Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

SecureZone: Secure and Efficient Multipath Routing for Mobile Ad Hoc Networks

Dr. Rani Sahu
Associate Professor
Department of Computer Science and Engineering, IES Group of Institutions Bhopal MP, INDIA
Email :rani.princy28@gmail.com

Vinay Sahu
Assistant Professor, Department of CS, LNCT, Bhopal MP, INDIA
Email :sahu.vinay@gmail.com

Dr. Pushplata Chouksey
Principal, Govt Hamidia Arts and Commerce College, Bhopal
Email :pushplatachouksey@gmail.com

Sourabh Jain
Assistant Professor, Eklavya University Damoh MP, INDIA
Email :sourabhjain1788@gmail.com

ABSTRACT

Mobile ad hoc networks (MANETs) represent collaborative networks formed by mobile nodes without a centralized infrastructure, finding application across diverse domains including military and security-sensitive operations. However, securing the routing process within MANETs poses significant challenges due to the absence of a central authority and the dynamic nature of the network. Existing routing protocols suffer from limitations such as bandwidth consumption and route request delays. In response, this paper introduces the Secure and Energy-efficient Zone-based Multipath Routing Protocol (SEZMRPR) for MANETs. SEZMRPR integrates proactive and reactive approaches while incorporating digital signatures and encryption techniques to ensure message integrity, data confidentiality, and end-to-end authentication at the IP layer. The paper provides a comprehensive design of SEZMRPR, assesses its resilience against security attacks, and evaluates its performance through simulations. Results demonstrate SEZMRPR's robustness against security threats, its efficient security performance with acceptable overhead, and its applicability in securing MANETs for military and security-sensitive operations. SEZMRPR, in conjunction with existing security measures, establishes a reliable framework for ensuring secure operations in ad hoc networks. Future enhancements may focus on optimizing performance, scalability, energy efficiency, and addressing quality of service requirements to further refine the protocol.

Keywords - **Zone-based Routing, security, energy efficiency, MANETs.**

Date of Submission: March 09, 2024 Date of Acceptance: April 05, 2024

I. INTRODUCTION:

Mobile ad hoc networks (MANETs)[1] have emerged as a vital technology, facilitating communication among mobile devices without relying on a centralized infrastructure. These networks have diverse applications in both civilian and military sectors, where traditional networks may be impractical or unavailable. However, the inherent characteristics of MANETs, including node mobility, resource constraints, and the absence of a centralized authority, present significant challenges for ensuring secure and efficient routing.

A primary concern in MANETs is the security of the routing process. With nodes autonomously organizing themselves into networks and operating in open and hostile environments, traditional security mechanisms designed for wired networks prove ineffective. MANETs are particularly vulnerable to various security threats such as eavesdropping, tampering, and denial-of-service attacks[2]

To address these challenges, researchers have proposed numerous routing protocols for MANETs. However, existing protocols often suffer from issues like high bandwidth consumption, route request delays, and susceptibility to security threats[3]. Therefore, there is a pressing need for a routing protocol that not only ensures secure and reliable communication but also optimizes energy efficiency to prolong the network's operational lifespan.

This paper introduces the Secure and Energy-efficient Zone-based Multipath Routing Protocol (SEZMRPR), a novel approach for enhancing security in MANETs while maintaining energy efficiency. The protocol integrates

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

advanced security mechanisms to safeguard the routing process. The paper provides a comprehensive design of SEZMRPR, detailing its proactive and reactive components that contribute to secure and energy-efficient routing. Furthermore, it evaluates SEZMRPR's resilience against a spectrum of security attacks, demonstrating its efficacy in mitigating prevalent threats in MANETs. Through simulations, the paper assesses the performance of SEZMRPR in terms of routing overhead, packet delivery ratio, and energy consumption, highlighting its efficiency and suitability for real-world implementation. Finally, the paper outlines potential avenues for future enhancements, including performance optimization, scalability improvements, energy efficiency refinements, and integration of quality of service (QoS) considerations.

The remainder of the paper is structured as follows: Section 2 provides an overview of related work in secure routing protocols for MANETs. Section 3 presents the detailed design and architecture of the SEZMRPR protocol. Section 4 evaluates the security resilience and performance of SEZMRPR through extensive simulations and discusses the implications of the findings. Finally, Section 5 concludes the paper, summarizing the contributions and outlining future research directions.

