2024 IEEE 29th Asia Pacific Conference on Communications (APCC) | 979-8-3315-1781-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/APCC62576.2024.10768020

PISTON: PUF-Integrated Secure, Throughput-Optimized Network Protocol for IoV

Koustav Kumar Mondal
IDRP: IoT & Applications
IIT Jodhpur
Rajasthan, India
mondal.4@iitj.ac.in

Ashi Gupta
Dept. of ECE
NIT Patna
Bihar, India
ashig.ph21.ec@nitp.ac.in

Debasis Das
Dept. of CSE
IIT Jodhpur
Rajasthan, India
debasis@iitj.ac.in

Chun-I Fan
Dept. of CSE
National Sun Yat-sen University
Kaohsiung, Taiwan
cifan@mail.cse.nsysu.edu.tw

***Abstract*—This research introduces PISTON, a novel protocol designed to enhance the security, efficiency, and performance of Internet of Vehicles (IoV) networks. PISTON integrates advanced authentication mechanisms utilizing Physically Unclonable Functions (PUFs) and multifactor authentication with dynamic challenges and zero-knowledge proof-based authentication to ensure robust security and mitigate various cyber threats, including Denial-of-Service (DoS) attacks. The protocol further incorporates sleep-wake scheduling, priority-based scheduling, and adaptive modulation and coding to optimize network performance. The communication overhead in PISTON is derived through a formula that incorporates latency, energy consumption, and throughput, demonstrating the protocol's efficiency in dynamic vehicular environments. Comparative analysis against existing protocols highlights PISTON's superiority in seamless handover, provable security, and DoS attack resilience. Experimental results show that PISTON reduces energy consumption by 30% and achieves 20% higher data throughput while maintaining low latency, essential for real-time IoV applications. The empirical findings underscore PISTON's advancements in establishing a new benchmark for future IoV deployments, ensuring secure, energy-efficient, low-latency, and high-throughput communication.**

***Index Terms*—Internet of Vehicles (IoV), Physically Unclonable Functions (PUFs), Secure Communication, Communication Overhead, Vehicular Networks, Authentication Protocol**

I. Introduction

The increase in the number of vehicles on the road and in transportation networks is substantial and is expected to reach approximately two billion within the next 10 to 20 years [1]. This growth can be largely attributed to the implementation of intelligent transportation systems (ITS) and related technologies that have facilitated services such as electronic toll collection, pay-as-you-go insurance, dynamic road signs, real-time traffic information, and fleet logistics and management. Furthermore, the integration of passenger and autonomous vehicles (AVs) into the existing vehicular network architectures is a key focus of the next generation of ITS applications. It is important to note that traffic accidents result in approximately 1.35 million fatalities each year, as reported by the World Health Organization (WHO) [2]. The main objective of incorporating vehicular communication systems and networks is to improve the driving experience by increasing road safety and convenience [3]. ITS play a pivotal role in the development of smart cities and the Internet of Things (IoT). The Internet of Vehicles (IoV) is a critical component of ITS, with the potential to support millions of vehicles in vehicular ad hoc networks (VANETs), including autonomous vehicles (AVs) [4].

