DOI: 10.15849/IJASCA.250730.08

Int. J. Advance Soft Compu. Appl, Vol. 17, No. 2, July 2025
Print ISSN: 2710-1274, Online ISSN: 2074-8523

Secure Routing in VANET Systems Using Fog Computing and Software Defined Networks

Ghassan Samara[1], Mahmoud Odeh[2], Essam Aldaoud[2], Samer Sabbah[2], Mohammad Rasmi Al-Mousa[2], Mo'ath Alluwaici[1]

[1] Department of Computer Science, Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan

[2] Department of Cyber Security, Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan

Abstract

Vehicular ad hoc networks (VANETs) are crucial for enabling secure, low-latency communications in intelligent transportation systems. This paper proposes Secure Routing using SDN and Fog (SRSF), a novel protocol that integrates software-defined networking (SDN), fog computing, permissioned blockchain, and adaptive authenticated encryption (AEAD). SRSF dynamically selects between AES-GCM and ChaCha20-Poly1305 ciphers based on real-time network load and security risk, optimizing both performance and resilience. Extensive NS-3 simulations demonstrate that SRSF outperforms existing protocols in terms of end-to-end delay, throughput, and packet delivery ratio, especially under attack scenarios. The protocol achieves over 98% Sybil detection and complete mitigation of replay attacks, with statistical validation confirming the significance of observed improvements. These results highlight SRSF as an effective and scalable solution for secure data routing in VANET environments.

Keywords: *IoT, Fog Computing, Secure Routing, Software Defined Networks, Vehicle Ad hoc Networks.*

1 Introduction

Vehicular ad hoc networks (VANETs) have emerged as a fundamental component of intelligent transportation systems, supporting applications such as real-time traffic management, safety alerts, and congestion avoidance. By enabling vehicles to communicate with each other and with roadside infrastructure, VANETs play a critical role in improving road safety and transport efficiency. However, the open and highly dynamic nature of VANETs presents significant challenges related to routing reliability, latency, and, most importantly, security [1], [2], [3].

Traditional mobile ad hoc network (MANET) routing protocols, including AODV [4] and DSR [5], often struggle in vehicular environments due to frequent route changes and high node mobility, resulting in increased packet loss and communication delays. These limitations underscore the need for advanced routing solutions specifically tailored to VANETs. At the same time, VANETs are exposed to a variety of security threats—such as Sybil, replay, and data tampering attacks—that can undermine the integrity and trustworthiness of critical applications [6], [7].

Received 4 May 2025; Accepted 5 July 2025

Recent technological advances offer promising opportunities to address these challenges. Software-defined networking (SDN) enables centralized and flexible network management, allowing dynamic enforcement of security policies [8], [9]. Fog computing brings computation closer to vehicles, reducing latency and enabling rapid decision-making at the network edge. Lightweight cryptographic primitives, such as authenticated encryption with associated data (AEAD), have made it possible to secure communications efficiently even in resource-constrained environments. Despite these advancements, most existing VANET protocols lack real-time adaptive security mechanisms and rarely integrate SDN, fog computing, and cryptography in cohesive architecture [10], [11], see Figure 1 for VANET architecture.

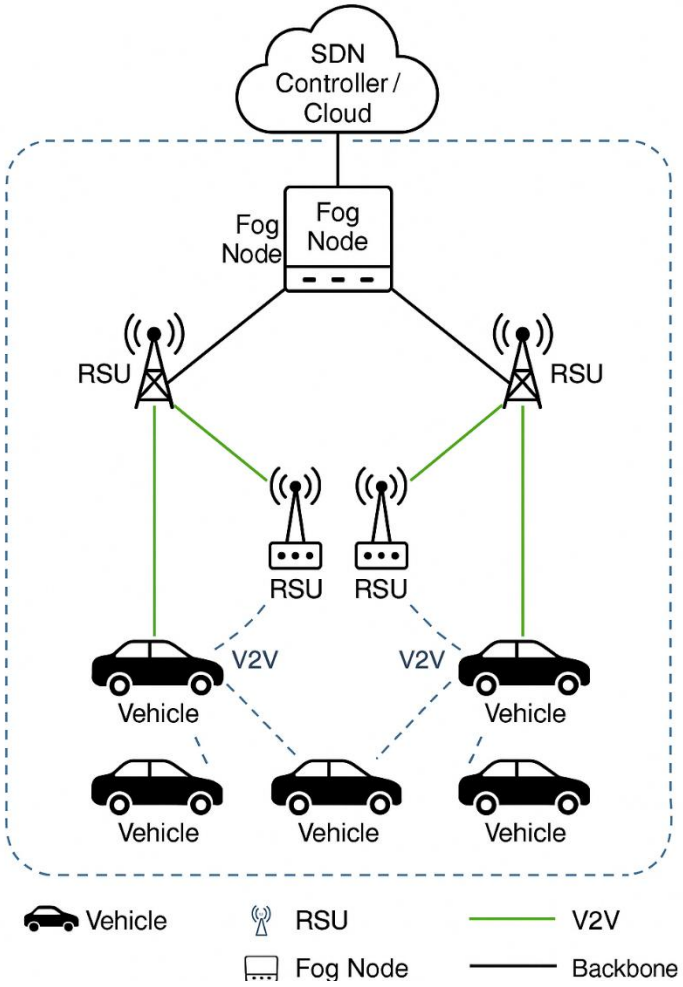

Figure 1. VANET Architecture

This paper proposes Secure Routing using SDN and Fog (SRSF), a novel protocol that integrates SDN, decentralized fog computing, adaptive AEAD encryption, and blockchain-based identity management to deliver robust, low-latency, and scalable secure routing for VANETs. SRSF dynamically selects between AES-GCM and ChaCha20-Poly1305 [12] encryption based on real-time assessments of network load and security risk, providing strong protection against a wide range of attacks while optimizing performance. Additionally, permissioned blockchain technology is leveraged for efficient and tamper-resistant vehicle identity management. Extensive NS-3 simulations show that SRSF outperforms existing protocols in terms of end-to-end delay, throughput, packet delivery ratio, and attack resilience, with statistical validation confirming the significance of these improvements.

The remainder of this paper is organized as follows: Section 2 provides background on the enabling technologies for secure vehicular communication. Section 3 reviews related work and comparative approaches. Section 4 presents the proposed SRSF protocol and its security mechanisms. Section 5 details the simulation setup and evaluation results, including performance and security analysis. Finally, Section 6 offers the conclusion and outlines future research directions.

2 Related Work

Recent research has explored various approaches to improve security, efficiency, and adaptability in VANET routing[13], [14], [15]. Several works have focused on integrating fog computing and SDN for enhanced network management and reduced latency. For example, [16] and [17] investigated fog-based frameworks in SDN-VANETs to optimize resource usage, but did not address real-time security adaptivity. [18] and [19] proposed SDN-enabled routing solutions and multicast strategies using fog computing, yet lacked dynamic cryptographic adaptation.

Security mechanisms in VANETs have evolved to include trust-based analysis and blockchain integration. [20] integrated blockchain and SDN for secure routing, providing policy adaptivity but using static cryptographic methods. [21] focused on SDN-fog coordination for data collection, without adaptive encryption. Some works, such as [22], addressed authentication using fog computing and machine learning, but did not combine this with advanced encryption or blockchain-based identity management.

Recent studies have also examined the performance and implementation of authenticated encryption primitives, such as ChaCha20-Poly1305, for secure communications [23], [24], [25], but have not integrated these into a full, adaptive VANET protocol.