II. LITERATURE REVIEW:

The paper[4] presents the Energy-Efficient Zone Routing Protocol (EEZRP), which focuses on optimizing energy consumption and improving communication reliability in mobile ad hoc networks. EEZRP adopts a zone-based approach, utilizing Zone Coordinators (ZCs) to oversee routing within non-overlapping zones. This protocol employs multipath routing to enhance redundancy and load balancing. Additionally, EEZRP integrates both proactive and reactive route maintenance mechanisms, ensuring scalability across networks of varying sizes. Simulation results demonstrate that EEZRP surpasses traditional protocols in terms of energy efficiency, network lifetime, and packet delivery ratio.

The paper[5] introduces a collaborative approach for enhancing secure routing in Mobile Ad-Hoc Networks (MANETs). This approach underscores the importance of node cooperation to bolster network security. Through a fusion of encryption, authentication, and key management techniques, the protocol guarantees secure data transmission within the network. By fostering collaboration among nodes, the protocol effectively mitigates vulnerabilities and enhances the overall reliability of routing in MANETs.

The paper[6] introduces a clustering-based secure fault-tolerant routing protocol tailored for MANETs. Employing clustering, the protocol organizes nodes into groups, thereby optimizing network efficiency and minimizing overhead. Integral to its design are secure error reporting mechanisms aimed at swiftly detecting and addressing faults within the network. By seamlessly merging fault tolerance with secure routing strategies, the protocol guarantees robust and secure data transmission, particularly in the dynamic and resource-constrained environments characteristic of MANETs.

The paper[7] presents a security-aware routing protocol tailored for Wireless Ad hoc Networks (WAHNs), emphasizing the prioritization of security considerations to counter potential threats and attacks. By integrating encryption, authentication, and secure key management mechanisms, the protocol guarantees the secure transmission of data and shields the network from malicious activities. This security-aware approach is geared towards bolstering the resilience and dependability of routing in WAHNs, rendering it suitable for applications demanding heightened security within dynamic and self-configuring networks.

The paper[8] introduces "SEAL" (Security-Aware List-Based Routing Protocol), a specialized routing protocol tailored for Mobile Ad hoc Networks (MANETs) with a robust emphasis on security. Utilizing a list-based approach, SEAL prioritizes secure routes to facilitate the safe transmission of data amidst potential threats or attacks. This protocol integrates encryption, authentication, and secure key management techniques to thwart malicious activities and unauthorized access. By amalgamating security principles with efficient routing decisions, SEAL bolsters the resilience and reliability of communication within dynamic and resource-constrained MANETs.

The paper[9] introduces "SARP-HWNs," a security-aware routing protocol designed specifically for Hybrid Wireless Networks (HWNs) featuring a trust-enhanced mechanism. By factoring in node trust levels, SARP-HWNs prioritizes secure routes to facilitate dependable and secure data transmission. The protocol integrates encryption, authentication, and secure key management mechanisms to safeguard against potential threats. SARP-HWNs endeavors to offer a resilient and secure routing solution tailored for HWNs, characterized by the coexistence of multiple wireless technologies.

The paper[10] presents a "Blockchain-assisted Secure Routing Protocol" designed for Cluster-based Mobile ad hoc Networks (MANETs). Leveraging blockchain technology, this protocol enhances security within cluster-based MANETs. Through the use of distributed ledger and cryptographic techniques, it guarantees secure and trustworthy data routing. This blockchain-assisted approach provides resilience against attacks and tampering, rendering it particularly well-suited for dynamic and self-organizing MANETs.

The paper[11] offers a comprehensive survey of "Trust-Based Secure Routing Protocols" deployed in Mobile Ad hoc Networks (MANETs). With a focus on protocols integrating trust mechanisms to bolster security in data routing, this survey meticulously evaluates and compares various trust-based approaches. By providing insights into their effectiveness, strengths, and limitations, the paper serves as a valuable resource for identifying trends and advancements in trust-based secure routing protocols. Consequently, it aids researchers and practitioners in selecting suitable solutions to secure MANETs within dynamic and challenging environments.