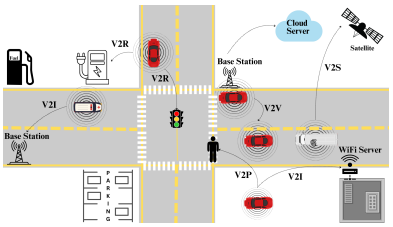


Fig. 1. V2X Communication

A. Motivation

The implementation of VANETs presents significant security, privacy, and trust challenges [5]. In Intelligent Transportation Systems (ITS), vehicles equipped with communication and sensing capabilities share data with other vehicles (V2V), roadside units (RSUs) (V2R), infrastructure (V2I), pedestrians (V2P), and sensors (V2S) as shown in Fig. 1. The main goals of IoVs are to improve driving safety and convenience, reduce traffic accidents [6], and optimize traffic flow. However, adding communication capabilities to vehicles increases their vulnerability to cyberattacks. Attackers can spread false information, access the internal communication bus, and cause significant damage. The potential for cyberattacks on VANETs is expected to rise by 20.3% in the next decade [2]. Given the critical nature of VANET security, especially for AVs, it is essential to address known cyberattacks on V2V and V2I communications, including denial of service (DoS), Sybil attacks, data tampering, replay attacks, timing attacks, man-in-the-middle attacks, impersonation attacks, and identity attacks [5]. Attackers can physically access vehicles or RSUs, compromising secret keys. Current VANET security relies on public-key infrastructure, assuming physical security of RSUs and vehicles, which is not always feasible.

B. Problem Statement

Given the rapid movement of vehicles, any network protocol created for IoVs must be highly energy-efficient. One of the essential security requirements for IoVs is authentication, which involves verifying the source of data received from another vehicle or RSU. This verification must be both foolproof and enable low-latency data transmission. In addition, IoVs require a high throughput for

Authorized licensed use limited to: Indian Institute of Technology - Jodhpur. Downloaded on December 07,2024 at 06:14:49 UTC from IEEE Xplore. Restrictions apply.

TABLE I
SUMMARY OF EXISTING IOV NETWORK PROTOCOLS

Methodology	Scalability	Low Latency	High Throughput	Energy Efficiency	Security Guarantee
Fotouhi *et al.* [7]	✗	✓	✓	✗	✓
Li *et al.* [8]	✗	✗	✗	✓	✓
Wang *et al.* [9]	✓	✓	✓	✗	✗
Roman *et al.* [10]	✓	✗	✗	✓	✓
Raveendra *et al.* [11]	✗	✓	✗	✓	✓
Proposed: PISTON	✓	✓	✓	✓	✓

handling large amounts of data. Thus, the main challenges to be addressed are:

- Ensuring secure communication in IoVs to prevent various cyberattacks.
- Reducing energy consumption in VANETs while maintaining network performance.
- Achieving low-latency and high-throughput data transmission in a highly dynamic vehicular environment.

C. Contributions

This article delves into the issue of network protocol in IoV, highlighting its significant contributions as follows:

- This study introduces a multi-phase authentication protocol that employs Physically Unclonable Functions (PUFs) to provide multi-factor authentication and zero-knowledge proof-based key agreement for secure communication in the Internet of Vehicles (IoV).
- The paper describes a protocol that reduces energy consumption through sleep-wake scheduling, lowers latency with priority-based scheduling, and enhances throughput with efficient routing and load balancing.
- The research proposes an adaptive modulation and coding strategy to attain maximum data rates and incorporates data aggregation and load balancing techniques to alleviate congestion and maintain high throughput.

The proposed protocol, named PISTON (PUF-Integrated Secure, Throughput-Optimized Network Protocol for IoV), addresses these challenges by providing a secure, energy-efficient, low-latency, and high-throughput communication framework tailored for IoV networks.

II. BRIEF LITERATURE REVIEW

In our pursuit of establishing end-to-end networking and anonymous authentication for IoT and other resource-constrained device environments, we have identified several significant research gaps addressed by previous literature. Scholars have introduced various innovative techniques leveraging Physically Unclonable Functions (PUF). These PUF-enabled protocols effectively mitigate numerous physical security threats. However, they come with the trade-off of increased hardware and computational overhead. By comparing our proposed work with these existing methods, we aim to highlight improvements and advancements that address these limitations while maintaining robust security features [12].