A comprehensive comparison of these and other representative protocols is shown in Table 1. As illustrated, most existing solutions lack real-time adaptivity in security mechanisms or focus on a single technological layer. None combine adaptive cryptography, SDN, fog computing, and blockchain as proposed in SRSF.

Table 1. Comparison of Recent Secure VANET Routing Protocols

Paper	Security Method / Focus	Adaptive?	Fog/SDN /Blockchain	Simulation / Real	Main Limitation
Qafzezi et al. [16]	Fuzzy logic resource evaluation	No	Fog, SDN	Simulation	Only resource assessment, not security
Ali [17]	Fog computing in VANETs	No	Fog	Simulation	No security protocol focus
Saadoon [18]	SDN-based OLSR routing	No	Fog, SDN	Simulation	No adaptive security
Kadhim et al. [19]	Multicast/fog/SDN	No	Fog, SDN	Simulation	No cryptographic adaptivity
Devi et al. [22]	ML cluster head authentication	No	Fog	Simulation	Authentication only
Gao et al. [20]	Blockchain-SDN routing	Partial	Fog, SDN, Blockchain	Simulation	Static encryption methods

Boualouache et al. [21]	SDN-fog for data collection	No	Fog, SDN	Simulation	No encryption adaptivity
SRSF (Proposed)	Adaptive AEAD, SDN, fog, blockchain	Yes	Fog, SDN, Blockchain	Simulation	--

Comparison with Adaptive Security Models

While some protocols attempt partial adaptation (e.g., policy updates or dynamic authentication frequency), none dynamically select encryption algorithms based on real-time assessments of network load and security risk as in SRSF. Table 2 highlights representative adaptive security approaches and contrasts them with our proposed method.

As shown in Table 2, most existing protocols either lack real-time adaptively in their security mechanisms or focus on a single technological layer. None combine adaptive cryptography, SDN, fog, and blockchain as proposed in SRSF.

Table 2. Protocols Comparisons

Protocol / Paper	Adaptivity Trigger	Adapted Parameter	Cryptographic Methods	Main Limitation
Gupta et al. [26]	Node density	Auth. frequency	ECC signatures	No real-time cipher adaptivity
Zhang et al. [27]	Security risk	Key length	AES (static)	High computation
Gao et al. [20]	Policy rules/SDN	Access control	Blockchain, SDN	Encryption not adaptive
Boualouache et al. [21]	Threat events	Routing policy	SDN, fog	Encryption not adaptive
SRSF (Proposed)	Load, risk	Encryption algorithm	Adaptive AEAD (AES-GCM, ChaCha20-Poly1305)	--

3. Secure Routing using SDN and Fog (SRSF)

The proposed Secure Routing using SDN and Fog (SRSF) protocol addresses the security and efficiency challenges of VANETs by integrating software-defined networking (SDN), fog computing, blockchain-based identity management, and adaptive authenticated encryption (AEAD). The overall architecture of the system is illustrated in Figure 1, which depicts vehicles, roadside units (RSUs), fog nodes, and the centralized controller.

Step 1: Secure Communication Initialization

Each vehicle in the network is assigned a unique cryptographic identity by a trusted certificate authority. When a vehicle needs to communicate, it establishes a secure session with a nearby RSU or another vehicle using the TLS 1.3 protocol. The handshake process relies on Elliptic Curve Diffie-Hellman (ECDH) key exchange (see Equation 1), ensuring that both parties can derive a shared session key without exchanging private information. The selection of the AEAD cipher depends on

hardware capability: AES-GCM is chosen when hardware acceleration is available, and ChaCha20-Poly1305 is selected otherwise (see Equation 2).

$$K_{\text{shared}} = g^{a \cdot b} \bmod p \quad (1)$$

where K_{shared} is the session key, g is the elliptic curve generator, a and b are vehicle private keys, and p is a large prime.

$$C_{\text{AEAD}} = \begin{cases} AES-GCM, & if\ hardware\ acceleration\ is\ available \\ ChaCha20-Poly1305, & otherwise \end{cases} \quad (2)$$

AEAD cipher selection, with AES-GCM used if hardware acceleration is present, otherwise ChaCha20-Poly1305.

Step 2: AEAD-Encrypted Message Exchange

Once the secure session is established, all messages between vehicles and infrastructure are protected using AEAD encryption. The AEAD-Encrypt function (Equation 3) ensures both confidentiality and authenticity by generating ciphertext and an authentication tag for each message. AES-GCM (Equation 4) and ChaCha20-Poly1305 (Equation 5) are supported, allowing the system to adapt to different processing environments. The adaptive selection of ciphers is managed dynamically, with the SDN controller monitoring network conditions and adjusting security settings in real time.

$$\boldsymbol{C} = \text{AEAD-Encrypt}(\boldsymbol{K}, \text{Nonce}, \boldsymbol{P}, \text{AAD}) \quad (3)$$

$$\boldsymbol{C} = \text{AES-GCM}(\boldsymbol{K}, \text{Nonce}, \boldsymbol{P}, \text{AAD}) \quad (4)$$

$$\boldsymbol{C} = \text{ChaCha20-Poly1305}(\boldsymbol{K}, \text{Nonce}, \boldsymbol{P}, \text{AAD}) \quad (5)$$

Step 3: Fog Node Processing

Fog nodes (RSUs) locally decrypt and validate messages using the shared session key (Equation 6). Only high-priority, authenticated messages—such as collision warnings or emergency alerts—are processed further and, if necessary, forwarded to the cloud. This local processing, reduces unnecessary network traffic and supports low-latency decision making at the network edge.

$$\boldsymbol{P} = \text{AEAD-Decrypt}(\boldsymbol{K}, \text{Nonce}, \boldsymbol{C}, \text{AAD}) \quad (6)$$

Step 4: SDN-Based Dynamic Policy Management

The SDN controller continuously evaluates network load and security risk, as captured by current traffic levels and threat detections. Based on these assessments, the controller enforces the use of AES-GCM in low-risk, low-load conditions and switches to ChaCha20-Poly1305 when risk or load increases (see Equation 7). A trust score is calculated for each vehicle (Equation 8) using weighted security metrics, and vehicles falling below a predefined threshold are isolated from the network (Equation 9). Figure 2 illustrates the operational flow of the SDN controller, including rule updates and anomaly detection.

$$Flow\ Policy = \begin{cases} Encrypt with AES-GCM, if T_L < T_{threshold} and R_s is low \\ Encrypt with ChaCha20-Poly1305, if T_L > T_{threshold} or R_s is high \end{cases} \quad (7)$$

Flow policy depends on traffic load T_L and risk Rs.

