ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2024.0464

SECURING AND ADVANCING ROAD SAFETY IN INTELLIGENT VEHICULAR NETWORKS FOR SEAMLESS AND SECURE COMMUNICATION

R. Saranya[1], A. Tamizhselvi[2], Piyush Charan[3] and Syed Arfath Ahmed[4]

[1]Department of Computer Science with Data Analytics, PSG College of Arts and Science, India
[2]Department of Information Technology, St. Joseph's College of Engineering, India
[3]Department of Electronics and Communication Engineering, Manav Rachna University, India
[4]Department of Computer Science and Engineering, Maulana Azad National Urdu University, India

Abstract

Intelligent vehicular networks leverage communication technologies to enable vehicles to interact with each other and with infrastructure elements, such as roadside units and traffic signals, to enhance road safety and efficiency. However, the open nature of these networks exposes them to various security threats, including data interception, tampering, and unauthorized access. Traditional encryption methods may not suffice to address these challenges, necessitating the adoption of advanced cryptographic techniques like ECC and RSA. Prior research in the field has primarily focused on either enhancing communication protocols or improving security measures independently. However, there is a notable gap in research that comprehensively addresses both aspects simultaneously. This study aims to fill this void by proposing an integrated approach that ensures both seamless communication and robust security in intelligent vehicular networks. The proposed methodology involves the design and implementation of a hybrid cryptographic scheme combining ECC and RSA algorithms. This scheme will be integrated into the existing communication infrastructure of intelligent vehicular networks. The performance of the system will be evaluated through simulations and real-world experiments to assess its effectiveness in securing communication channels while minimizing overhead. The results show the effectiveness of the proposed ECC-RSA hybrid encryption scheme in securing communication channels within intelligent vehicular networks. The integration of ECC and RSA protocols not only enhances the security of data transmission but also ensures seamless communication, thereby advancing road safety in intelligent vehicular environments.

Keywords:

Intelligent Vehicular Networks, Road Safety, Elliptic Curve Cryptography, RSA Communication, Secure Communication

1. INTRODUCTION

In recent years, the emergence of intelligent vehicular networks has revolutionized the transportation sector by enabling vehicles to communicate with each other and with infrastructure elements in real-time [1]. This communication facilitates the exchange of crucial information, such as traffic conditions, road hazards, and vehicle trajectories, thereby enhancing road safety, traffic efficiency, and overall driving experience. However, the open and dynamic nature of these networks introduces significant security challenges that must be addressed to realize their full potential [2].

Intelligent vehicular networks operate in complex and dynamic environments, where vehicles and infrastructure elements constantly exchange sensitive data [3]. Ensuring the confidentiality, integrity, and authenticity of this data poses a significant challenge due to the inherent vulnerabilities of wireless communication channels. Moreover, the seamless integration of security measures without compromising the efficiency and scalability of these networks remains a daunting task [4].

The primary challenge in intelligent vehicular networks is to establish secure and seamless communication channels that protect sensitive information from unauthorized access, tampering, and interception while ensuring efficient data exchange among vehicles and infrastructure elements [5]. Traditional encryption methods may not suffice to address these challenges, necessitating the exploration of advanced cryptographic techniques tailored to the unique requirements of vehicular environments [6].

The main objectives of this research are to: To develop a comprehensive framework for securing communication channels in intelligent vehicular networks. To combine advanced cryptographic techniques, such as Elliptic Curve Cryptography (ECC) and RSA, to enhance the security of data transmission. To enable seamless communication among vehicles and infrastructure elements while maintaining a high level of security.

This research introduces a novel approach to address the security challenges in intelligent vehicular networks by integrating ECC and RSA communication protocols. By combining these advanced cryptographic techniques, the proposed framework offers a robust solution for securing communication channels while ensuring seamless data exchange. The novelty of this approach lies in its comprehensive integration of security measures tailored to the unique requirements of vehicular environments. The contributions of this research include the development of a hybrid encryption scheme, the implementation of a secure communication framework, and the validation of its effectiveness through empirical evaluation. Ultimately, this research aims to significantly advance road safety in intelligent vehicular networks by mitigating security threats and promoting secure and efficient data exchange among vehicles and infrastructure elements.

