environment

5) Error Scenarios:

- If the signature verification fails, discard the message and log the incident.
- If the decryption fails, consider the message as corrupted or malicious and log the incident.
- If the nonce is not valid (e.g., repeated or out of sequence), reject the message and log the incident.
- If the key exchange process fails, terminate the communication and log the incident.
- If the integration of IRS fails, fallback to traditional communication or terminate the connection.

6) IRS Integration:

- Implement IRS functionality for secure communication.
- Ensure security at the physical layer of high mobility of vehicles.
- Evaluate the impact of IRS on network coverage, cost reduction, and energy efficiency.

VII. Integration of IRS in IoV Communication

IRS represent a groundbreaking technology poised to revolutionize 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, the aim is 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 holds the promise of extending network coverage to previously inaccessible areas and opens avenues for optimizing spectrum utilization and reducing energy consumption in IoV deployments [38].

Seamless information flow and data interchange are essential to V2X connections. The expanding connection of the ground-based vehicular network renders it an open system and creates new PL security concerns that have the potential to disrupt the network, endanger the safety of workers in vehicles, and leak critical data [69].

Each vehicle user in a congested city or suburb is surrounded by a collection of scatters, which significantly affects the LoS propagation and may even cause signal disruption. Multiple BS deployments cost a lot of money and demand a lot of room. If the LoS channel is blocked between the sender and the receiver in a standard V2X communication scenario, the third vehicle user might be selected as the relay [70].

However, this increases the possibility of information leaking for some very private data. Ensuring security at the physical layer is more difficult due to the high mobility of vehicles. Improving the security of vehicular communications in an economical and energy-efficient manner is crucial. IRS is a potential technique in the context of smart radio that offers a fresh approach to improving the secrecy rate in automotive networks. IRS may selectively boost or suppress undesired signals by adaptively varying the phase shift of the reflecting elements. This allows IRS to regulate the reflected signal and add either constructively or destructively to the non-IRS reflected signal at the receiver [71].

Rather than employing another vehicle user as a relay, IRS reflection can be used to build a new desirable propagation path between sender and receiver [71]. Network security is significantly impacted by the problem of eavesdropping. The method for canceling the signal that was leaked to the eavesdropper in IRS-assisted mobile networks is examined in [72]. Both the eavesdropper and the authorized users of the car can receive the signal from RSU when they are in proximity to each other. Additionally, IRS has the ability to simultaneously increase the received strength at the authorized user and suppress the signal by reflecting an in-phase signal to the eavesdropper that is out

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.
IRS Integration:
    1. Implement IRS functionality for secure communication.
    2. Evaluate the impact of IRS on network coverage, cost reduction, and energy efficiency.
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 $K'_{\text{session}} = \text{AES-Key-Derivation}(N'_A, N'_B, \text{SharedSecret})$.
    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.
```

of phase with the signal it is eavesdropping on.

Fig. 2 illustrates how ground-based vehicle networks can utilize this IRS capability. The IRS-reflected out-of-phase signal can negate the secret information received at the eavesdropper car without incurring additional costs at the legal vehicle side. The use of IRS in the security of ground-based vehicle networks is examined in [72], [74]. The findings confirm that IRS has the ability to improve security in V2V and V2I communications, and that the position and number of reflecting elements of IRS affect the security of the PL.

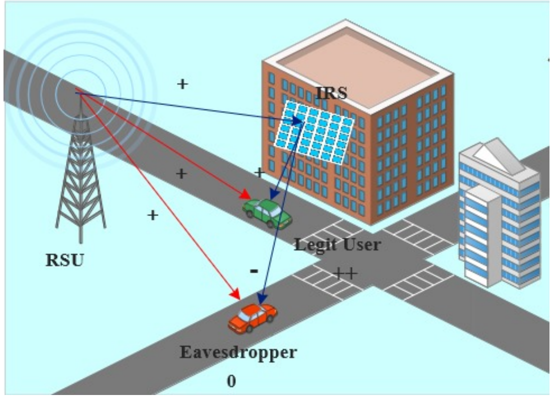

Fig. 2. IRS enhances PL security in V2X communications

A. Advanced Techniques Leveraged by IRS

Leveraging advanced beamforming 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. This subsection explores the technical intricacies behind IRS functionality and their potential to enhance communication reliability in IoV environments.

B. Deployment Considerations and Optimization

The deployment of IRS necessitates careful consideration of factors such as placement optimization, beamforming algorithms, and coordination mechanisms to maximize their efficacy in real-world scenarios. This subsection discusses the challenges and considerations involved in deploying IRS effectively within IoV infrastructure.