The paper[12] introduces a "Hierarchical Energy Efficient Secure Routing Protocol" tailored for Wireless Body Area

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

Networks (WBANs), aimed at optimizing route selection. Employing a hierarchical structure, the protocol minimizes energy consumption and enhances network efficiency. It incorporates essential security mechanisms, such as encryption and authentication, to guarantee secure data transmission within the body area network. Furthermore, the paper offers a comprehensive analysis and evaluation of the proposed protocol, showcasing its effectiveness and practical benefits in real-world scenarios.

The paper[13] presents an "Enhanced Energy Efficient Secure Routing Protocol" tailored for Mobile Ad hoc Networks (MANETs), with a dual focus on optimizing energy consumption and ensuring secure data transmission among network nodes. Through a detailed analysis, the paper demonstrates the protocol's performance, showcasing its effectiveness in achieving both energy efficiency and security objectives within dynamic and resource-constrained MANETs.

III. Design and Architecture of the Proposed SEZMRPR Protocol:

We propose SEZMRPR as a comprehensive and viable solution to address the limitations identified in existing approaches for securing ad hoc routing[14-18], with the goal of establishing secure routing in diverse ad hoc network environments.

3.1 Protocol Overview:

SEZMRPR represents an advanced routing protocol designed for secure communication within MANETs with a focus on energy efficiency. It takes inspiration from the Zone Base Multipath Routing AOMDV framework but introduces enhancements to strengthen security measures and streamline resource management. This protocol uniquely combines security features with energy-conscious strategies by dividing the network into zones for localized security protocol application. Authentication and data integrity are ensured through RSA digital signatures, utilizing both symmetric and asymmetric key encryption methods for confidentiality. Moreover, SEZMRPR implements a certification process to verify nodes' credentials before establishing secure communication channels. By integrating security and energy efficiency, SEZMRPR excels in optimizing resource allocation, reducing energy consumption, dynamically selecting energy-saving pathways, distributing traffic load efficiently, and maintaining these routes effectively over time. In summary, SEZMRPR offers an energy-efficient solution for secure routing in MANETs, enhancing security measures while maximizing resource utilization. Prior to engaging in any communication, every common node (CN) must undergo certification by certification authorities (CA) and receive public keys, as detailed in the subsequent section.

3.2 Certification Process:

SEZMRPR integrates a certification process to guarantee secure communication within the network. Trusted certification authorities (CAs) act as reliable servers, with common nodes (CNs) playing a crucial role [19]. All legitimate nodes are equipped with the public keys of CAs. The certification process is depicted in Fig. 1. SEZMRPR functions as a two-phase protocol. In the initial phase, known as the preliminary certification process, each CN obtains the necessary keys from its nearest CA. Subsequently, in the secure routing phase, these keys are utilized for secure intra-zone or inter-zone routing, leveraging digital signatures and message encryption to enhance security.

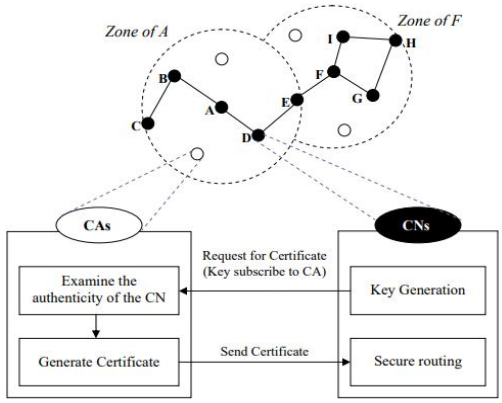

Fig. 1: Certification Process in SEZMRPR

3.3 Algorithm for Certification Process in SEZMRPR:

Input: Node X requesting a certificate from its nearest CA.
Output: Certificate (certX) issued by the CA.
Algorithm:

1. Node X sends a certificate request message to its nearest CA:
   - X → CA: certX_request.
2. The CA receives the certificate request from Node X.
3. The CA generates a certificate for Node X containing the following information:
   - Node X's IP address
   - Public key for verification (VKX)
   - Public key for encryption (EKX)
   - Creation timestamp (t)
   - Expiration time (e)
4. The CA securely signs the certificate using its private key (SKCA):
   - CA → X: certX = [IPX, VKX, EKX, t, e] | signCA.
5. Node X receives the certificate (certX) from the CA.
6. The certificate (certX) includes essential credentials for secure communication within the SEZMRPR network:
   - Node X's IP address

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

- Verification public key (VKX)
- Encryption public key (EKX)
- Creation timestamp (t)
- Expiration time (e)

7. The certificate is augmented with the CA's digital signature (signCA) to ensure authenticity and integrity.
8. Node X now holds a valid certificate (certX) issued by the CA, enabling secure communication within the SEZMRPR network.