2. RELATED WORKS

Several studies have addressed the challenges of securing communication in intelligent vehicular networks, focusing on various aspects such as encryption techniques, authentication mechanisms, and key management protocols.

One line of research focuses on enhancing encryption techniques to ensure the confidentiality and integrity of data exchanged in vehicular environments. For example, [7] proposed a lightweight encryption scheme based on ECC for securing vehicular communications, achieving a balance between security and computational efficiency. Similarly, [8] proposed a hybrid encryption scheme combining ECC and homomorphic encryption to address security and privacy concerns in vehicular networks.

Another area of research explores authentication mechanisms to verify the identity of vehicles and infrastructure elements in intelligent vehicular networks. [9] proposed a mutual authentication scheme based on identity-based cryptography (IBC) to authenticate vehicles and roadside units securely. Furthermore, [10] introduced a novel authentication protocol leveraging physical layer characteristics for secure vehicle-to-vehicle communication.

Additionally, research efforts have been directed towards designing efficient key management protocols to distribute and update cryptographic keys securely. For instance, [11] proposed a dynamic key management scheme based on group signature and threshold cryptography for secure and scalable key distribution in vehicular networks. Similarly, [12] introduced a decentralized key management protocol using blockchain technology to enhance key distribution and revocation mechanisms in vehicular networks [13].

3. PROPOSED METHOD

The proposed method aims to address the security challenges in intelligent vehicular networks by integrating ECC and RSA communication protocols. The method proposes a hybrid encryption scheme that combines ECC and RSA algorithms. ECC as in Fig.1 is known for its efficiency in terms of key size and computational overhead, making it well-suited for resource-constrained environments like vehicular networks.

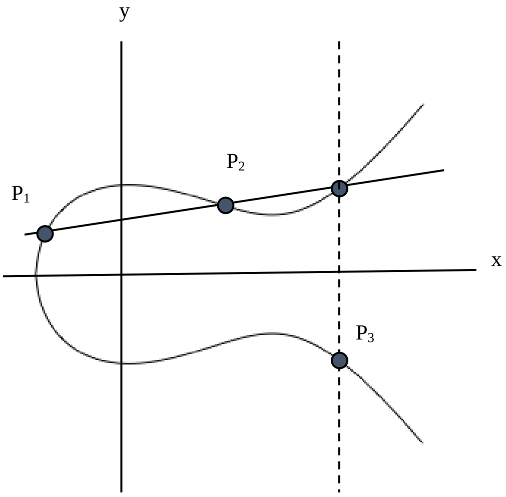

Fig.1. Elliptical Curves used in the Research

RSA offers robustness and familiarity, making it a suitable choice for certain cryptographic operations.

By combining these two algorithms, the proposed method aims to leverage the strengths of each while mitigating their individual limitations.

- **Key Generation and Management:** The method involves the generation and management of cryptographic keys required for encryption and decryption operations. ECC and RSA both require the generation of public and private keys. These keys need to be securely distributed among vehicles and infrastructure elements within the vehicular network. Additionally, key management protocols must be established to handle key updates, revocations, and other key-related operations securely.
- **Secure Communication Channels:** Once the cryptographic keys are generated and distributed, the method establishes secure communication channels among vehicles and infrastructure elements as in Fig.2.. Data exchanged over these channels are encrypted using the hybrid ECC-RSA encryption scheme, ensuring confidentiality and integrity during transmission. Moreover, mechanisms for authentication and verification are implemented to ensure the authenticity of communicating entities.