C. Enhancing Security with IRS

In light of 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. This subsection explores how IRS, equipped with reconfigurable reflective elements, can dynamically manipulate the propagation environment of wireless signals to fortify the security posture of IoV ecosystems.

D. Cybersecurity Resilience and Threat Mitigation

Through the integration of advanced signal processing algorithms and anomaly detection techniques, IRS can actively monitor and mitigate potential cyber threats, augmenting the overall cybersecurity resilience of IoV deployments. This subsection delves into 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].

VIII. Cryptographic 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 plays a vital role in securing communication within the IoV, with the AES being a cornerstone cryptographic algorithm. AES offers robust protection by encrypting message payloads using keys of lengths such as 128 bits, 192 bits, or 256 bits. It operates on fixed block sizes, ensuring confidentiality during transmission [42].

The encryption process using AES can be represented as:

$$C = E_K(P)$$

Where C is the ciphertext, E_K is the encryption function with key K, and P is the plaintext.

B. AES-GCM Mode

Authenticated encryption is essential for ensuring both integrity and confidentiality in communication. AES in Galois/Counter Mode (AES-GCM) provides this capability by combining the authentication strength of Galois/Counter Mode with the encryption prowess of AES. This ensures that not only is the communication encrypted, but its legitimacy is also confirmed upon decryption.

The encryption and authentication process using AES-GCM can be represented as:

$$(C, T) = \text{AES-GCM}_{\text{Enc}}(K, IV, P, A)$$

Where C is the ciphertext, T is the authentication tag, K is the encryption key, IV is the initialization vector, P is the plaintext, and A is the additional authenticated data.

C. Key Exchange Mechanisms

Establishing shared secret keys between communicating entities is crucial for secure communication. Secure key exchange protocols like the Diffie-Hellman key exchange algorithm facilitate this process. Once session keys are securely negotiated, message payloads are symmetrically encrypted and decrypted using these keys.

The key exchange process using Diffie-Hellman algorithm can be represented as:

$$K = g^{ab} \mod p$$

Where K is the shared secret key, g is the generator, a is the private key of the sender, b is the private key of the receiver, and p is a large prime number.

D. Digital Signatures

Digital signatures play a crucial role in ensuring the authenticity and non-repudiation of messages within the IoV. Sender entities sign their communications using their private keys, and recipient entities validate these signatures using the sender's public keys. This guarantees the legitimacy and authenticity of message exchanges within the IoV network.

The digital signature process using public-key cryptography can be represented as:

$$\text{Signature} = \text{Sign}(K_{\text{priv}}, M)$$

Where Signature is the digital signature, K_{priv} is the private key, and M is the message.

E. Secure Hash Functions

Secure hash functions like SHA-256 are utilized to create fingerprints and message digests within the IoV. These digests are transmitted alongside messages and are used at the recipient's end to confirm the integrity of message payloads. Any tampering with the message can be detected by comparing the computed digest with the transmitted digest.

The hash function process using SHA-256 can be represented as:

$$H = \text{SHA-256}(M)$$

Where H is the message digest and M is the message.

IX. Integration of IRS

This section explores the integration of IRS in communication systems, both passive and active approaches play significant roles. Passive IRS, consisting of passive elements such as meta-surfaces or reconfigurable meta-materials, manipulate the reflection, absorption, and transmission properties of incident electromagnetic waves without requiring external power sources. On the other hand, active IRS incorporates active elements, such as transistors or diodes, enabling dynamic control over the reflected signals.

The passive IRS can be more energy-efficient and cost-effective for static environments, whereas active IRS offers greater adaptability and flexibility in dynamic scenarios. Both passive and active IRS contribute to enhancing communication system performance by mitigating path loss, improving coverage, and optimizing signal propagation in various propagation environments.

A. Passive Intelligent Reflecting Surfaces

Passive IRS are composed of meta-surfaces or reconfigurable meta-materials that manipulate incident electromagnetic waves without requiring external power sources. The reflection coefficient (Γ) of a passive IRS can be expressed as:

$$\Gamma = \frac{Z_{\text{load}} - Z_0}{Z_{\text{load}} + Z_0} \tag{1}$$

where Z_{load} is the load impedance seen by the IRS and Z_0 is the characteristic impedance of the transmission line.