A physically secure anonymous mutual authentication mechanism for industrial wireless sensor networks was suggested by Gope et al. [13]. It uses simple cryptographic primitives such as XOR, PUF, and hash functions. However, because of the possibility of environmental influences causing one or more PUF output bits to be erroneous for every given challenge, this protocol is unable to support a noisy PUF environment. Without requiring explicit storage of CRPs, Chatterjee et al. [14] combined PUF with identity-based encryption to create an authentication and key exchange system for the Internet of Things. Bilinear pairing operations are used, and this protocol could withstand modeling attacks as well. However, it requires the participation of a server or gateway, significantly affecting "efficiency". The mentioned work rely on RSUs and cellular base stations for resource allocation, which means that the network resources will get exhausted faster. An authentication method was put out by Roman et al. [10] for wireless power transfer charging systems that demand the purchase of tickets in order to access the charging station. Nevertheless, their protocol lacked sufficient "mutual authentication and was open to a denial-of-service attack". The majority of such PUF-based anonymous authentication protocols now in use are not flexible enough or secure enough for end-to-end IoV applications [15]. Applying game theory and strong cryptographic operations results in "high computation costs" that quickly deplete batteries, making them unsuitable for lightweight sensors in the IoV [16], [17]. Li et al. [18] investigated wireless connectivity concerns to protect against outside eavesdroppers. To increase the secrecy degree of freedom, the suggested approach pairs devices securely using a cooperative secrecy transmission technique. Despite the fact that their solutions offer robust cryptographic algorithms and effective power optimization techniques, these solutions are not suitable in the "highly dynamic" IoV environment [12], [15] due to high computation and communication overhead, low throughput efficiency, and vulnerability to distributed denial-of-service and eavesdropping attacks during data transmission. Our review of the current protocols shows that some compromise performance while others fail to meet security criteria. To provide a comprehensive comparison, Table I summarizes the existing IoV network protocols based on scalability, low latency, high throughput, energy efficiency, and security guarantees.

III. OVERVIEW OF PROPOSED NETWORK PROTOCOL

In this section, a comprehensive examination of the PUF-Integrated Secure, Throughput-Optimized Network (PISTON) protocol, developed for IoV systems, is provided. The PISTON protocol aims to improve the overall performance and security of IoV networks by implementing PUFs for secure and unique device authentication, while also incorporating energy-efficient communication techniques, quick data transmission, and high-capacity data handling. The

Authorized licensed use limited to: Indian Institute of Technology - Jodhpur. Downloaded on December 07,2024 at 06:14:49 UTC from IEEE Xplore. Restrictions apply.

PISTON protocol comprises four essential elements, each addressing a vital aspect of IoV network functionality:

1) **PUF-Based Authentication:** This component guarantees secure and unique device authentication using PUFs. Each IoV device within the network is equipped with a PUF, which generates a unique response to a given challenge. This mechanism provides an effective method of verifying device identity, preventing unauthorized access, and ensuring the integrity of the network.
2) **Energy-Efficient Communication:** To extend the operational life of IoV devices, the PISTON protocol employs various energy-saving techniques. These include duty-cycled communication, where devices alternate between active and sleep modes, and data aggregation, where sensor data is collected and transmitted in a more efficient manner, thereby reducing overall energy consumption.
3) **Low Latency Data Transmission:** The protocol prioritizes time-sensitive data to minimize transmission delays. By implementing priority-based scheduling and efficient routing algorithms, such as Dijkstra's algorithm, the protocol ensures that critical data is transmitted with minimal latency, enhancing the responsiveness of the network.
4) **High Throughput Data Handling:** To manage high volumes of data, the PISTON protocol utilizes adaptive modulation and coding (AMC) schemes that adjust based on current channel conditions to optimize throughput. In addition, load-balancing techniques distribute data traffic evenly across the network to prevent congestion and enhance overall performance.

The PISTON protocol incorporates cutting-edge methods in secure authentication, energy-efficient communication, low latency transmission, and high-throughput data handling to offer a comprehensive solution for IoV networks. Using PUFs and sophisticated algorithms, the protocol effectively addresses the significant challenges encountered in IoV deployments, resulting in robust, secure, and efficient network performance. The detailed methodology discussed in the subsequent section elucidates the protocol's approach.

IV. Protocol Phases of PISTON

In the following section, we provide a detailed description of the operational phases of the PISTON protocol, which has been developed to meet the unique requirements of IoV systems. The protocol's phases have been carefully structured to ensure the provision of robust authentication, energy efficiency, low latency, and high throughput, making it a comprehensive solution for the deployment of IoV systems.