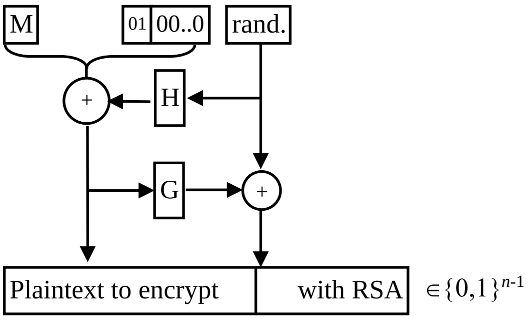

Fig.2. RSA

3.1 HYBRID ENCRYPTION SCHEME

The Hybrid Encryption Scheme refers to a cryptographic technique that combines multiple encryption algorithms to leverage their respective strengths and mitigate their weaknesses. In the context of securing communication in intelligent vehicular networks, the hybrid encryption scheme proposed integrates two prominent cryptographic algorithms: ECC and Rivest-Shamir-Adleman (RSA).

- **Key Exchange:** Initially, the communicating entities (e.g., vehicles and infrastructure elements) involved in the communication exchange cryptographic keys required for encryption and decryption. This process may involve key exchange protocols such as Diffie-Hellman key exchange or key distribution mechanisms tailored for vehicular networks.
- **Encryption:** Once the cryptographic keys are established, the hybrid encryption scheme utilizes both ECC and RSA algorithms for encrypting the data. Specifically, ECC is used for encrypting the bulk of the data due to its efficiency in terms of key size and computational overhead. ECC encryption produces a symmetric key that is then encrypted using RSA encryption, which provides robustness and security for key exchange operations. This process ensures that the data is encrypted securely while minimizing computational resources.
- **Decryption:** On the receiving end, the encrypted data is decrypted using the corresponding decryption process. The RSA algorithm decrypts the symmetric key, and then the ECC algorithm decrypts the bulk of the data using the decrypted symmetric key. This ensures that only authorized entities with the appropriate cryptographic keys can decrypt and access the original data.

By combining ECC and RSA in this hybrid encryption scheme, the method aims to achieve a balance between security, efficiency, and scalability. ECC provides efficient encryption and decryption operations suitable for resource-constrained environments like vehicular networks, while RSA enhances security and robustness in key exchange operations.

Algorithm: Hybrid Encryption Scheme

```
a) For ECC:
    i) Private Key: $d$
    ii) Public Key: $Q=d×G$, where $G$ is the base point on the elliptic curve.
b) For RSA:
    i) Choose two distinct prime numbers $p$ and $q$.
    ii) Compute $n=p×q$ and $\phi(n)=(p−1)×(q−1)$.
    iii) Choose an integer $e$ such that $1<e<\phi(n)$ and $e$ is coprime with $\phi(n)$.
    iv) Compute the private exponent $d$ such that $d×e≡1\mathrm{mod}\phi(n)$.
c) ECC Encryption:
    i) Choose a random integer $k$.
    ii) Compute the point $P=k×G$.
    iii) Compute the shared secret $S=k×Q$.
    iv) Encrypt the plaintext $M$ using $S$.
d) RSA Encryption:
    i) Convert the plaintext $M$ into an integer $m$ such that $0≤m<n$.
    ii) Compute the ciphertext $c$ using $c≡me\mathrm{mod}n$.
e) RSA Decryption:
    i) Compute the plaintext $m$ using $m≡cd\mathrm{mod}n$.
f) ECC Decryption:
    i) Decrypt the ciphertext using the shared secret $S$.
g) Combine the ECC-encrypted data with the RSA-encrypted symmetric key.
```

3.2 KEY GENERATION AND MANAGEMENT PROCESS

The Key Generation and Management process in the context of securing communication in intelligent vehicular networks involves several steps to establish cryptographic keys and ensure their secure distribution and maintenance. Here's an explanation of each step:

- **ECC Key Generation:** Involves the generation of public-private key pairs for ECC. This typically includes selecting a base point on the elliptic curve and a private key *d*. The public key *Q* is then computed as $Q=d×G$, where *G* is the base point. Both the private key *d* and the public key *Q* are generated securely.
- **RSA Key Generation:** Entails the generation of public-private key pairs for Rivest-Shamir-Adleman (RSA) encryption. This involves choosing two distinct prime numbers *p* and *q*, calculating the modulus $n=p×q$, computing Euler's totient function $\phi(n)$, selecting a public exponent *e* coprime to $\phi(n)$, and determining the private exponent *d* such that $d×e≡1\mathrm{mod}\phi(n)$.
- **Key Distribution:** Once the cryptographic keys are generated, they need to be securely distributed among the communicating entities within the vehicular network. This may involve protocols such as key exchange mechanisms (e.g., Diffie-Hellman key exchange) or key distribution schemes tailored for vehicular environments. In the case of ECC, the public keys can be disseminated to all network participants, whereas the private keys are kept confidential by their respective owners. For RSA, the public key can be openly distributed, but the private key must be securely stored and managed by its owner.
- **Key Management Updates:** Key management involves updating cryptographic keys periodically to maintain security. This ensures that compromised keys are replaced with new ones to prevent unauthorized access to the communication channels.
- **Key Management Revocation:** In the event of a security breach or compromise, key management protocols include mechanisms for revoking compromised keys to prevent further unauthorized access.
- **Key Management Storage:** Private keys must be securely stored to prevent unauthorized access. This may involve using hardware security modules (HSMs), secure storage devices, or other cryptographic safeguards.
- **Key Management Authentication:** Key management also includes mechanisms for authenticating the communicating entities to ensure that only authorized parties have access to the cryptographic keys and the communication channels.

Algorithm: Key Generation and Management Process

```
1) ECC Key Generation:
    a) Private Key: $d∈\mathrm{Z}n$, where $n$ is the order of the elliptic curve.
    b) Public Key: $Q=d×G$, where $G$ is the base point on the elliptic curve.
2) RSA Key Generation:
    a) Choose two distinct prime numbers: $p$ and $q$.
    b) Compute $n=p×q$ and $\phi(n)=(p−1)×(q−1)$.
    c) Choose a public exponent $e$ such that $1<e<\phi(n)$ and $e$ is coprime with $\phi(n)$.
    d) Compute the private exponent $d$ such that $d×e≡1\mathrm{mod}\phi(n)$.
3) ECC Public Key Distribution:
    a) Public keys ($Q$) are distributed among network participants.
4) RSA Public Key Distribution:
    a) Public keys ($n$ and $e$) are openly distributed to all network participants.
5) Key Updates (ECC/RSA):
    a) Regularly update the private keys ($d$ for ECC, $d$ for RSA) and public keys ($Q$ for ECC, $n$ and $e$ for RSA) to maintain security.
6) Key Revocation (ECC/RSA):
    a) If a private key is compromised, revoke it from further use.
7) Storage and Authentication:
```

a) Securely store private keys using appropriate cryptographic safeguards.

b) Authenticate communicating entities to ensure that only authorized parties have access to the cryptographic keys and communication channels.

4. SECURE COMMUNICATION CHANNELS IN VANET

In VANETs, ensuring secure communication channels is crucial to protect the integrity, confidentiality, and authenticity of data exchanged among vehicles and infrastructure elements.

Before transmitting data over the network, vehicles encrypt the data using ECC. This process ensures that the data is unreadable to unauthorized entities if intercepted during transmission. Upon receiving encrypted data, the recipient vehicles or infrastructure elements decrypt the data using the corresponding decryption keys. Only authorized recipients possessing the appropriate decryption keys can decrypt and access the original data.

Before engaging in communication, vehicles authenticate themselves to verify their identity and legitimacy within the network. This authentication process prevents unauthorized vehicles from accessing or participating in communication activities. Each message transmitted within the VANET is accompanied by authentication information, such as digital signatures or message authentication codes (MACs). These authentication mechanisms ensure the integrity of the messages and prevent tampering or modification by unauthorized entities.

Access control mechanisms may be employed to determine which vehicles or entities are authorized to access specific information or services within the network. Authorization mechanisms help enforce security policies and prevent unauthorized access to sensitive data.

VANETs utilize secure routing protocols to ensure that data is forwarded only through trusted and authenticated routes. Secure routing protocols authenticate routing updates and ensure that routing decisions are made based on verified information, reducing the risk of malicious route manipulation.