It is imperative for all nodes in the SEZMRPR network to maintain updated certificates provided by their respective CAs to establish secure communication channels and facilitate secure routing within the network.

3.4 Components of SEZMRPR Architecture:

The architecture of SEZMRPR is a customized version of the Zone Based Routing Protocol AOMDV, incorporating features for secure routing and effective key management. It consists of separate and self-sufficient components assigned with specific roles. The functions and interconnections of each component are illustrated in Fig. 2.

IV. Design of Secure and Energy-efficient Zone-based Multipath Routing Protocol (SEZMRPR):

This section provides a detailed insight into the architectural design of the SEZMRPR protocol, outlining its components and their individual functionalities.

4.1 Components of SEZMRPR Architecture

The architecture of SEZMRPR is a customized version of the Zone Based Routing Protocol AOMDV, incorporating features for secure routing and effective key management. It consists of separate and self-sufficient components assigned with specific roles [20]. The functions and interconnections of each component are illustrated in Fig. 2.

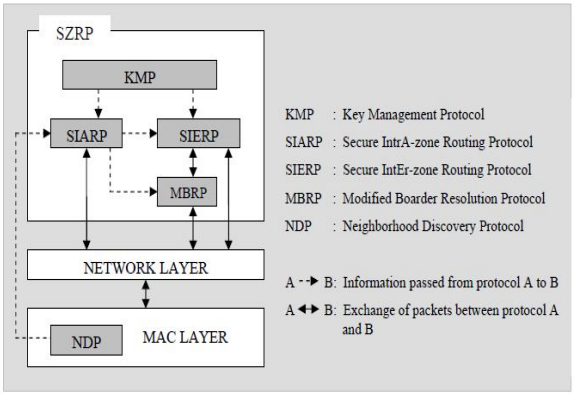

Fig 2: Architecture of SEZMRPR

4.2 Components of SEZMRPR Architecture:

1. Key Management Protocol (KMP):
   This component manages the public key certification process, guaranteeing the secure issuance and administration of certificates across the network.
2. Secure Intrazone Routing Protocol (SIARP):
   Responsible for proactive link-state routing within a zone, enabling efficient and secure communication among nodes within the same zone.
3. Secure Interzone Routing Protocol (SIERP):
   Tasked with reactive secure route discovery and maintenance between different zones, facilitating secure communication across zones while adapting dynamically to network changes.
4. Neighborhood Discovery Protocol (NDP):
   Focused on identifying neighboring nodes and monitoring link failures, essential for maintaining an updated network topology view and ensuring dependable communication.
5. Modified Border Resolution Protocol (MBRP):
   Utilizes the bordercasting technique to streamline interzone route discovery, enhancing the process of finding secure routes between zones while minimizing overhead.

4.3 Secure Routing Algorithm

The following section outlines the intrazone and interzone routing procedures in SEZMRPR, utilizing the network diagram presented in Fig. 3. Detailed algorithms for both processes are provided in (A) and (B).

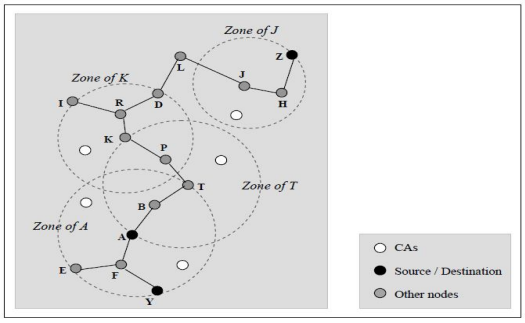

Fig 3: Intrazone and Interzone destinations of node A (zone radius β = 2)

4.4 Algorithm for Secure Intra-Zone Routing:

Input: Source node A, destination node Y within the same zone

Output: Secure communication channel between A and Y using session key KAY

1. A selects a route to Y within the same zone from its SIARP routing table.
2. A sends a Session Key Request (SKREQ) packet to Y:
   - Construct SKREQ packet: [SKREQ, IPY, certA] | signA
   - Transmit SKREQ packet to Y: A → Y
3. Y receives the SKREQ packet:

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

- Verify the packet's signature using A's public key.
- Authenticate the packet.
- Generate a session key KAY.