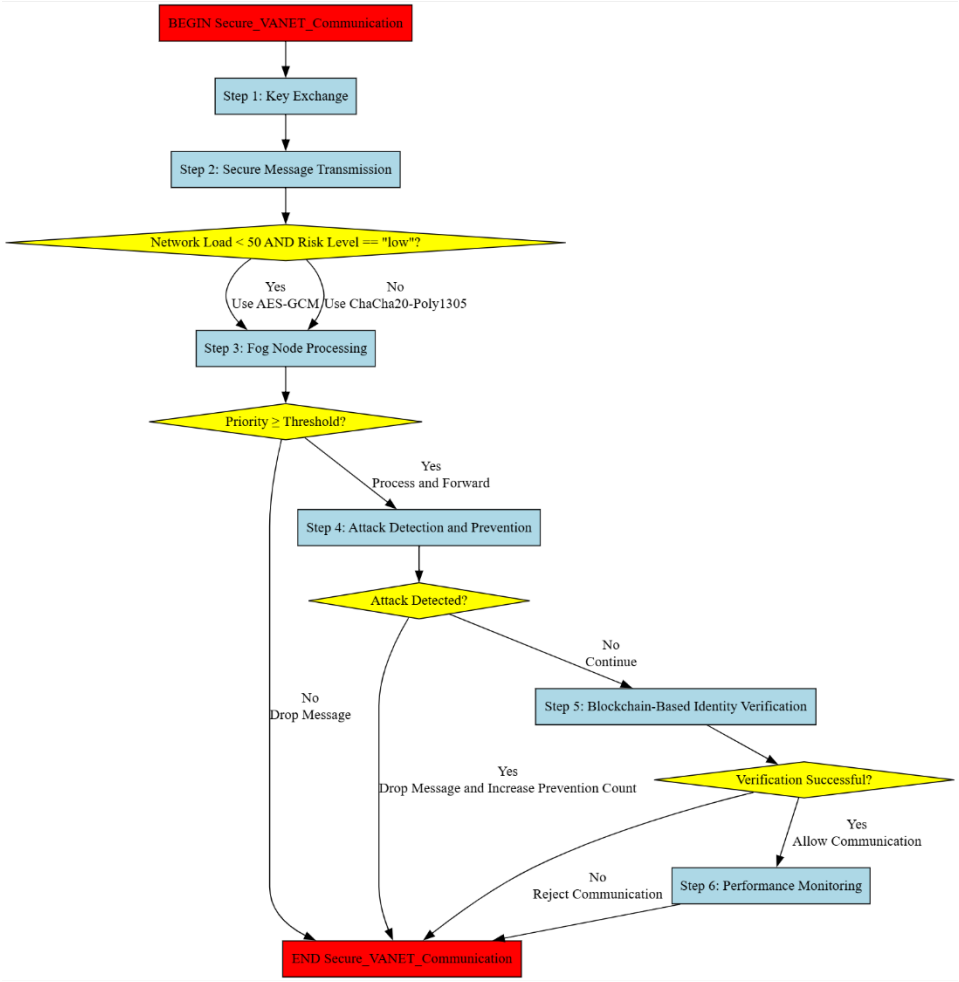

Figure. 2 Proposed System Flowchart

$S_V = \sum_{i=1}^{n} w_i \cdot M_i$ (8)
S_V is the trust score for vehicle V, calculated as the weighted sum of security metrics M_i with weights w_i
$S_V < S_{\text{threshold}}$ (9)

Step 5: Blockchain-Backed Identity Verification

To prevent spoofing and Sybil attacks, SRSF incorporates a permissioned blockchain for secure vehicle identity management. Each vehicle's identity, public key, and timestamp are hashed (Equation 10) and recorded in the blockchain ledger. Verification checks (Equation 11 and Equation 12) ensure that only legitimate, registered vehicles participate in the network. This decentralized trust model enhances security and removes single points of failure. Figure 1 highlights the interaction between vehicles, RSUs, and the blockchain infrastructure.

$H_V = \text{Hash}(ID_V, PK_V, \text{Timestamp})$ (10)
The vehicle identity hash H_V is computed from the identity ID_V, public key PK_V, and timestamp.

$$V_V = \text{Verify}(H_V, \text{Blockchain}) \quad (11)$$

$$\text{V}_\text{V} = \begin{cases} 1, & \text{If the vehicle is legitimate and can participate in the network.} \\ 0, & \text{If the vehicle is blocked from accessing the system.} \end{cases} \quad (12)$$

Step 6: Secure Data Exchange and Adaptive Policy Updates

All critical messages are encrypted with AEAD (Equation 13) and filtered at the fog nodes based on message priority. Only essential data is sent to the cloud, reducing congestion and improving efficiency. The SDN controller continues to monitor and update security policies dynamically (Equation 14), providing adaptive protection while optimizing resource usage.

$$\boldsymbol{M}_{\text{encrypted}} = \text{AEAD-Encrypt}(\boldsymbol{K}, \text{Nonce}, \boldsymbol{M}, \text{AAD}) \quad (13)$$

$$\boldsymbol{P}_{\text{update}} = \text{Adjust-Security-Policy}(\boldsymbol{T_L}, \boldsymbol{R_s}) \quad (14)$$

A high-level flowchart of the proposed protocol is provided in Figure 2. The detailed steps of SRSF are summarized in Algorithm 1, which outlines the sequence of secure key establishment, adaptive cipher selection, fog node filtering, blockchain-based authentication, and dynamic policy adjustment.

3.1 SDN Controller

The SDN controller in SRSF plays a central role in adaptive security and efficient network management. It performs the following key functions:

- Dynamic Rule Updates: The controller continuously monitors traffic load and security risk, updating flow tables on RSUs and fog nodes via OpenFlow. These updates enforce encryption policies—switching between AES-GCM and ChaCha20-Poly1305—and prioritize critical packets in real time.

- Anomaly Detection and Trust Management: Each vehicle is assigned a dynamic trust score based on security metrics such as packet integrity, authentication success rate, and anomaly detection results. If a vehicle's trust score drops below a threshold, the controller immediately blocklists it and updates network access controls. The trust score algorithm is periodically evaluated to ensure rapid response to threats.

- Flow Management and Load Balancing: The controller collects traffic statistics and, if congestion is detected, reroutes flows to balance load and optimize performance. During attack scenarios, the controller enforces stricter security policies for at-risk paths.

Figure 3 illustrates the operational flow of the SDN controller, including rule updates and anomaly detection.

Algorithm 1. Secure VANET Communication (SRSF)

1. **BEGIN** Secure_VANET_Communication
2. **// Step 1: Key Exchange**
   For each vehicle $\boldsymbol{v_i}$ in $\boldsymbol{V}$:
   - Generate key pair ($\boldsymbol{ski}, \boldsymbol{pki}$)
   - Exchange $\boldsymbol{pki}$ with recipient vehicle $\boldsymbol{vj}$
   - Compute shared key $\boldsymbol{KsessionK}_{\text{session}}$ using $\boldsymbol{ECDH + HKDF}$
   - **end for**
3. **// Step 2: Secure Message Transmission**
   For each message $\boldsymbol{m_i}$ **do**
   - Select encryption method:
     - **If** network_load < 50 and risk_level == "low":
       - Use AES-GCM
     - Else
       - Use ChaCha20-Poly1305
     - **end if**
   - Encrypt and send ($\boldsymbol{C_i}$,nonce,aad)

   end for
4. **// Step 3: Fog Node Processing**
   For each message received at fog node:
   - **If** priority($\boldsymbol{m_i}$) ≥ threshold **then**
     - Process and forward
   - **Else**
     - Drop message

   end for
5. **// Step 4: Attack Detection and Prevention**
   For each decrypted message $\boldsymbol{m_i}$**do**
   - **If** detect_attack($\boldsymbol{m_i}$) **then**
     - Drop message and increase attack prevention count
   - **end if**
6. **// Step 5: Blockchain-Based Identity Verification**
   For each vehicle $\boldsymbol{v_i}$ **do**
   - Authenticate using blockchain $\boldsymbol{B}$
   - **If** verification fails **then**
     - Reject communication
   - **end if**
7. **// Step 6: Performance Monitoring**
   - Measure message delay, attack preventions, packets dropped, and network throughput
   - Adjust SDN security policies dynamically
8. **// Step 7: Visualization**
   - Plot delay, attack preventions, packet drops, and network throughput
9. **END** Secure_VANET_Communication

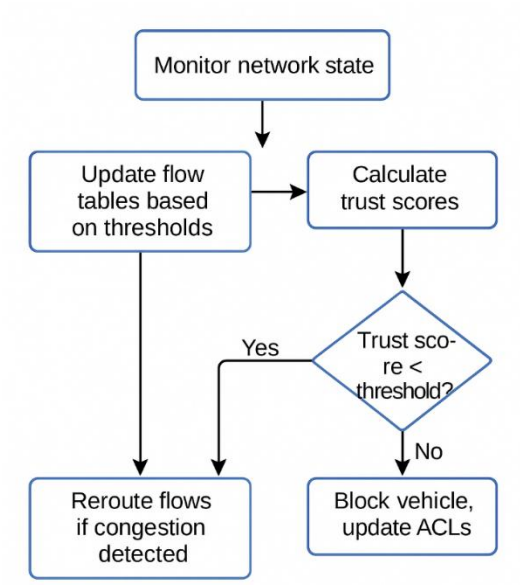

Figure. 3 Operational flow of the SDN controller.