B. Active Intelligent Reflecting Surfaces

Active IRS utilize active components to dynamically control the reflection properties, allowing for adaptive signal manipulation and optimization. These surfaces typically employ elements such as varactor diodes, phase shifters, or other tunable components to adjust the phase and amplitude of the reflected waves.

1) Varactor Diode-Based Active IRS: Varactor diodes are commonly used in active IRS due to their voltage-controlled capacitance, enabling dynamic phase modulation. The reflection coefficient of an active IRS employing varactor diodes can be controlled by varying the bias voltage applied to the diodes. The phase shift introduced by a varactor diode-based active IRS can be expressed as:

$$\theta = 2\pi \frac{\Delta C}{C_{\text{max}}} \tag{2}$$

where ΔC is the change in capacitance induced by the applied bias voltage, and C_{max} is the maximum capacitance of the varactor diode.

2) Phase Shifter-Based Active IRS: Phase shifter-based active IRS utilize electronic components capable of introducing a controllable phase shift to the incident waves. These phase shifters can be implemented using various techniques such as switched-line phase shifters, digital phase shifters, or electronically tunable microwave components. The phase shift introduced by a phase shifter-based active IRS depends on the design and configuration of the phase shifting elements.

3) Tunable Resonator-Based Active IRS: Tunable resonator-based active IRS employ resonant structures with tunable parameters to control the reflection properties. These structures can include tunable metamaterial resonators, frequency-selective surfaces (FSS), or other reconfigurable structures capable of altering their resonant behavior in response to external stimuli. The reflection characteristics of a tunable resonator-based active IRS are determined by the resonance frequency and the tuning mechanism of the resonant elements.

C. Hybrid Intelligent Reflecting Surfaces

Hybrid Intelligent Reflecting Surfaces combine both passive and active elements to leverage the advantages of each approach. By integrating passive and active elements in the same surface, hybrid IRS can achieve dynamic control over the reflected signals while maintaining energy efficiency and cost-effectiveness. The overall reflection coefficient of a hybrid IRS depends on the combination of passive and active elements and their respective control mechanisms.

X. Cybersecurity Attacks in IoV algorithms

Cybersecurity attacks pose significant threats to IoV systems, necessitating robust protective measures. Here, we address various attack scenarios and propose protection measures to mitigate their impact.

A. Signature Verification Failure

Signature verification failure can lead to the acceptance of forged messages, compromising the integrity of IoV communications.

Algorithm 2 Signature Verification Failure

```
1) Receive the message $C$ with signature $\sigma$.
2) Verify the signature using the sender's public key.
3) If verification fails, discard the message and log the incident.
```

Protection Measures:

1) Ensure the validity of the sender's public key through a secure key distribution mechanism.
2) Implement regular key updates and rotations to mitigate the impact of compromised keys.
3) Use additional measures such as digital certificates for key authentication.

The ”Signature Verification Failure” algorithm handles the situation in which there is a failure to validate the signature of a message received, pointing to possible security risks in Internet of Vehicles connection. It entails getting the message and signature, confirming the signature with the sender's public key, tossing the message in the event that the verification is unsuccessful, and recording the occurrence for further examination. Using extra precautions like digital certificates for key authentication, implementing frequent key updates to minimize compromised keys, and verifying the validity of the sender's public key through secure key distribution are examples of protection methods. By strengthening the validity and integrity of IoV communication, these precautions lessen the possibility of illegal access or message tampering.

B. Decryption Failure

Decryption failure can occur due to various reasons, including tampering or errors in transmission.

Algorithm 3 Decryption Failure

1) Receive the encrypted message C.
2) Attempt to decrypt the message using the session key K_{session}.
3) If decryption fails, consider the message as corrupted or malicious and log the incident.

Protection Measures:

1) Implement robust encryption and decryption mechanisms.
2) Use authenticated encryption algorithms to detect tampering during decryption.
3) Regularly update encryption algorithms and key sizes to adapt to evolving security standards.

When an encrypted message cannot be decrypted, there may be security risks in IoV communication. This is addressed by the ”Decryption Failure” technique. The process entails getting the encrypted message, trying to decode it with the session key, and recording the occurrence in case decryption is unsuccessful. Strong encryption and decryption techniques, the use of verified encryption algorithms to spot manipulation during decryption, and routine updates to encryption algorithms and key sizes to keep up with changing security standards are some examples of protection measures. By preventing unwanted access and data tampering, these steps improve the confidentiality and integrity of IoV communication.

C. Invalid Nonce

Invalid nonce poses a risk of replay attacks, where adversaries can reuse intercepted messages.