4. Y sends a Session Key Reply (SKREP) packet to A:
   - Construct SKREP packet: [SKREP, IPA, certY, (KAY)EKA] | signY
   - Dispatch SKREP packet to A: Y → A
5. A receives the SKREP packet:
   - Verify the packet's signature using Y's public key.
   - Decrypt the packet using A's private key to obtain the session key KAY.
6. A encrypts the data packet with KAY and transmits it to Y along the same route (A-F-Y).
7. Subsequent communication between A and Y is secured using the session key KAY.

4.5 Algorithm for Secure Inter-Zone Routing:

Input: Source node A, destination node Z in a different zone
Output: Secure communication channel between A and Z using session key KAZ

1. A initiates secure route discovery by bordercasting an SRD packet to peripheral nodes (T, E, and Y) with MBRP's assistance:
   - Construct SRD packet: [SRD, IPZ, certA, β, NA, t] | signA
   - Bordercast SRD packet: A → Bordercast
2. Peripheral nodes validate the SRD packet, establish a reverse path to A, sign and append their certificates, and rebordercast the packet if they lack a route to Z.
3. Rebordercasting continues until a node with a valid route to Z is reached. At that node, the SRD is forwarded to Z:
   - Construct and forward SRD packet: [[SRD, IPZ, certA, β, NA, t] | signA] | signT, certT → K → J → Z
4. Z verifies J's signature, retrieves the encrypted session key KAZ, and creates an SRR packet:
   - Construct SRR packet: [SRR, IPA, certZ, NA, t, (KAZ)EKA] | signZ
   - Transmit SRR packet to H: Z → H
5. As the SRR packet traverses the reverse path, each node validates the previous hop's signature, removes the certificate and signature, signs the packet, appends its certificate, and forwards it to the next hop.
6. A receives the SRR packet from J, validates J's signature, retrieves the session key KAZ, and encrypts the data packet using KAZ.
7. A sends the encrypted packet to Z along the same route (A-F-J-Z).
8. Subsequent communication between A and Z is secured using the session key KAZ.

These algorithms ensure secure intra-zone and inter-zone routing in SEZMRPR, enabling nodes within the same zone and different zones to establish secure communication channels using session keys.

4.6 Route Maintenance:

Route maintenance in the Secure and Energy-efficient Zone-based Multipath Routing Protocol (SEZMRPR) ensures dependable and energy-efficient communication in ad hoc networks. It encompasses the following procedures:

1. **Link Failure Detection**: SEZMRPR identifies link failures by either periodic hello messages or continuous signal monitoring.
2. **Route Error Signaling**: When a link failure occurs, nodes generate Route Error (RE) messages, digitally signed, to inform neighboring nodes and the source node.
3. **Route Repair or Redirection**: Neighboring nodes and the source node initiate actions to repair or redirect routes, utilizing available alternatives.
4. **Multipath Utilization**: SEZMRPR leverages multiple paths to alleviate link failures, enhance load balancing, and fortify network resilience.

Regarding energy efficiency, SEZMRPR optimizes energy usage by selecting energy-efficient paths and distributing traffic evenly. These mechanisms ensure reliable and energy-efficient routing, facilitating secure communication while conserving network resources in SEZMRPR. In conclusion, SEZMRPR amalgamates robust security features with energy optimization techniques, rendering it a dependable and efficient solution for routing in wireless ad hoc networks. It safeguards against diverse security threats while minimizing energy consumption, making it well-suited for resource-constrained environments.

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

V. RESULTS AND DISCUSSION

This section presents the results of simulations conducted using the NS2.35 simulator [21].

5.1 Simulation Parameters

The protocol's performance evaluation using the event-driven ns2.34[21] simulator has been completed[22]. A random mobility model was selected for the simulation, and nodes were randomly distributed within a rectangular area measuring 1500 m x 1000 m. Specific parameters have been set in the TCL script of the network to facilitate the simulation of this protocol, as detailed in Table 1.