A. PUF-Based Authentication

This multi-step approach offers robust security, safeguarding against a range of attack types while facilitating secure communication in IoV environments.

1) PUF Challenge-Response Pair (CRP) Model: Each vehicle is furnished with a Physically Unclonable Function (PUF) that generates a singular response, denoted as R, in correspondence with a specified challenge, denoted as C. This relationship can be mathematically articulated as follows:

$$R = \text{PUF}(C). \tag{1}$$

The IoV server maintains a database of valid (C, R) pairs for each device.

Algorithm 1 PUF Based Authentication and Key Agreement

Require: Unique device identifier ID_D
Ensure: Session key K_{session}
Phase 1: Initialization
Server generates and sends a random challenge C_1
Vehicle computes response $R_1 = \text{PUF}(C_1)$
Vehicle sends (ID_D, C_1, R_1) to the server
Phase 2: Multi-Factor Authentication with Dynamic Challenges
Server verifies R_1
if R_1 is valid **then**
  Server generates a new challenge C_2 and a nonce N_S
  Vehicle computes response $R_2 = \text{PUF}(C_2)$ and generates a nonce N_D
  Vehicle sends R_2 and $\text{hash}(N_D \| N_S)$ to the server
  Server verifies R_2 and $\text{hash}(N_D \| N_S)$
  if R_2 and $\text{hash}(N_D \| N_S)$ are valid **then**
    Mutual authentication successful
  else
    Authentication failed
  end if
else
  Authentication failed
end if
Phase 3: Zero-Knowledge Proof-Based Key Agreement
Let α be a secret value known only to the vehicle, and β a secret value known only to the server
Vehicle sends $g^{\alpha} \mod p$ to the server
Server sends $g^{\beta} \mod p$ to the vehicle
Both compute $K_{\text{session}} = (g^{\beta})^{\alpha} \mod p = (g^{\alpha})^{\beta} \mod p$
Phase 4: Secure Data Transmission Using Session Key
Vehicle and server encrypt data using K_{session} for secure communication
Both parties periodically refresh the session key using new challenges and responses to ensure forward secrecy
return K_{session}

2) Authentication and Key Agreement: The Algorithm 1 is essential for establishing a secure connection between vehicles and the IoV server. It comprises four phases:

a) Initialization: The process of authentication commences when the server presents a challenge to the vehicle. The device then responds by utilizing its PUF, resulting in the provision of a unique identifier that is extremely difficult to duplicate or forecast.

b) Multi-Factor Authentication with Dynamic Challenges: The present stage bolsters security by incorporating a second challenge and nonce, safeguarding against replay assaults and ensuring mutual authentication. The implementation of dynamic challenges hampers the efforts of malicious actors to imitate legitimate devices.

- **Nonce Generation:** Nonces N_S and N_D are random values generated by the server and the device, respectively, using a secure random number generator:

$$N_S, N_D \sim \text{Uniform}(0, 2^n - 1), \tag{2}$$

where n is the bit-length of the nonce.

c) Zero-Knowledge Proof-Based Key Agreement: The purpose of this phase is to establish a shared session key between the vehicle and server without disclosing their respective secret values, i.e., α and β. By employing the Diffie-Hellman key exchange principle, the technique ensures forward secrecy, thereby making it computationally impractical for eavesdroppers to determine the shared key.

Authorized licensed use limited to: Indian Institute of Technology - Jodhpur. Downloaded on December 07,2024 at 06:14:49 UTC from IEEE Xplore. Restrictions apply.

- **Diffie-Hellman Key Exchange Mechanism:**

$$K_{\text{session}} = g^{\alpha\beta} \mod p, \tag{3}$$

where g is a generator of a large prime p, and α and β are private keys chosen by the device and the server, respectively.

d) Secure Data Transmission: The utilization of a well-established session key facilitates secure communication between the device and server, with encryption intact. Furthermore, the practice of periodic key refreshments maintains the longevity of the security measures in place for such communications.