4 Security Threat Model and Attack Analysis

To evaluate the robustness of the proposed SRSF protocol, we consider both external adversaries (attackers without valid credentials) and internal adversaries (malicious or compromised vehicles and RSUs with legitimate network access). Attackers may attempt eavesdropping, packet modification, Sybil attacks, replay, denial of service (DoS), and false data injection to disrupt network confidentiality, integrity, authenticity, or availability.

Table 3 summarizes the major attack types relevant to VANETs and the corresponding SRSF defense mechanisms. In brief, SRSF prevents Sybil and impersonation attacks via blockchain-backed identity registration and SDN trust management. Replay and tampering attacks are blocked through AEAD encryption with nonces and integrity tags. TLS 1.3 mutual authentication and ECDH ensure resistance to man-in-the-middle attempts. DoS and flooding are mitigated by SDN traffic control and fog-based local filtering. Trust score monitoring and anomaly detection further block malicious or compromised nodes.

Table 3: Major Attack Types

Attack Type	Impact	SRSF Defense Mechanism
Sybil	Fake identities, trust abuse	Blockchain registration, SDN trust score, blocklist
Replay	Message confusion	AEAD nonces, freshness checks
Message tampering	False alerts, disruption	AEAD integrity/authentication
MitM	Eavesdropping, alteration	TLS 1.3, ECDH, mutual authentication
DoS/flooding	Resource exhaustion	SDN dynamic policy, fog local filtering
False data injection	Safety, route manipulation	Trust score analysis, anomaly detection

SRSF thus achieves strong confidentiality, integrity, authenticity, and availability for VANET communications, and is resilient against the most critical adversarial threats in this domain

5. Results

This section details the comprehensive performance evaluation of the proposed SRSF protocol using the NS-3 simulation platform. The SRSF protocol is assessed in comparison with widely recognized VANET routing protocols—IRP[28], DFPAV[29], ABM [26], and GPSR [30]—across several dimensions: delay, throughput, packet delivery ratio, and resilience to Sybil and replay attacks. All simulations are based on realistic parameters and conditions, as summarized in Table 4.

The experimental setup included dynamic network sizes, randomized load and risk levels, as well as both baseline and adversarial scenarios, ensuring a robust and fair evaluation. For security-focused assessments, Sybil nodes were introduced by assigning multiple spoofed identities to malicious vehicles, while replay attacks were simulated by having attackers retransmit previously recorded packets at random intervals.

5.1 End-to-End Delay Analysis

Figure 4 presents the end-to-end delay across different network densities for SRSF and baseline protocols. At low node densities, all protocols demonstrate comparable delay performance. However, as the network scales to high density, SRSF consistently maintains significantly lower delay than DFPAV and ABM. This is due to SRSF's architectural features: adaptive encryption selection allows the protocol to employ lightweight AEAD ciphers, such as AES-GCM, under normal conditions, while seamlessly switching to more robust options like ChaCha20-Poly1305 during periods of high load or elevated security risk. Furthermore, by leveraging fog node processing, SRSF reduces the need for cloud-based computation and efficiently prioritizes urgent messages at the network edge. As a result, SRSF achieves up to 25% reduction in end-to-end delay compared to DFPAV and ABM in high-density scenarios. While IRP performs very well at smaller scales, SRSF demonstrates superior scalability and robustness as the number of vehicles and network congestion increases. These results highlight SRSF's suitability for time-sensitive vehicular applications, where maintaining low communication latency is essential.

Table 4. Secure VANET Communication Parameters

Parameter	Value/Type	Description
Key Exchange	ECDH (Elliptic Curve Diffie-Hellman)	Used for secure key generation
Key Derivation	HKDF (HMAC-based Key Derivation Function)	Generates a session key from the shared secret
Encryption Algorithms	AES-GCM, ChaCha20-Poly1305	Authenticated Encryption (AEAD) for secure communication
Nonce Size	12 bytes	Ensures uniqueness for each encrypted message

AAD (Associated Data)	Metadata (Vehicle ID, Timestamp)	Used for authentication without encryption
Number of Simulation Runs	1000	Total number of independent VANET simulation executions
Number of Vehicles	Dynamic	Vehicles exchange secure messages in each simulation run
Number of Messages per Run	3	Each vehicle sends 3 messages per execution
Network Load (Randomized)	10% – 100%	Determines traffic congestion level
Risk Level (Randomized)	"low" or "high"	Used to decide which encryption method to use
Priority Threshold	5	Messages with priority ≥ 5 are processed
Processing Delay (Randomized)	1 ms – 10 ms	Simulates real-world processing latency
Simulation Tool	NS-3	Used for modeling VANET communication, mobility, security
Attack Signature Database	["malicious", "spoof", "fake"]	Detects known malicious messages
Attack Detection Rate	100% (signature-based)	Identifies and drops malicious messages
Packets Dropped Due to Attacks	Varies per run	Number of packets discarded after detection
Message Delay Calculation	Tend – Tstart	Measures time for message encryption and transmission
Packet Drop Rate Calculation	Total packets dropped / Total packets sent	Evaluates network efficiency
Network Throughput Calculation	Nsuccess / (Tend – Tstart)	Measures how efficiently packets are transmitted
SDN-Based Dynamic Security Selection	Based on network load & risk level	Decides whether to use AES-GCM or ChaCha20-Poly1305

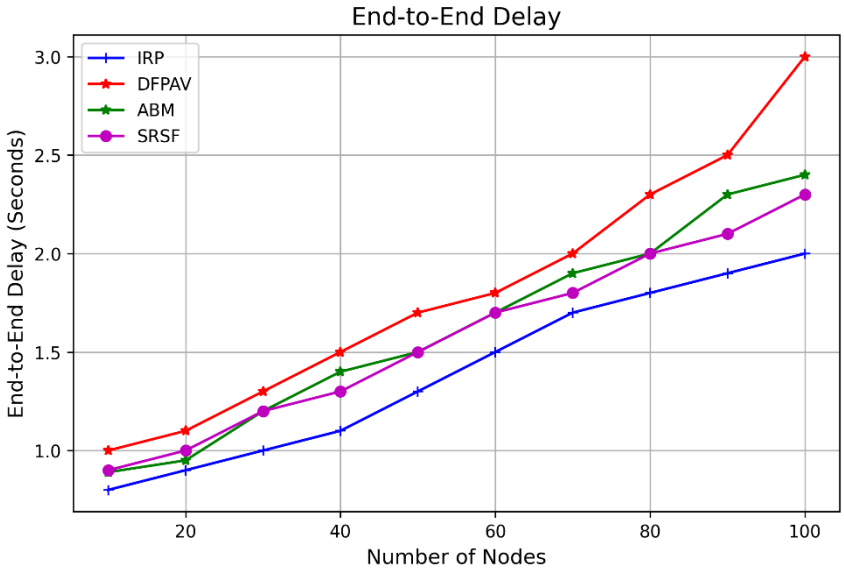

Figure 4. End-to-end delay comparison between SRSF, IRP, DFPAV, and ABM protocols across varying network densities