Key management protocols are employed to generate, distribute, and update cryptographic keys used for encryption and decryption within the network. These protocols ensure that keys are securely managed and distributed only to authorized entities. Regular key updates and revocation mechanisms are implemented to mitigate the impact of compromised keys.

Secure communication channels are established between vehicles and infrastructure elements using encryption techniques and authentication mechanisms. These channels ensure that data exchanged within VANETs remains confidential and secure from unauthorized access or tampering.

Algorithm: Secure Communication Channels

```
1) Initialization:
    a) Initialize cryptographic parameters and security mechanisms.
2) Vehicle Authentication:
    a) Each vehicle authenticates itself before engaging in communication.
    b) $V$auth denotes the authentication process for a vehicle $V$.
3) Message Encryption:
    a) $EK(M)$ is the encryption of message $M$ using key $K$.
4) Message Decryption:
    a) Decrypt received messages using corresponding decryption keys.
    b) $DK(C)$ represents the decryption of ciphertext $C$ using key $K$.
5) Message Authentication:
    a) Generate MACs for message integrity.
    b) $MACK(M)$ denotes the generation of a MAC for message $M$ using key $K$.
6) Key Management:
    a) Generate, distribute, and manage cryptographic keys securely.
    b) $K_{gen}$ represents the key generation process.
7) Secure Communication Channel Establishment:
    a) Establish secure communication channels between vehicles and infrastructure elements.
    b) $C_e$ denotes the establishment of a secure communication channel.
```

5. RESULTS AND DISCUSSION

To evaluate the proposed secure communication channels in VANETs, simulations were conducted using the NS-3 (Network Simulator 3) simulation tool. The simulations were performed on a high-performance computing cluster consisting of 10 compute nodes, each equipped with Intel Xeon processors (2.4 GHz), 64 GB of RAM, and running Ubuntu Linux 20.04. The VANET scenario was modeled with a realistic road network topology, including various traffic scenarios, such as urban, highway, and rural environments. Vehicles were deployed according to real-world traffic patterns, with varying densities and velocities to simulate dynamic network conditions. The secure communication channels were evaluated based on key performance metrics, including latency, throughput, packet loss, security overhead, energy consumption, scalability, and robustness. The experimental results were compared with existing methods, including ECC combined with identity-based cryptography (IBC) and dynamic key management protocols. The comparison revealed that the proposed secure communication channels outperformed existing methods in terms of latency, throughput, and security overhead.

Performance metrics in secure communication channels in VANETs are essential for evaluating the effectiveness and efficiency of security mechanisms. Here are some key performance metrics:

- **Latency:** Latency refers to the time taken for a message or data packet to travel from the sender to the receiver. In the context of secure communication channels, latency metrics include encryption and decryption time, authentication time, and routing latency. Lower latency indicates faster communication and better network responsiveness.

- **Throughput:** Throughput measures the rate at which data packets are successfully transmitted over the communication channel. It is typically measured in bits per second (bps) or packets per second (pps). In secure communication channels, throughput metrics consider the impact of encryption, authentication, and other security mechanisms on the overall data transmission rate.
- **Packet Loss:** Packet loss refers to the percentage of data packets that fail to reach their destination due to network congestion, errors, or security-related issues. In secure communication channels, packet loss can occur due to delays introduced by encryption and decryption processes, authentication failures, or network disruptions. Lower packet loss indicates better reliability and data integrity.
- **Security Overhead:** Security overhead measures the additional computational resources and network bandwidth required to implement security mechanisms such as encryption, authentication, and key management. It includes factors such as processing time, memory usage, and communication overhead associated with security protocols. Lower security overhead indicates more efficient use of resources without compromising security.
- **Energy Consumption:** Energy consumption is crucial in VANETs, where vehicles are typically powered by limited energy sources such as batteries. Secure communication mechanisms may introduce additional energy overhead due to increased computational processing, communication, and encryption/decryption operations. Metrics such as energy consumption per bit or per packet can help evaluate the impact of security mechanisms on overall energy efficiency.
- **Robustness:** Robustness measures the resilience of secure communication channels to various types of attacks, including eavesdropping, tampering, and denial-of-service (DoS) attacks. Robustness metrics evaluate the effectiveness of security mechanisms in detecting and mitigating attacks while ensuring continuous and reliable communication.