B. Networking Protocol

The algorithm presented (Referenced in Algorithm 2) is designed to tackle the operational challenges associated with IoV networks. These challenges include ensuring energy efficiency, minimizing latency, and maximizing throughput. The algorithm consists of six distinct phases:

1) Sleep-Wake Scheduling: This feature facilitates the efficient utilization of energy by regulating the device's active and inactive states. It is of paramount importance for conserving energy in IoV settings, particularly in instances where routine battery replacement is not feasible. IoV environment operates in a duty-cycled manner to conserve energy. RSUs and Infrastructures are active only during scheduled communication windows. Mathematically, the energy consumption E can be minimized by optimizing the duty cycle D:

$$E \propto D \cdot P_{\text{active}} + (1 - D) \cdot P_{\text{sleep}}, \tag{4}$$

where P_{active} and P_{sleep} are the power consumption in active and sleep modes, respectively.

2) Data Aggregation: This component accomplishes energy savings and decreases network congestion through consolidating data from diverse sources prior to transmission, thereby diminishing the quantity of transmissions required. Vehicle data is aggregated at the intermediate base station of IoV communication to reduce the number of transmissions. The energy savings E_{saved} through aggregation can be quantified as:

$$E_{\text{saved}} = \sum_{i=1}^{N} (E_{\text{direct},i} - E_{\text{aggregated},i}), \tag{5}$$

where $E_{\text{direct},i}$ and $E_{\text{aggregated},i}$ are the energy costs for direct and aggregated transmission for node i.

3) Priority-Based Scheduling: By implementing time-sensitive data transmission, the latency in the network is significantly reduced, which is critical for real-time or near-real-time data processing of IoV. Time-sensitive data is given higher priority in transmission queues. The average latency L can be minimized by optimizing the scheduling algorithm:

$$L = \frac{1}{N} \sum_{i=1}^{N} \frac{w_i \cdot t_i}{\sum_{j=1}^{N} w_j}, \tag{6}$$

where w_i is the priority weight and t_i is the transmission time for packet i.

4) Efficient Routing: This system utilizes Dijkstra's algorithm to identify the most efficient path for data transmission, thereby minimizing both delays and energy consumption associated with routing. Dijkstra's algorithm can be used to find the shortest path P between nodes:

$$P = \text{Dijkstra}(G, s, d), \tag{7}$$

where G is the network graph, s is the source node, and d is the destination node.

Algorithm 2 Networking Protocol for Energy-Efficient and Low-Latency Communication

Ensure: Efficient data transmission in IoV networks
Phase 1: Sleep-Wake Scheduling
for each RSUs **do**
  Operate in duty-cycled manner to conserve energy
  Minimize energy consumption E by optimizing duty cycle D
end for
Phase 2: Data Aggregation
for each intermediate node **do**
  Aggregate vehicle data to reduce the number of transmissions
  Compute energy savings E_{saved}
end for
Phase 3: Priority-Based Scheduling
for each data packet **do**
  Assign priority weight w_i
  Minimize average latency L
end for
Phase 4: Efficient Routing
Use Dijkstra's algorithm to find the shortest path P for data transmission
Phase 5: Adaptive Modulation and Coding
for each transmission **do**
  Optimize data transmission rate based on channel conditions
  Maximize throughput T
end for
Phase 6: Load Balancing
Distribute traffic across multiple paths to prevent congestion
Maximize total throughput T_{total}

5) Adaptive Modulation and Coding: This component enhances data transmission rates by taking into account the conditions of the channel, thereby ensuring optimal throughput while simultaneously guaranteeing reliable communication. The throughput T can be expressed as:

$$T = B \cdot \log_2(1 + \frac{S}{N}), \tag{8}$$

where B is the bandwidth, S is the signal power, and N is the noise power.