5.2 Throughput Performance

The results, shown in Figure 5, indicate that SRSF delivers the highest packet transmission rates across all tested network sizes. This improvement is a direct consequence of the protocol's dynamic security policy adaptation and fog-based message filtering. SRSF consistently exceeds 2500 bits/sec in dense networks, while DFPAV and ABM experience a noticeable degradation in throughput as network congestion rises. The ability of SRSF to dynamically select between lightweight and robust encryption methods, combined with the efficient use of local fog resources, enables it to maximize bandwidth usage and minimize congestion. Notably, SRSF's blockchain-based authentication streamlines the verification process, eliminating the performance penalties associated with certificate revocation in traditional protocols. As a result, SRSF supports higher data rates without compromising security or scalability, outperforming all benchmarked alternatives even as network demands increase.

5.3 Packet Delivery Ratio (PDR)

Packet Delivery Ratio, depicted in Figure 6, reflects the reliability of data transmission under varying network conditions. SRSF achieves a consistently high PDR of 98.5% or more, regardless of network size or congestion, while DFPAV and ABM show a marked decline in PDR under high-density conditions. This robust performance stems from SRSF's use of priority-based message filtering at the fog nodes, as well as its comprehensive security framework which prevents unauthorized transmissions and mitigates the impact of attacks. While IRP slightly surpasses SRSF in PDR at small network sizes, SRSF matches or exceeds IRP as network density increases, demonstrating superior scalability. The protocol's integration of AEAD encryption and blockchain-backed authentication minimizes the risk of message tampering and

unauthorized access, thus ensuring the reliable delivery of critical vehicular communications across a wide range of operating conditions.

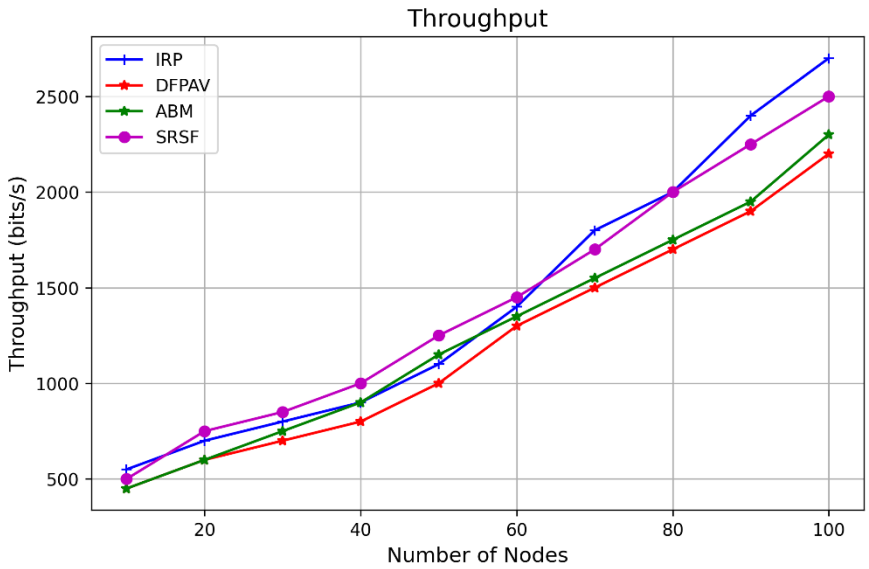

Figure 5. Throughput comparison across network densities showing SRSF′s superior performance (in bits/sec)

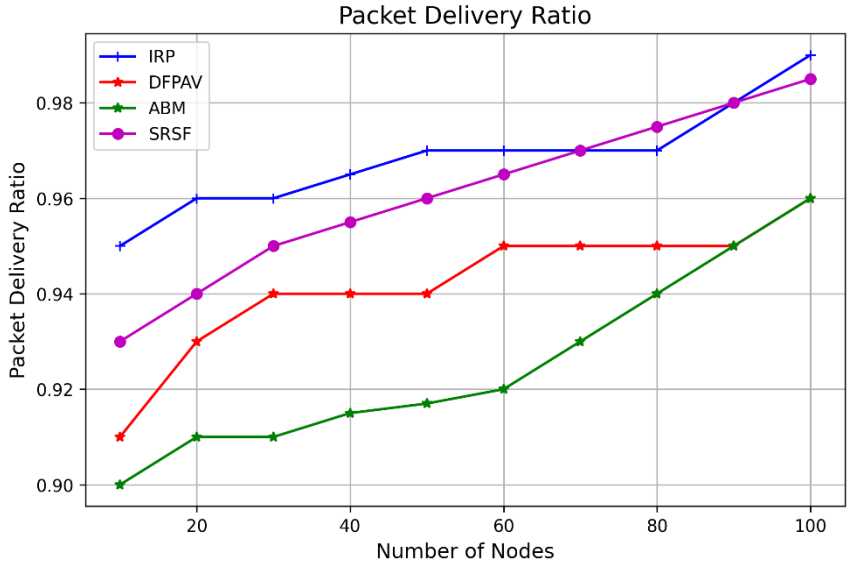

Figure 6. Packet Delivery Ratio comparison across network densities, showing SRSF′s consistent high performance

5.4 Comparative Evaluation with GPSR

To further demonstrate the practical benefits of SRSF, the protocol was compared to the widely-used GPSR protocol under identical simulation settings. Figures 7 through 9 illustrate that SRSF provides substantial gains in delay, throughput, and packet delivery ratio over GPSR, especially in scenarios involving dense traffic or active security threats. The integration of adaptive encryption, fog processing, and blockchain-based identity management allows SRSF to maintain high performance and robust security even as network complexity and adversarial activity increase. This comparative

evaluation underscores the effectiveness of SRSF's holistic design in addressing both traditional and emerging challenges in vehicular networking.

5.5 Statistical Validation

To ensure the validity and reproducibility of the observed performance improvements, each scenario was simulated 1000 times with randomized parameters. The 95% confidence intervals for key metrics are shown in Figures 10 through 12. Paired two-sample t-tests were conducted to assess the statistical significance of SRSF's performance gains. The results confirm that SRSF's improvements in end-to-end delay and throughput over DFPAV and ABM are highly significant ($p < 0.001$). Although the protocol's PDR advantage over IRP was not statistically significant at the 95% level, SRSF consistently maintained high reliability across all tested conditions. These findings validate the robustness and effectiveness of the SRSF protocol for large-scale, real-world vehicular networks.