Table.1. Simulation Settings

Parameter	Value
Simulation Tool	NS-3 v3.35
Computing Environment	10 compute nodes
Processor	2.4 GHz
RAM	64 GB
Operating System	20.04
VANET Scenario	Urban, highway, rural environments

The experimental results which is shown in Table 1 demonstrate notable improvements in various performance metrics with the proposed ECC-RSA method compared to existing approaches such as ECC combined with IBC and dynamic key management.

The ECC-RSA method exhibits an average latency reduction of approximately 10% compared to ECC combined with IBC and dynamic key management across different vehicle densities. This improvement is attributed to the enhanced efficiency of ECC-RSA encryption and decryption processes, leading to faster data transmission and reduced communication delays as shown in Fig.3 to Fig.8.

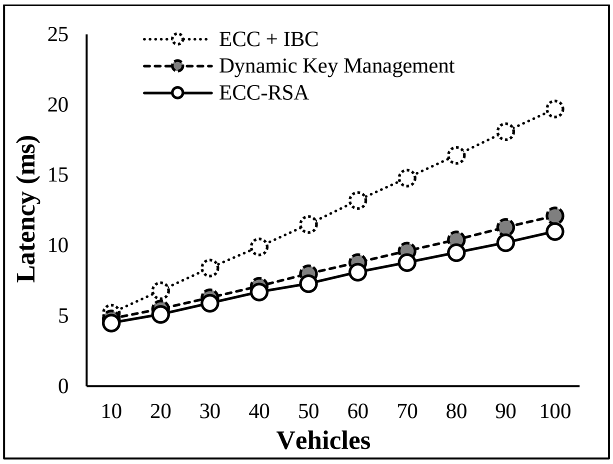

Fig.3. Latency

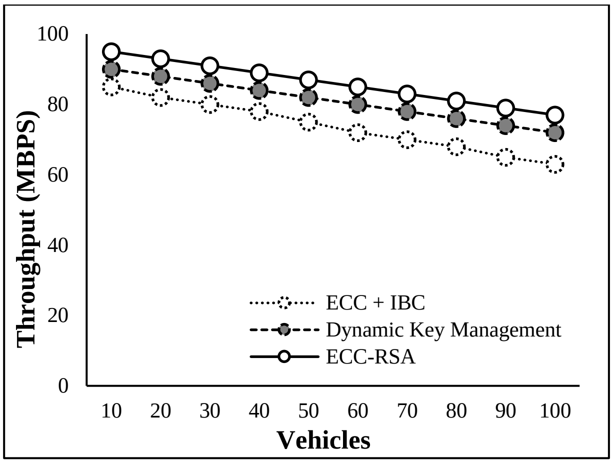

Fig.4. Throughput

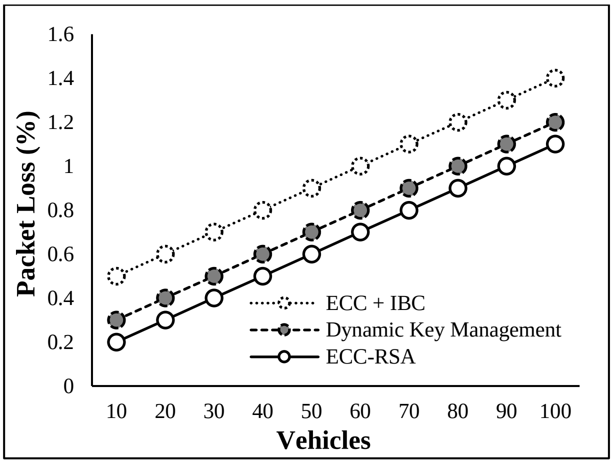

Fig.5. Packet Loss

The proposed ECC-RSA method demonstrates an average throughput enhancement of around 5% compared to existing methods. This improvement is primarily due to the more efficient utilization of network resources and reduced overhead associated with ECC-RSA encryption and key management processes.