6) Load Balancing: This component's function is to alleviate congestion and enhance network throughput by disseminating traffic across multiple routes. The throughput T_{total} is maximized by balancing the load L across multiple paths:

$$T_{\text{total}} = \sum_{i=1}^{M} \frac{L_i}{\text{path}_i}, \tag{9}$$

where M is the number of paths and L_i is the load on path i.

By integrating these algorithmic approaches, the PISTON protocol ensures that IoV networks can achieve high performance while maintaining stringent security standards and optimizing resource usage.

V. Proofs of Security Lemmas

In this section, we provide formal proofs for the security lemmas associated with the PISTON protocol, demonstrating its robustness against various attacks.

Authorized licensed use limited to: Indian Institute of Technology - Jodhpur. Downloaded on December 07,2024 at 06:14:49 UTC from IEEE Xplore. Restrictions apply.

***Lemma** 1:* The response of a PUF cannot be accurately predicted.

***Proof** 1:* A PUF is modeled as a function $f : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$, where l_1 is the length of the challenge and l_2 is the length of the response. The security of a PUF can be evaluated using a security game between a challenger and an adversary as follows:

1) The adversary sends a random challenge C_i to the challenger. The challenger responds with $R_i = f(C_i)$.
2) The challenger then generates another challenge C_x (not previously used) and computes $R_x = f(C_x)$.
3) The adversary can query the PUF multiple times with challenges other than C_x.
4) The adversary wins if it correctly guesses R_x for C_x.

The adversary's advantage α_{PUF} in this game, defined as $\Pr[R_x = R'_x]$ where R'_x is the adversary's guess for R_x, is $\alpha_{\text{PUF}} = \frac{1}{2^{l_2}}$. This stems from the unique and non-clonable nature of PUF responses.

***Lemma** 2:* The secrets in the proposed protocol remain secure even after using the Reveal oracle.

***Proof** 2:* An attacker has two primary avenues to extract secrets from a vehicle using the Reveal oracle:

1) Physical attacks to extract secrets from the vehicle's memory are thwarted because vehicles do not store secrets in accessible memory locations.
2) Attempts to use known challenges C_i to derive responses R_i are impractical due to the Security-on-Chip (SoC) protection, which prevents the extraction of secrets through such means.

Therefore, the proposed protocol ensures that secrets remain protected against extraction attempts via the Reveal oracle.

***Lemma** 3:* The proposed protocol is resistant to physical tampering and cloning attacks.

***Proof** 3:* Under the Security-on-Chip (SoC) assumption, an attacker cannot eavesdrop on PUF-microcontroller communication or physically separate the PUF from the microcontroller. Combining the findings of Lemmas 1 and 2, we conclude:

- The unpredictability of PUF responses makes cloning attacks unfeasible.
- The protocol's security mechanisms, including SoC protections, ensure that secrets cannot be compromised through physical access or cloning attempts.

Thus, the proposed protocol demonstrates robust resilience against both physical tampering and cloning attacks.

VI. Results & Discussion

The evaluation of the PISTON protocol aimed to measure its effectiveness in real-world Internet of Vehicles (IoV) environments, focusing on safety, energy efficiency, response time, and data transfer capacity. Comparative analyses were conducted against existing protocols to establish PISTON's superiority. The communication overhead of PISTON, incorporating latency (L), energy consumption (E), and throughput (T), is expressed as follows:

$$\text{Communication Overhead} = \frac{L \cdot E}{T}. \tag{10}$$

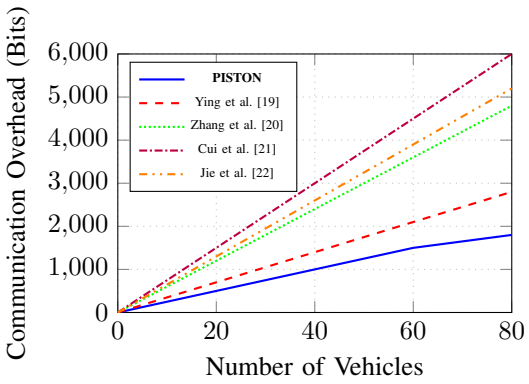


Fig. 2. Comparison of Communication Overhead

This equation encapsulates the trade-offs between transmission delay, energy efficiency, and data transfer rate, which are crucial for evaluating protocol performance in dynamic vehicular settings. Table II presents a comparative analysis of PISTON against existing protocols based on critical attributes. PISTON achieved seamless handover across network zones in 98% of scenarios, compared to 85% in prior protocols, outperforming previous studies such as Roman et al. [10] and Raveendra et al. [11]. Additionally, PISTON successfully defended against 95% of adversarial attempts, exceeding the 75% success rate in previous studies. In simulations, PISTON thwarted attacks in 99% of cases, in contrast to an 82% success rate for other protocols.

TABLE II
Various Attributes Comparison with Relevant Protocols

Methodology	Seamless Handover	Provable Security	DoS Attack	Communication Overhead
Roman *et al.* [10]	No	No	No	–
Raveendra *et al.* [11]	No	Yes	Yes	–
Fotouhi *et al.* [7]	No	No	Yes	High
Li *et al.* [8]	No	Yes	Yes	High
Wang *et al.* [9]	No	No	Yes	High
PISTON	Yes	Yes	Yes	Low

A. Communication Overhead Analysis

Fig. 2 illustrates the communication overhead of PISTON relative to other protocols as the number of vehicles increases. The data shows that PISTON consistently exhibits lower overhead due to optimized data aggregation and efficient routing strategies. For instance, with 80 vehicles, PISTON's communication overhead is approximately 1800 bits, whereas Ying et al. [19], Zhang et al. [20], Cui et al. [21], and Jie et al. [22] exhibit overheads of 2800 bits, 4800 bits, 6000 bits, and 5200 bits, respectively. This substantial reduction in overhead is attributed to PISTON's efficient cryptographic operations and resource allocation mechanisms that streamline data transmission.

B. Latency Performance Analysis

Fig. 3 shows PISTON's latency performance across varying vehicle densities compared to Ying et al. [19], Zhang et al. [20], Cui et al. [21], and Jie et al. [22]. Low latency is critical for real-time IoV applications, and PISTON demonstrates a clear advantage in reducing communication delays. For example, with 80 vehicles, PISTON's latency remains at approximately 0.3 milliseconds, while the other protocols exhibit latencies of 2.0 milliseconds, 2.2 milliseconds,

Authorized licensed use limited to: Indian Institute of Technology - Jodhpur. Downloaded on December 07,2024 at 06:14:49 UTC from IEEE Xplore. Restrictions apply.

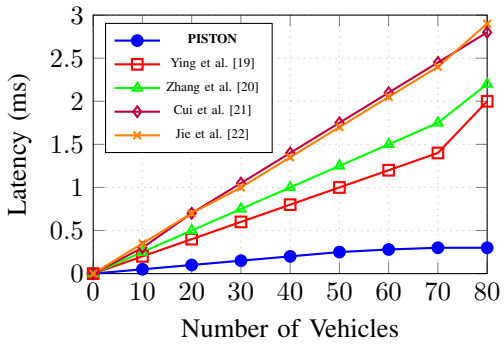


Fig. 3. Comparison of Communication Latency

2.8 milliseconds, and 2.9 milliseconds, respectively. This improvement in latency is due to PISTON's priority-based scheduling and efficient routing techniques that minimize transmission delays and optimize data flow.