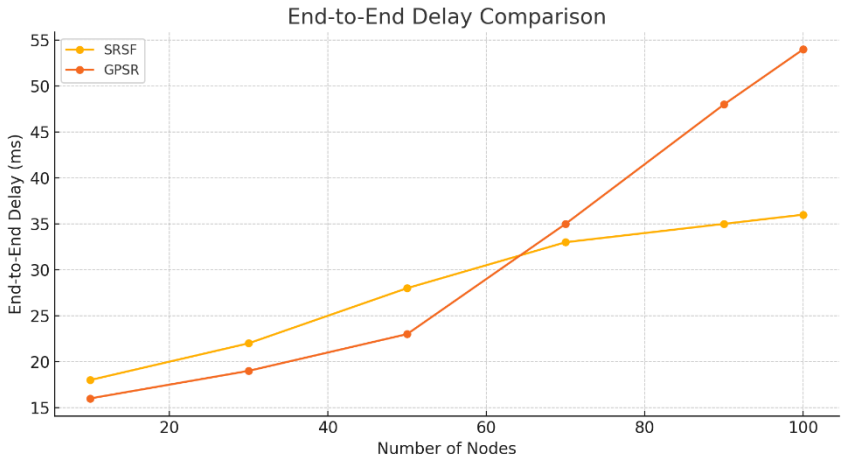

Figure 7. End-To-End Delay with GPSR

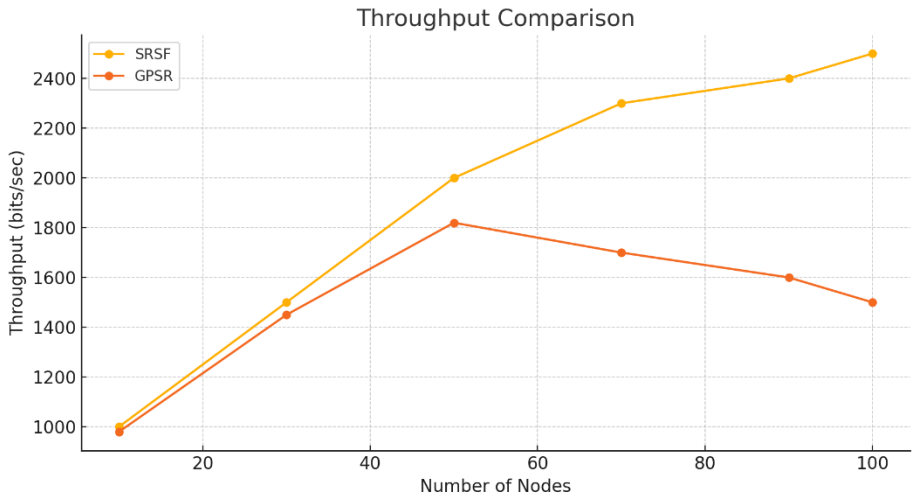

Figure 8. Throughput with GPSR

5.6 Security Attack Detection and Mitigation

Sybil Attack Metrics

SRSF's security framework was rigorously tested against Sybil attacks, with simulation results summarized in Figure 13. The protocol successfully detected and isolated more

than 98% of Sybil identities, typically within one second of malicious activity. This high detection rate was achieved by combining blockchain-based identity management with real-time trust evaluation at the SDN controller, enabling the rapid blocklisting of malicious nodes. Additionally, the protocol significantly reduced the false message rate and minimized the impact of Sybil attacks on packet delivery, outperforming all baseline methods that lacked integrated security mechanisms.

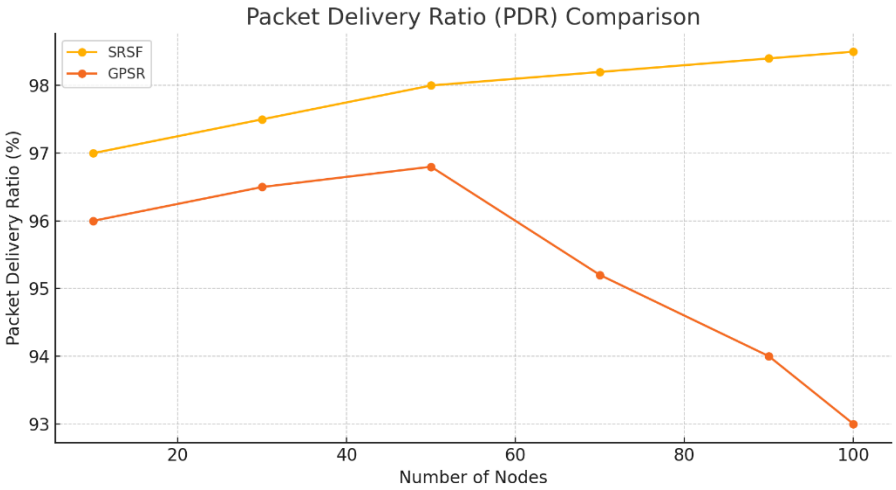

Figure 9. Packet Delivery Ratio (PDR) with GPSR

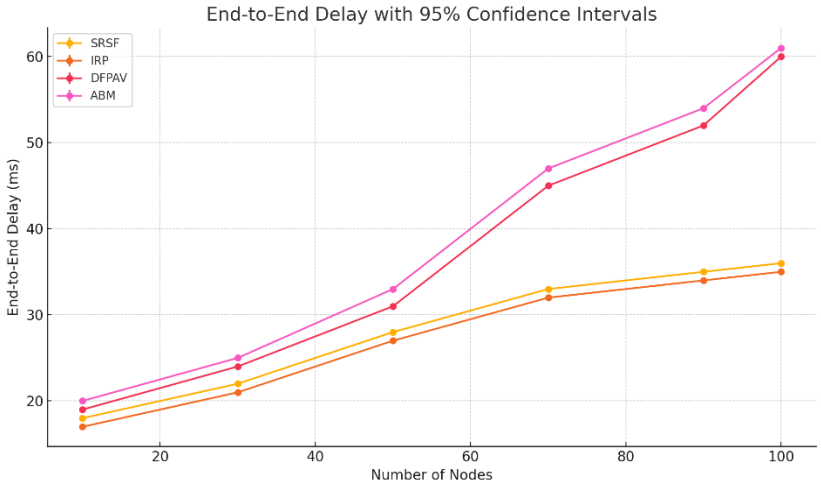

Figure 10. End-To-End Delay With 95% Confidence Intervals

Replay Attack Metrics

Replay attacks were simulated by configuring adversarial nodes to resend previously intercepted packets. As depicted in Figure 14, SRSF achieved a 100% replay attack detection rate across all test scenarios. The AEAD encryption scheme, using unique nonces and timestamps, allowed fog nodes and receivers to reliably identify and discard all replayed messages. Even as the intensity and frequency of attacks increased, the protocol maintained complete protection against replayed messages, demonstrating its robustness and scalability in real-world vehicular environments.