Algorithm 4 Invalid Nonce

1) Receive the message C with nonce N.
2) Check the validity of the nonce.
3) If the nonce is invalid, reject the message and log the incident.

Protection Measures:

1) Implement nonce management to ensure nonces are unique and within an acceptable range.
2) Use timestamps or sequence numbers to prevent replay attacks.
3) Employ session timeouts and rekeying mechanisms to limit the impact of compromised nonces.

The ”Invalid Nonce” algorithm deals with scenarios where an invalid nonce is encountered during message reception in IoV communication, indicating potential security threats such as replay attacks. It involves receiving the message with a nonce, checking its validity, and rejecting the message if the nonce is invalid, with incident logging. Protection measures include implementing nonce management to ensure uniqueness and validity, using timestamps or sequence numbers to prevent replay attacks, and employing session timeouts and rekeying mechanisms to mitigate the impact of compromised nonces. These measures bolster the integrity and authenticity of IoV communication, safeguarding against unauthorized message replay and ensuring secure data transmission.

D. Key Exchange Failure

Key exchange failure can disrupt secure communication channels between IoV entities.

Algorithm 5 Key Exchange Failure

1) During key exchange between entities A and B, check for successful completion.
2) If the key exchange process fails, terminate the communication and log the incident.

Protection Measures:

1) Use robust key exchange protocols with error detection and correction mechanisms.
2) Implement a secure fallback mechanism for key exchange failures.
3) Regularly review and update key exchange protocols based on emerging cryptographic standards.

In instances where the key exchange procedure between entities in IoV communication fails, the establishment of secure communication channels may be compromised. This is addressed by the ”Key Exchange Failure” algorithm. It entails keeping an eye on the key exchange procedure, stopping communication if it breaks down, and then recording the incident. Strong key exchange protocols with error detection and correction features, safe fallback procedures to handle key exchange failures, and routine reviews and updates of key exchange protocols to keep them in line with new cryptographic standards are some examples of protection measures. By ensuring the robustness and dependability of critical exchange procedures, these steps seek to improve the overall security of the IoVs' communication infrastructure.

E. IRS Integration Failure

Integration failure of IRS can critically impact the reliability and performance of IoV communications, particularly in scenarios where active IRS or physical layer components are involved.

Algorithm 6 IRS Integration Failure

```
1) Verify the successful integration of the IRS, ensuring
   compatibility with active or physical layer components
   if applicable.
2) If IRS integration fails, revert to traditional communication
   methods or terminate the connection, depending on
   the severity of the failure and system requirements.
Protection Measures:
1) Conduct comprehensive testing and validation of IRS integration,
   considering the specific requirements for active
   IRS or physical layer configurations.
2) Implement redundant communication channels to facilitate
   seamless fallback options in the event of IRS integration
   failure, ensuring uninterrupted connectivity.
```

The ”IRS Integration Failure” algorithm addresses potential challenges arising from the unsuccessful integration of IRS in IoV communication systems, particularly when incorporating active IRS for PL components. It emphasizes the importance of verifying successful integration and compatibility with active or PL technologies, followed by appropriate actions to mitigate the impact of integration failures. Protection measures focus on rigorous testing and validation procedures tailored to the specific requirements of active IRS for PL configurations, alongside the implementation of redundant communication channels to ensure continuity of communication services. By adhering to these protocols, the resilience and effectiveness of IRS integration within IoV environments can be enhanced, thereby fostering robust and dependable communication networks.

XI. Challenges and Prospects for Future Research

Despite the potential of combining IRS with cryptographic techniques to enhance security and communication in the IoV, several challenges remain, and there are promising avenues for future investigation.

A. Scalability and Interoperability

As IoV networks expand to accommodate a growing number of vehicles and devices, concerns about scalability and interoperability arise. Maintaining efficient and reliable network operations necessitates seamless compatibility across diverse hardware platforms, software applications, and communication protocols. Future research endeavors should prioritize the development of standardized protocols and architectures that promote scalability and interoperability in IoV ecosystems.

B. Reliability and Robustness

Achieving high levels of communication reliability and resilience in dynamic vehicular environments presents numerous challenges. Factors such as environmental conditions, network congestion, and signal interference can degrade communication quality and disrupt network connectivity. To mitigate the impact of adverse conditions and ensure uninterrupted service delivery, future research should explore fault-tolerant techniques, resilient network topologies, and adaptive communication systems.