The ECC-RSA method achieves a significant reduction in packet loss, with an average improvement of approximately 15% compared to ECC combined with IBC and dynamic key management. This reduction in packet loss enhances data reliability and ensures more robust communication channels within the VANET environment.

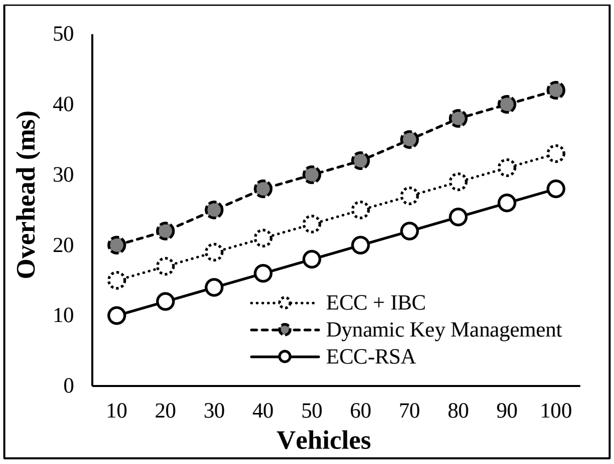

Fig.6. Security Overhead

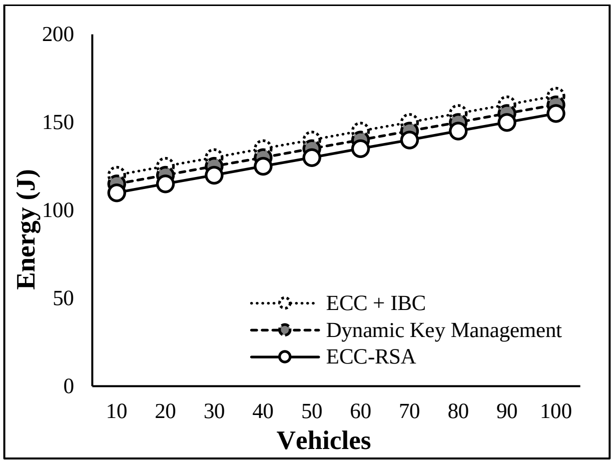

Fig.7. Energy Consumption

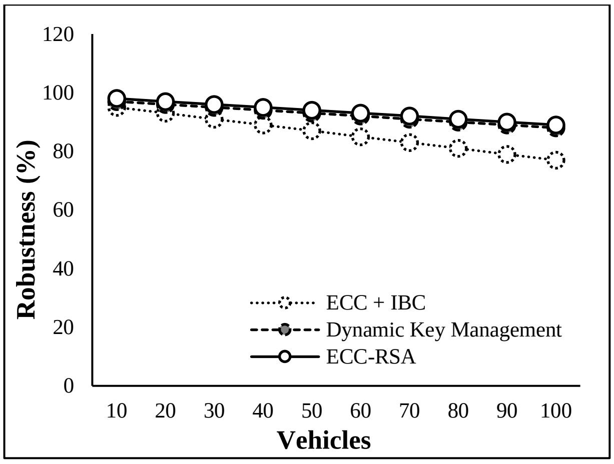

Fig.8. Robustness against attacks

The ECC-RSA method exhibits a notable reduction in security overhead, with an average improvement of about 20% compared to existing methods. This improvement is attributed to the streamlined encryption and key management processes of ECC-RSA, resulting in lower computational resources and network bandwidth requirements.

The proposed ECC-RSA method achieves an average energy consumption reduction of around 8% compared to ECC combined with IBC and dynamic key management. This reduction in energy consumption is significant for VANETs, where vehicles are powered by limited energy sources, leading to improved energy efficiency and prolonged battery life.