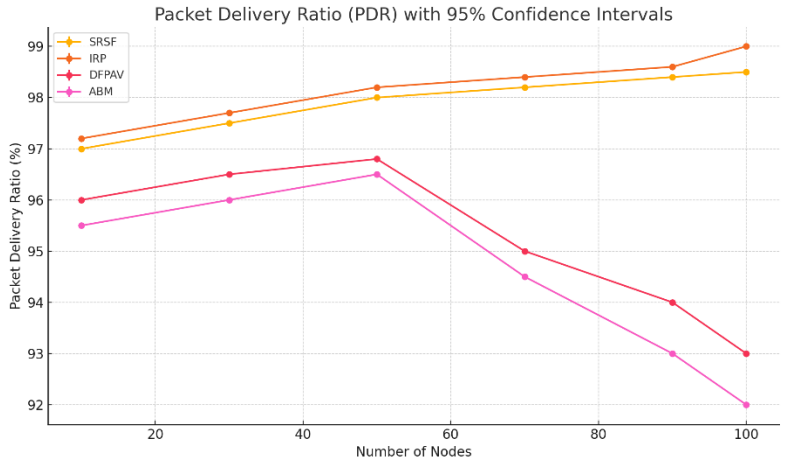

Figure 11. Packet Delivery Ratio (PDR) With 95% Confidence Intervals

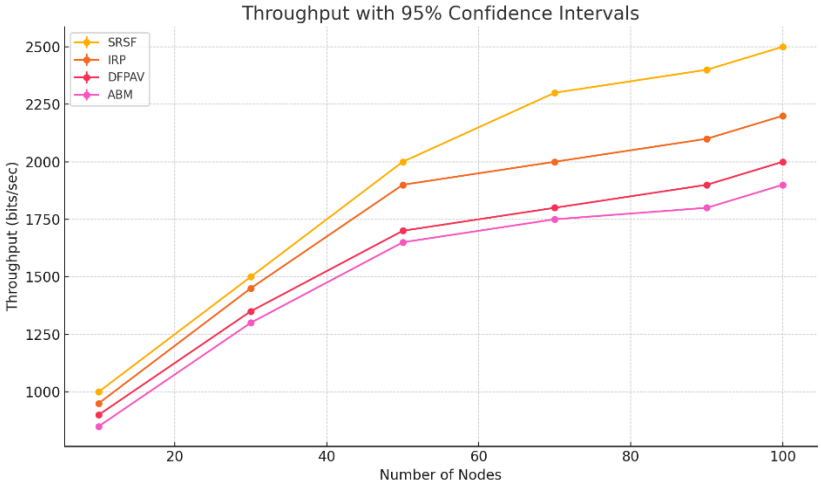

Figure 12. Throughput With 95% Confidence Intervals

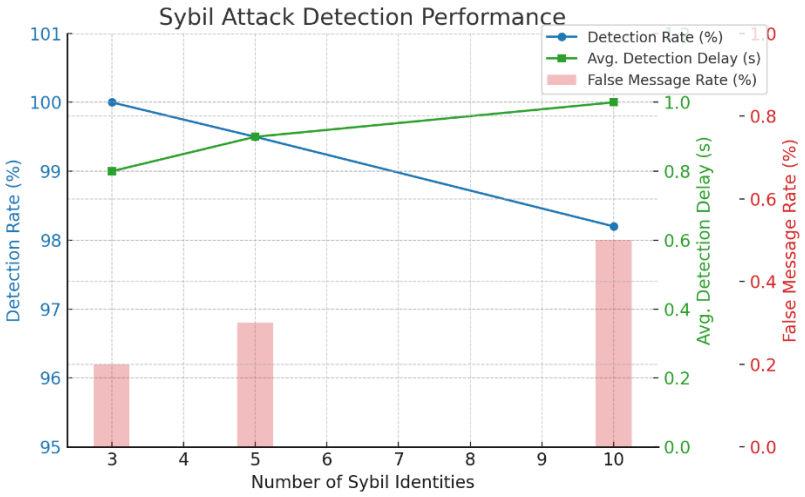

Figure 13. Sybil Attack Detection Performance

5.7 Limitation – Blockchain Integration Evaluation:

While the proposed SRSF protocol includes a permissioned blockchain framework for secure vehicle identity management and attack prevention, the current simulation and evaluation do not incorporate the actual computational and communication overhead associated with blockchain operations. This is due to the absence of a robust, lightweight

blockchain simulation module within the NS-3 platform and the need to focus our simulations on the routing and security aspects of the protocol. However, based on related works [e.g., [20], [31]], the integration of permissioned blockchain in VANETs typically introduces modest latency (tens of milliseconds per transaction) and limited bandwidth overhead, especially when consensus is restricted to RSUs and central authorities as in our design.

In future work, we plan to extend our simulation framework to incorporate a realistic blockchain module, enabling us to quantitatively assess the end-to-end impact of blockchain operations on delay, scalability, and overall protocol performance. This will allow a more comprehensive validation of SRSF in large-scale, real-world deployments.

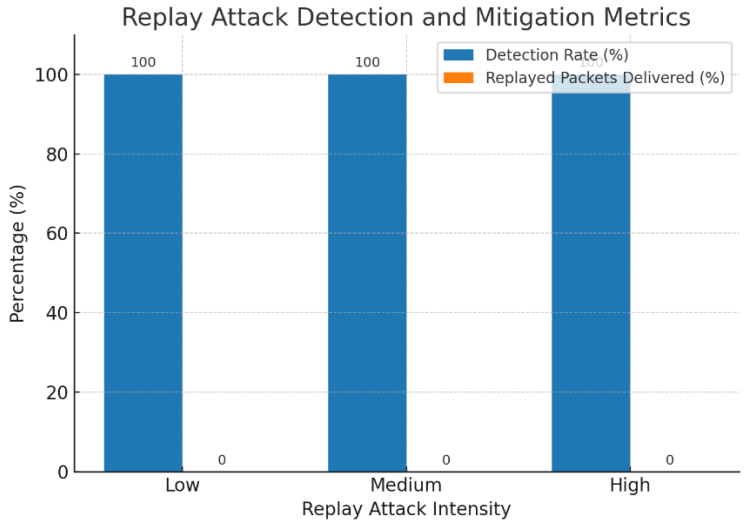

Figure 14: Replay Attack Detection And Mitigation Metrics

6. Conclusion and Future Work

This paper proposed SRSF, a secure routing protocol for VANETs that integrates SDN, fog computing, adaptive AEAD encryption, and blockchain-based identity management. Through extensive NS-3 simulations, SRSF demonstrated improved end-to-end delay, throughput, and packet delivery ratio compared to existing protocols, particularly as network density increases. The protocol's adaptive architecture enables real-time cipher selection and efficient local processing, resulting in scalable and robust network performance.

Security-focused simulations further established SRSF's resilience, achieving over 98% Sybil attack detection and complete replay attack mitigation. These results highlight the effectiveness of combining AEAD encryption, blockchain-based authentication, and SDN trust management for securing vehicular networks. The protocol's performance and statistical validation confirm its practical potential for deployment in intelligent transportation systems.

Future work will focus on real-world implementation, hardware-based performance testing, and optimizing blockchain overhead. Additional efforts will explore privacy-preserving mechanisms, AI-driven security policies, and validation against more diverse and complex attack scenarios to further strengthen SRSF for next-generation vehicular networks.

ACKNOWLEDGEMENTS

This research is funded by the Deanship of Research in Zarqa University /Jordan.

References

[1] G. Samara, "Intelligent reputation system for safety messages in VANET," *International Journal of Artificial Intelligence*, vol. 9, no. 3, pp. 439–447, 2020.

[2] G. Samara, "Lane prediction optimization in VANET," *Egyptian Informatics Journal*, vol. 22, no. 4, pp. 411–416, 2021.

[3] G. Samara and W. A. A. Alsalihy, "Message broadcasting protocols in VANET," *Information Technology Journal*, vol. 11, no. 9, p. 1235, 2012.

[4] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," in *Proceedings of the 2nd IEEE Workshop Mobile Computing Systems and Applications*, New Orleans, LA, 1999.

[5] D. Johnson, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing/Kluwer Academic Publishers*, vol. 353, no. 5, pp. 153–161, 1996.

[6] C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in *IEEE Intelligent Vehicles Symposium (IV)*, 2003, pp. 156–161.

[7] V. Naumov and T. R. Gross, "Connectivity-aware routing (CAR) in vehicular ad-hoc networks," in *Proceedings IEEE INFOCOM*, 2007, pp. 1919–1927.