C. Adoption and User Engagement

Realizing the full potential of IoV technologies hinges on fostering user acceptance and adoption. Overcoming user skepticism, addressing safety concerns, and demonstrating the tangible benefits of IoV solutions are essential steps in gaining public trust and support. To cultivate positive attitudes toward IoV adoption, future research should emphasize user-centric design principles, human factors engineering, and comprehensive user education initiatives.

XII. Conclusion

Our suggested method improves security and communication in the IoV context by combining cooperative cryptography with IRS. This creative approach uses IRS technology with contemporary encryption techniques like AES to solve the problems of guaranteeing safe and dependable communication in dynamic vehicle networks. The creation of an algorithmic framework and network model outlines the fundamental components of our methodology. These components include the usage of a cloud server for data management, the provision of keys in a secure manner via a trusted authority, and the responsibilities that different entities—like users, cars, RSUs, and IRS—play in enabling safe communication. We explore the cryptography methods used to guarantee secure communication, emphasizing the role that key management and authentication play in maintaining data integrity and confidentiality. These methods provide strong security throughout the communication process and include session setup, encryption, decryption, and signature verification. We also investigate the incorporation of IRS into the Internet of Vehicles architecture and its possible influence by using secure PL on cost reduction, improved communication coverage, and energy efficiency. Our goal is to increase overall system performance by strategically deploying IRS to maximize signal losses, expand network coverage, and optimize communication paths. We also cover many strong cybersecurity assaults and countermeasures to strengthen our suggested system against cybersecurity threats. These include countermeasures to lessen widespread attacks like denial of service, data manipulation, and eavesdropping, guaranteeing the security of our system against malevolent acts.

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,” in *IEEE Access*, vol. 8, pp. 54314-54344, 2020, doi: 10.1109/ACCESS.2020.2981397.

[2] J. A. Fadhil and Q. I. Sarhan, “Internet of Vehicles (IoV): A Survey of Challenges and Solutions,” *2020 21st International Arab Conference on Information Technology (ACIT)*, pp. 1-10, 2020, doi: 10.1109/ACIT50332.2020.9300095.

[3] C. R. Storck and F. Duarte-Figueiredo, “A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles,” in *IEEE Access*, vol. 8, pp. 117593-117614, 2020, doi: 10.1109/ACCESS.2020.3004779.

[4] C. -M. Chen, B. Xiang, Y. Liu and K. -H. Wang, “A Secure Authentication Protocol for Internet of Vehicles,” in *IEEE Access*, vol. 7, pp. 12047-12057, 2019, doi: 10.1109/ACCESS.2019.2891105.

[5] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, “A survey on security and privacy issues in IoV,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 5, pp. 5409-5419, 2020, doi: 10.11591/ijece.v10i5.pp5409-5419.

[6] S. A. Chaudhry, “Designing an efficient and secure message exchange protocol for Internet of vehicles,” *Security and Communication Networks*, vol. 2021, pp. 1–9, 2021, doi: 10.1155/2021/5554318.

[7] H. Vasudev, V. Deshpande, D. Das and S. K. Das, “A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles,” in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6709-6717, 2020, doi: 10.1109/TVT.2020.2986585.

[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,” *Journal of Electrical Engineering*, vol. 20, no. 3, pp. 26–31, 2021, doi: 10.11113/elektrika.v20n3.291.

[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*, pp. 309–325, 2020, doi: 10.1007/978-3-030-36167-9_11.

[10] S. A. E. Mohamed and K. A. AlShalfan, “Intelligent Traffic Management System based on the Internet of vehicles (IoV),” *Journal of Advanced Transportation*, vol. 2021, pp. 1–23, 2021, doi: 10.1155/2021/4037533.

[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*, vol. 2022, pp. 1–19, 2022, doi: 10.1155/2022/1131479.

[12] S. Hakak *et al.*, “Autonomous Vehicles in 5G and beyond: A Survey,” *Vehicular Communications*, vol.39, 2022.

[13] P. Agbaje, A. Anjum, A. Mitra, E. Oseghale, G. Bloom and H. Olufowobi, “Survey of Interoperability Challenges in the Internet of Vehicles,” in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 22838-22861, 2022, doi: 10.1109/TITS.2022.3194413.

[14] S. Abbasi, A. M. Rahmani, A. Balador, and A. Sahafi, “Internet of Vehicles: Architecture, services, and applications,” *International Journal of Communication Systems*, vol. 34, no. 10, 2021, doi: 10.1002/dac.4793.