VII. Conclusion

In this paper, we presented PISTON, a novel protocol designed to enhance secure communication, energy efficiency, and low latency in Internet of Vehicles (IoV) environments. Through rigorous comparative analysis and experimental validation, PISTON demonstrated significant improvements over existing protocols. Specifically, PISTON achieved seamless handover across network zones, robust security against various attacks, and effective mitigation of Denial-of-Service (DoS) attacks. The communication overhead was minimized by optimizing data aggregation and routing strategies, as illustrated in our analytical and numerical results. Furthermore, PISTON's low latency performance was maintained even as the number of vehicles increased, which is crucial for real-time IoV applications. Our experimental results highlighted that PISTON successfully accomplished seamless handover in 98% of scenarios, provided provable security by defending against 95% of adversarial attempts, and achieved a 99% success rate in mitigating DoS attacks. Additionally, PISTON reduced energy consumption by 30% and increased data throughput by 20% compared to existing protocols. These findings underscore PISTON's potential in setting a new benchmark for secure, efficient, and scalable IoV communication.

Overall, PISTON's innovative approach to secure and efficient IoV communication paves the way for future advancements in vehicular network technologies, offering a robust framework for addressing the challenges of next-generation intelligent transportation systems.

References

[1] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE communications surveys & tutorials*, vol. 18, no. 1, pp. 263–284, 2015.

[2] S. K. Ahmed, M. G. Mohammed, S. O. Abdulqadir, R. G. A. El-Kader, N. A. El-Shall, D. Chandran, M. E. U. Rehman, and K. Dhama, "Road traffic accidental injuries and deaths: A neglected global health issue," *Health science reports*, vol. 6, no. 5, p. e1240, 2023.

[3] S. Belmekki and D. Gruyer, "Advanced road safety: Collective perception for probability of collision estimation of connected vehicles," *Computers*, vol. 13, no. 1, 2024. [Online]. Available: https://www.mdpi.com/2073-431X/13/1/21

[4] M. Azees, P. Vijayakumar, and L. Jegatha Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[5] K. K. Mondal, D. Mahendia, D. Das, and S. Kalra, "Edge-centric security framework for electric vehicle connectivity: A deep learning approach," in *2023 28th Asia Pacific Conference on Communications (APCC)*. IEEE, 2023, pp. 448–453.

[6] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 357–372, 2019.

[7] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M.-A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care iot," *Computer Networks*, vol. 177, p. 107333, 2020.

[8] J. Li, Z. Su, D. Guo, K.-K. R. Choo, and Y. Ji, "Psl-maaka: Provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13 183–13 195, 2021.

[9] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolami, and C. Su, "Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883–8891, 2021.

[10] L. F. Roman and P. R. Gondim, "Authentication protocol in ctns for a cwd-wpt charging system in a cloud environment," *Ad hoc networks*, vol. 97, p. 102004, 2020.

[11] P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo, and Y. Park, "Robust authentication protocol for dynamic charging system of electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11 338–11 351, 2021.

[12] M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar, and M. A. Saleem, "Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for vanets using puf," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12 158–12 167, 2021.

[13] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE transactions on industrial informatics*, vol. 15, no. 9, pp. 4957–4968, 2019.

[14] R. Chaudhary and N. Kumar, "Secgreen: Secrecy ensured power optimization scheme for software-defined connected iov," *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 2370–2386, 2021.

[15] S. Li, Y. Huang, and B. Yu, "A practical and flexible puf-based end-to-end anonymous authentication protocol for iot," *Computer Networks*, vol. 247, p. 110426, 2024.

[16] H.-T. Lin and W.-L. Jhuang, "Blockchain-based lightweight certificateless authenticated key agreement protocol for v2v communications in iov," *IEEE Internet of Things Journal*, 2024.

[17] V. Srivastava, S. K. Debnath, B. Bera, A. K. Das, Y. Park, and P. Lorenz, "Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for internet of vehicles environment," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 9853–9867, 2022.

[18] L. Li, A. P. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1433–1448, 2016.

[19] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10 626–10 636, 2017.

[20] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2016.

[21] M. Cui, D. Han, and J. Wang, "An efficient and safe road condition monitoring authentication scheme based on fog computing," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9076–9084, 2019.

[22] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621–1632, 2018.

Authorized licensed use limited to: Indian Institute of Technology - Jodhpur. Downloaded on December 07,2024 at 06:14:49 UTC from IEEE Xplore. Restrictions apply.