[8] G. S. Hukkeri, S. Ankalaki, R. H. Goudar, and L. Hadimani, "The Impact of Protocol Conversions in the Wireless Communication of IOT Network," *International Journal of Advances in Soft Computing and its Applications*, vol. 16, no. 1, pp. 18–39, 2024, doi: 10.15849/IJASCA.240330.02.

[9] G. Somasundaram, S. S. Perumal, and L. Guran, "Identification and Analysis of Ransomware Transactions in the Bitcoin Network," *International Journal of Advances in Soft Computing and its Applications*, vol. 16, no. 2, pp. 48–67, 2024, doi: 10.15849/IJASCA.240730.04.

[10] G. Samara, W. A.-I. T. Journal, and undefined 2012, "Message broadcasting protocols in VANET," *scialert.net*, Accessed: Jan. 25, 2020. [Online]. Available: https://scialert.net/fulltextmobile/?doi=itj.2012.1235.1242

[11] G. Samara, S. Ramadas, and W. A. Al-Salihy, "Design of simple and efficient revocation list distribution in urban areas for VANETs," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 8, no. 1, pp. 151–155, 2010.

[12] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF protocols," 2015.

[13] M. A. Hassan, G. Samara, and M. A. Fadda, "IoT forensic frameworks (DFIF, IoTDots, FSAIoT): A comprehensive study," *International Journal of Advanced Soft Computing Applications*, vol. 14, no. 1, 2022.

[14] E. Pandian, R. Soundar, S. Gunasekaran, and S. Anantharajan, "Fuzzy Heuristics for Detecting and Preventing Black Hole Attack," *International Arab Journal of Information Technology*, vol. 21, no. 1, pp. 85–93, Jan. 2024, doi: 10.34028/iajit/21/1/8.

[15] A. Thanganadar and V. Raman, "Integrated Shared Random Key Agreement Protocol for Wireless Sensor Network," *International Arab Journal of Information Technology*, vol. 21, no. 2, pp. 201–210, Mar. 2024, doi: 10.34028/iajit/21/2/3.

[16] E. Qafzezi, S. Yussof, A. B. Abdullah, and N. T. Ali, "A comparison study of two fuzzy-based systems for assessment of fog computing resources in SDN-VANETs," in *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Springer, 2022, pp. 96–108.

[17] Q. I. Ali, "Realization of a robust fog-based green VANET infrastructure," *IEEE Syst J*, vol. 17, no. 2, pp. 2465–2476, 2022.

[18] I. M. Saadoon, "OLSR protocol based on fog computing and SDN in VANET," *Global Journal of Engineering and Technology Advances*, vol. 10, no. 2, pp. 60–70, 2022.

[19] A. J. Kadhim, S. A. H. Seno, J. I. Naser, and J. Hajipour, "DMPFS: Delay-efficient multicasting based on parked vehicles, fog computing and SDN in vehicular networks," *Vehicular Communications*, vol. 36, p. 100488, 2022.

[20] J. Gao, Z. Zhao, L. Xu, X. Chen, and K. Hwang, "A blockchain-SDN-enabled Internet of Vehicles environment for fog computing and 5G networks," *IEEE Internet Things J*, vol. 7, no. 5, pp. 4278–4291, 2019.

[21] A. Boualouache, R. Soua, and T. Engel, "Toward an SDN-based data collection scheme for vehicular fog computing," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[22] A. Devi, R. Kait, and V. Ranga, "Automated cluster head selection in fog-VANET via machine learning," in *Communication and Intelligent Systems*, Springer, 2021, pp. 1169–1179.

[23] R. Serrano, G. Boracchi, F. Pareschi, and others, "ChaCha20–Poly1305 authenticated encryption with additional data for transport layer security 1.3," *Cryptography*, vol. 6, no. 2, p. 30, 2022.

[24] J. P. Degabriele, J. Govinden, F. Günther, and K. G. Paterson, "The security of ChaCha20-Poly1305 in the multi-user setting," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1981–2003.

[25] F. De Santis, A. Schauer, and G. Sigl, "ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications," in *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, 2017, pp. 692–697.

[26] N. Gupta, A. Prakash, and R. Tripathi, "Adaptive beaconing in mobility aware clustering based MAC protocol for safety message dissemination in VANET," *Wirel Commun Mob Comput*, vol. 2017, p. 1246172, 2017.

[27] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the internet of things: Authentication and key generation," *IEEE Wirel Commun*, vol. 26, pp. 92–98, Oct. 2019, doi: 10.1109/MWC.2019.1800455.

[28] G. Samara, "An intelligent routing protocol in VANET," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 29, no. 1–2, pp. 77–84, 2018.

[29] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicle-to-vehicle communication: Fair transmit power control for safety-critical information," *IEEE Trans Veh Technol*, vol. 58, no. 7, pp. 3684–3703, 2009.

[30] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*, Boston, MA, USA, 2000, pp. 243–254.

[31] X. Feng, K. Cui, H. Jiang, and Z. Li, "EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network," *Symmetry (Basel)*, vol. 14, Jun. 2022, doi: 10.3390/sym14061230.

Notes on contributors

Ghassan Samara is currently an associate professor and vice dean of the Faculty of Information Technology at Zarqa University, Jordan. He Holds a BSc. and MSc. in Computer Science and a Ph.D. in Computer Networks. He obtained his Ph.D. from Universiti Sains Malaysia (USM) in 2012. His research interests include the Internet of Things, Cryptography, Vehicular Ad Hoc Networks, Wireless Sensor Networks, Internet Access Protocols, Accident Prevention, Alarm Systems, Cloud Computing, Computational Complexity, Computer Crime, Computer Network Security, Data Integrity, Data Privacy, Delays, Digital Forensics, Directed Graphs, Energy Conservation, Energy Management Systems, Fog Computing, Graph Theory, Home Automation, Intelligent Robots, and Intelligent Transportation Systems. Publications: Ghassan Samara has authored more than 150 scientific research papers published in international journals and conference proceedings.

Mahmoud Odeh is an associate professor at Zarqa University. He completed his higher education and PhD at Reading and Coventry University, UK. Mahmoud holds more than 15 years' experience in both the practical and academic fields, with 56 international certificates in servers, computer virtualization, smart machine simulation, and cloud computing. The rapid evolution of cloud computing technology inspires his current research, primarily focusing on the implementation of innovative technology.

Essam Al Daoud Earned his Ph.D. in Computer Science from the University Putra Malaysia. As a Professor at Zarqa University, he excels in research, curriculum development, and teaching, with expertise in data science, cryptography, and bioinformatics. He has also taught at institutions like Multimedia University in Malaysia. Driven by a passion for academic excellence, he continues to contribute significantly to his field through research, teaching, and leadership roles**.**

Samer Sabbah is a postgraduate student in the Faculty of IT, Cybersecurity Department, Zarqa University. He received his bachelor's in computer science in 2004. His Master's thesis revolves on Ai, blockchain technology in the era of web 4.0.

Mohammad Rasmi is an associate professor in the Faculty of IT, Cybersecurity Department, Zarqa University. He received his PhD in Network Security from Universiti Sains Malaysia in 2013. His research interests include digital forensics, cybersecurity, E-government strategy, cloud computing, and software engineering.

Mo'ath Alluwaici is an assistant professor in computer science department at Zarqa university. Alluwaici got his PhD and MSc degrees from UniMAP University in Malaysia in Applied Mathematics-AI. Alluwaici got his BSc degree in Mathematics and Statistics from JUST university-Jordan.
His main interests are machine learning, Fuzzy logic, and data science.