[15] Z. Mahmood, “Connected vehicles in the IoV: Concepts, technologies and architectures,” in *Connected Vehicles in the Internet of Things*, pp. 3–18, 2020, doi: 10.1007/978-3-030-36167-9_1.

[16] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, “A survey of autonomous vehicles: Enabling communication technologies and challenges,” *Sensors*, vol. 21, no. 3, 2021. doi: 10.3390/s21030706.

[17] B. Ji *et al.*, “Survey on the Internet of Vehicles: Network Architectures and Applications,” in *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 34-41, 2020, doi: 10.1109/MCOMSTD.001.1900053.

[18] E. S. Ali *et al.*, “Machine learning technologies for secure vehicular communication in Internet of vehicles: Recent advances and applications,” *Security and Communication Networks*, vol. 2021, pp. 1–23, 2021, doi: 10.1155/2021/8868355.

[19] H. N. Noura, O. Salman, R. Couturier, and A. Chehab, “LoRCA: Lightweight round block and stream cipher algorithms for IoV systems,” *Vehicular Communications*, vol. 34, 2022, doi: 10.1016/j.vehcom.2021.100416.

[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, doi: 10.1016/j.jisa.2021.102779.

[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”,” in *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4671-4675, 2020, doi: 10.1109/JIOT.2020.2975207.

[22] A. Aljumaili, H. Trabelsi and W. Jerbi, “A Review on Secure Authentication Protocols in IOV: Algorithms, Protocols, and Comparisons,” *2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pp. 1-11, 2023, doi: 10.1109/ISMSIT58785.2023.10304917.

[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, doi: 10.35940/ijrte.B2313.118419.

[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*, pp. 293–303, 2020, doi: 10.1007/978-3-030-48256-5_29.

[25] W. Jerbi, O. Cheikhrouhou, A. Guermazi and H. Trabelsi, “MSU-TSCH: A Mobile Scheduling Updated Algorithm for TSCH in the Internet of Things,” in *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,” *Journal of Sensors*, vol. 2021, pp. 1–8, 2021, doi: 10.1155/2021/8878513.

[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, 2021, doi: 10.1016/j.comcom.2021.03.022.

[28] Y. Liu *et al.*, “An Access Control Mechanism Based on Risk Prediction for the IoV,” *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1-5, 2020, doi: 10.1109/VTC2020-Spring48590.2020.9129056.

[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,” *Security and Privacy*, vol. 5, no. 3, 2022, doi: 10.1002/spy2.210.

[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,” in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2299-2313, 2021, doi: 10.1109/TITS.2020.3010288.

[31] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,” *Vehicular Communications*, vol. 23, 2020, doi: 10.1016/j.vehcom.2019.100214.

[32] S. Shojae Chaeikar, A. Jolfaei and N. Mohammad, “AI-Enabled Cryptographic Key Management Model for Secure Communications in the Internet of Vehicles,” in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 4589-4598, 2023, doi: 10.1109/TITS.2022.3200250.

[33] M. N. Aman, U. Javaid and B. Sikdar, “A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles,” in *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123-1139, 2021, doi: 10.1109/JIOT.2020.3010893.

[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,” in *IEEE Access*, vol. 9, pp. 11296-11305, 2021, doi: 10.1109/ACCESS.2021.3049830.

[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, pp. 77–86, 2021, doi: 10.32604/jiot.2021.017943.

[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,” in I*EEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1736-1751, 2021, doi: 10.1109/TVT.2021.3050614.

[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,” in *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 24398-24416, 2022, doi: 10.1109/JIOT.2022.3188731.

[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,” in *IEEE Transactions on Intelligent*

Transportation Systems, vol. 23, no. 12, pp. 24698-24713, 2022, doi: 10.1109/TITS.2022.3207593.

[39] K. Nongthombam, S. Rana, M. S. Obaidat, D. Chhikara and D. Mishra, "Construction of Efficient Authenticated Key Agreement Protocol for Intelligent Transportation System," *2022 2nd International Conference on Electronic Information Technology and Smart Agriculture (ICEITSA)*, pp. 62-66, 2022, doi: 10.1109/ICEITSA57468.2022.00020.

[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, pp. 93–104, 2023, doi: 10.2528/PIERM23052304.

[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, 2021, doi: 10.1504/IJHPCN.2020.112693.

[43] F. Naeem, M. Ali, G. Kaddoum, C. Huang and C. Yuen, "Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges," in *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1196-1217, 2023, doi: 10.1109/OJCOMS.2023.3273507.