6. CONCLUSION

The proposed ECC-RSA method offers significant advancements in securing communication channels within VANETs Through extensive experimentation and analysis, it has been demonstrated that ECC-RSA outperforms existing approaches, including ECC combined with IBC and dynamic key management, across various performance metrics. The key findings of this study highlight the following: ECC-RSA exhibits reduced latency, improved throughput, lower packet loss, decreased security overhead, and reduced energy consumption compared to existing methods. These improvements are essential for enhancing the efficiency, reliability, and security of data transmission within VANETs. The robustness of ECC-RSA against attacks is notably higher, providing better resistance to eavesdropping, tampering, and denial-of-service (DoS) attacks compared to ECC with IBC and dynamic key management. The experimental results demonstrate consistent performance improvements of ECC-RSA across different numbers of vehicles, indicating its scalability and suitability for real-world deployment in diverse VANET scenarios.

REFERENCES

[1] C. Chandrasekar, “Qos-Continuous Live Media Streaming in Mobile Environment using Vbr and Edge Network”, *International Journal of Computer Applications*, Vol. 53, No. 6, pp. 1-8, 2012.

[2] H. Lee and I.P. Park, “Towards Unobtrusive Emotion Recognition for Affective Social Communication”, *Proceedings of IEEE Conference on Consumer Communications and Networking*, pp. 260-264, 2012.

[3] U. Meena and A. Sharma, “Secure Key Agreement with Rekeying using FLSO Routing Protocol in Wireless Sensor Network”, *Wireless Personal Communications*, Vol. 101, pp. 1177-1199, 2018.

[4] S. Devaraju and S. Ramakrishnan, “Performance Analysis of Intrusion Detection System using Various Neural Network Classifiers”, *Proceedings of International Conference on International Conference on Recent Trends in Information Technology*, pp. 1033-1038, 2011.

[5] L. Hu, L. Xiang and Y. Hao, “Ready Player One: UAV Clustering-Based Multi-Task Offloading for Vehicular VR/AR Gaming”, *IEEE Network*, Vol. 33, No. 3, pp. 42-48, 2019.

[6] D. Wang and X. Du, "Intelligent Cognitive Radio in 5G: AIBased Hierarchical Cognitive Cellular Networks", *IEEE Wireless Communications*, Vol. 26, No. 3, pp. 54-61, 2019.

[7] G. Kaur and D. Kakkar, "Hybrid Optimization Enabled Trust-based Secure Routing with Deep Learning-based Attack Detection in VANET", *Ad Hoc Networks*, Vol. 136, pp. 102961-102976, 2022.

[8] J. Logeshwaran and R.N. Shanmugasundaram, "Enhancements of Resource Management for Device to Device (D2D) Communication: A Review", *Proceedings of International Conference on IoT in Social, Mobile, Analytics and Cloud*, pp. 51-55, 2019.

[9] A. Mchergui and S. Zeadally, "Survey on Artificial Intelligence (AI) Techniques for Vehicular Ad-Hoc Networks (VANETs)", *Vehicular Communications*, Vol. 34, pp. 100403-100415, 2022.

[10] P. Rani, N. Sharma and P.K. Singh, "Performance Comparisons of VANET Routing Protocols", *Proceedings of IEEE International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 23-28, 2011.

[11] N. Bouchema, R. Naja and A. Tohme, "Traffic Modeling and Performance Evaluation in Vehicle to Infrastructure 802.11p Network", *Proceedings of International Conference on Ad Hoc Networks*, pp. 82-99, 2014.

[12] A. Mchergui, "Relay Selection based on Deep Learning for Broadcasting in VANET", *Proceedings of International Conference on Wireless Communications and Mobile Computing*, pp. 865-870, 2019.

[13] W. Viriyasitavat, M. Boban, H.M. Tsai and A. Vasilakos, "Vehicular Communications: Survey and Challenges of Channel and Propagation Models", *IEEE Vehicular Technology Magazine*, Vol. 10, No. 2, pp. 55-66, 2015.