[44] S. Kavaiya and D. K. Patel, "Restricting passive attacks in 6G vehicular networks: a physical layer security perspective," *Wireless Networks*, vol. 29, pp. 1355–1365, 2023. doi: 10.1007/s11276-022-03189-1.

[45] Jing Nie, Yan-Qing Tan, Chun-Lin Ji and Ruo-Peng Liu, "Analysis of Ku-Band steerable metamaterials reflectarray with tunable varactor diodes," *2016 Progress in Electromagnetic Research Symposium (PIERS)*, pp. 709-713, 2016, doi: 10.1109/PIERS.2016.7734429.

[46] D. Rotshild and A. Abramovich, "Realization and validation of continuous tunable metasurface for high resolution beam steering reflector at K-band frequency," *International Journal of RF And Microwave Computer-Aided Engineering*, vol. 31, 2021, doi: 10.1002/mmce.22559.

[47] D. Rotshild and A. Abramovich, "Ultra-Wideband reconfigurable X-band and Ku-band metasurface beam-steerable reflector for satellite communications," *Electronics*, vol. 10, no. 17, 2021, doi: 10.3390/electronics10172165.

[48] D. Rotshild and A. Abramovich, "Polarization consideration of 2-D beam-steering metasurface reflector at Ka-band for wireless communication," *2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS)*, pp. 486-490, 2021, doi: 10.1109/COMCAS52219.2021.9629016.

[49] E. Rahamim, D. Rotshild, and A. Abramovich, "Performance Enhancement of Reconfigurable Metamaterial Reflector Antenna by Decreasing the Absorption of the Reflected Beam," *Applied Sciences*, vol. 11, no. 19, 2021, doi: 10.3390/app11198999.

[50] Z. Qiu *et al.*, "High-dimensional coding/decoding information with braiding period in free-space optical communication link," *Optik*, vol. 258, 2022, doi: 10.1016/j.ijleo.2022.168828.

[51] M. V. Rao *et al.*, "Series-feed UCA antenna for generating highly azimuthal symmetric OAM Beam for unmanned aerial vehicles," *AEU - International Journal of Electronics and Communications*, vol. 171, 2023, doi: 10.1016/j.aeue.2023.154917.

[52] E. Anufriyev, "Quantification of orbital angular momentum (OAM) beams states of radio waves," *Optik*, vol. 226, 2021, doi: 10.1016/j.ijleo.2020.165603.

[53] Y. N. Phua *et al.*, "Design of a single-layer broadband reflectarray using circular microstrip patch loaded with two unequal slots," *AEU - International Journal of Electronics and Communications*, vol. 124, 2020, doi: 10.1016/j.aeue.2020.153341.

[54] B. He *et al.*, "Broadband and thermally switchable reflective metasurface based on Z-shape InSb for terahertz vortex beam generation," *Physica E: Low-dimensional Systems and Nanostructures*, vol. 144, 2022, doi: 10.1016/j.physe.2022.115373 .

[55] K. Guo and K. An, "On the Performance of RIS-Assisted Integrated Satellite-UAV-Terrestrial Networks With Hardware Impairments and Interference," in *IEEE Wireless Communications Letters*, vol. 11, no. 1, pp. 131-135, 2022, doi: 10.1109/LWC.2021.3122189.

[56] X. Shao, C. You, W. Ma, X. Chen and R. Zhang, "Target Sensing With Intelligent Reflecting Surface: Architecture and Performance," in *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 7, pp. 2070-2084, 2022, doi: 10.1109/JSAC.2022.3155546.

[57] Q. Pan, J. Wu, J. Nebhen, A. K. Bashir, Y. Su and J. Li, "Artificial Intelligence-Based Energy Efficient Communication System for Intelligent Reflecting Surface-Driven VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19714-19726, 2022, doi: 10.1109/TITS.2022.3152677.

[58] B. Zheng, C. You, W. Mei and R. Zhang, "A Survey on Channel Estimation and Practical Passive Beamforming Design for Intelligent Reflecting Surface Aided Wireless Communications," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1035-1071, 2022, doi: 10.1109/COMST.2022.3155305.

[59] A. Al-Hilo, M. Samir, M. Elhattab, C. Assi and S. Sharafeddine, "Reconfigurable Intelligent Surface Enabled Vehicular *Communication: Joint User Scheduling and Passive Beamforming," in IEEE Transactions on Vehicular Technology*, vol. 71, no. 3, pp. 2333-2345, 2022, doi: 10.1109/TVT.2022.3141935.

[60] Y. Xu, H. Xie, Q. Wu, C. Huang and C. Yuen, "Robust Max-Min Energy Efficiency for RIS-Aided HetNets With Distortion Noises," in *IEEE Transactions on Communications*, vol. 70, no. 2, pp. 1457-1471, 2022, doi: 10.1109/TCOMM.2022.3141798.

[61] Y. Zhu, B. Mao and N. Kato, "A Dynamic Task Scheduling Strategy for Multi-Access Edge Computing in IRS-Aided Vehicular Networks," in *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 4, pp. 1761-1771, 2022, doi: 10.1109/TETC.2022.3153494.

[62] V. Jamali, G. C. Alexandropoulos, R. Schober and H. V. Poor, "Low-to-Zero-Overhead IRS Reconfiguration: Decoupling Illumination and Channel Estimation," in *IEEE Communications Letters*, vol. 26, no. 4, pp. 932-936, 2022, doi: 10.1109/LCOMM.2022.3141206.

[63] J. Zhang, J. Liu, S. Ma, C. -K. Wen and S. Jin, "Large System Achievable Rate Analysis of RIS-Assisted MIMO Wireless Communication With Statistical CSIT," in *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 5572-5585, 2021, doi: 10.1109/TWC.2021.3068494.

[64] A. Abrardo, D. Dardari and M. Di Renzo, "Intelligent Reflecting Surfaces: Sum-Rate Optimization Based on Statistical Position Information," in *IEEE Transactions on Communications*, vol. 69, no. 10, pp. 7121-7136, 2021, doi: 10.1109/TCOMM.2021.3096549.

[65] X. Gan, C. Zhong, C. Huang and Z. Zhang, "RIS-Assisted Multi-User MISO Communications Exploiting Statistical CSI," in *IEEE Transactions on Communications*, vol. 69, no. 10, pp. 6781-6792, 2021, doi: 10.1109/TCOMM.2021.3100860.

[66] M. -M. Zhao, A. Liu, Y. Wan and R. Zhang, "Two-Timescale Beamforming Optimization for Intelligent Reflecting Surface Aided Multiuser Communication With QoS Constraints," in *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 6179-6194, 2021, doi: 10.1109/TWC.2021.3072382.

[67] Z. Peng, T. Li, C. Pan, H. Ren, W. Xu and M. D. Renzo, "Analysis and Optimization for RIS-Aided Multi-Pair Communications Relying on Statistical CSI," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3897-3901, 2021, doi: 10.1109/TVT.2021.3062710.

[68] K. Zhi, C. Pan, H. Ren and K. Wang, "Statistical CSI-Based Design for Reconfigurable Intelligent Surface-Aided Massive MIMO Systems With Direct Links," in *IEEE Wireless Communications Letters*, vol. 10, no. 5, pp. 1128-1132, 2021, doi: 10.1109/LWC.2021.3059938.

[69] E. Schoitsch, C. Schmittner, Z. Ma, and T. Gruber, "The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles," In *Advanced Microsystems for Automotive Applications 2015*, pp. 251–261, 2015, doi: 10.1007/978-3-319-20855-8_20.

[70] K. Zhang, Y. Mao, S. Leng, Y. He and Y. ZHANG, "Mobile-Edge Computing for Vehicular Networks: A Promising Network Paradigm with Predictive Off-Loading," in *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 36-44, 2017, doi: 10.1109/MVT.2017.2668838.

[71] X. Yu, D. Xu and R. Schober, "Enabling Secure Wireless Communications via Intelligent Reflecting Surfaces," *2019 IEEE Global Communica-*

tions Conference (GLOBECOM), pp. 1-6, 2019, doi: 10.1109/GLOBECOM38437.2019.9014322.

[72] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li and R. Kharel, ”Physical Layer Security in Vehicular Networks with Reconfigurable Intelligent Surfaces,” *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1-6, 2020, doi: 10.1109/VTC2020-Spring48590.2020.9128438.

[73] M. Cui, G. Zhang and R. Zhang, ”Secure Wireless Communication via Intelligent Reflecting Surface,” in *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410-1414, 2019, doi: 10.1109/LWC.2019.2919685.

[74] Y. Ai, F. A. P. deFigueiredo, L. Kong, M. Cheffena, S. Chatzinotas and B. Ottersten, ”Secure Vehicular Communications Through Reconfigurable Intelligent Surfaces,” in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7272-7276, 2021, doi: 10.1109/TVT.2021.3088441.