The following table shows the simulation parameters used in simulations.

PARAMETERS	VALUE
Simulator	NS2.35
Simulation Area	1500 m x 1000 m
Number of nodes	50, 75 and 100 nodes
Node Speed	20 Meter/second
Queue size	50 packets
Studies Routing Protocols	AODV, AOMDV & SEZMRPR
Data Payload	512 bytes/packet
Initial energy	50 joule
Idle Power	0.100 J/bit
Sense Power	0.0175 J/bit
Energy consumption of transmitting data	0.035 J/bit
Energy consumption of receiving data	0.035 J/bit
Traffic Type	CBR
Simulation Time	200 Seconds
Channel Type	Wireless channel
MAC type	802.11
Mobility	Random Way point
Antenna model	Omni

TABLE 1: SIMULATION PARAMETERS

The SEZMRPR zone-based approach is assessed using metrics such as throughput, end-to-end delay, packet delivery ratio, energy consumption, and network lifetime. The examination of these metrics across varying numbers of nodes is presented in the subsequent section.

5.2.1 Average Throughput:

Throughput is the total amount of data successfully transmitted from a sender to a receiver per unit of time, typically measured in bytes per second (bytes/sec) [23]. It reflects the overall efficiency of a system. The average throughput can be calculated using the formula TH = I / T, where TH represents the throughput, I is the inventory (amount produced), and T is the time taken to produce that inventory. This formula is derived from Little's Law, which assesses the average number of items over a specific period. Throughput rate is crucial for businesses to evaluate their production or service efficiency.

$$\sum_{i=1}^{m} \frac{(ZN_i)/(ZT_{i,f} - ZT_{i,s})}{m}$$

Where

ZNi = Total number of bytes transmitted by node i.

ZTi, f = Time stamp at which transmission finishes from node i.

ZTi, s = Time stamp at which transmission starts at node i.

m = Total number of nodes.

Analysis of Throughput on Varied Number of Nodes

The evaluation of throughput in the Secure and Energy-efficient Zone-based Multipath Routing Protocol (SEZMRPR) was performed on networks comprising 50, 75, and 100 nodes, each moving at a speed of 3 meters per second, with a consistent packet size of 512 bytes. SEZMRPR integrates proactive and reactive routing strategies to minimize delays and improve data delivery efficiency. Furthermore, the protocol utilizes digital signatures and encryption to ensure secure communication, safeguarding against data manipulation and unauthorized entry. These security measures enhance data transmission reliability, leading to an overall enhancement in throughput performance.

TABLE 2 THROUGHPUT OF AODV, AOMDV AND SEZMRPR WITH DIFFERENT NUMBER OF NODES

PROTOCOLS	NUMBER OF NODES VS THROUGHPUT		
	50	75	100
AODV	6718.66	8708.63	9249.71
AOMDV	6852.44	8979.59	15186.84
SEZMRPR	12666.85	22366.39	26055.05

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

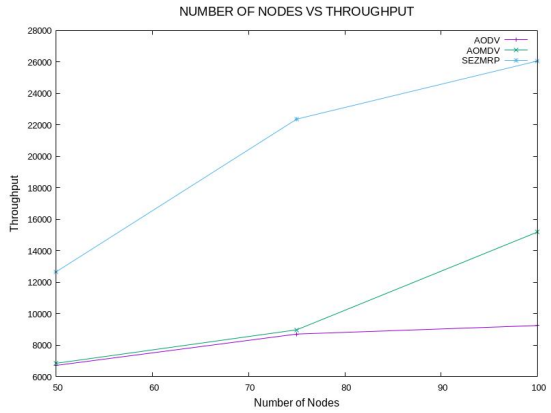

Fig. 5 Throughput comparison based on Scenario 4

SEZMRPR outperforms AODV and AOMDV in terms of throughput for different packet sizes (50, 75, and 100 bytes), showcasing its superior efficiency and effectiveness in delivering data compared to the other two routing protocols. The results indicate that SEZMRPR consistently achieves higher throughput percentages across all packet sizes, making it a promising choice for enhancing network performance in various scenarios

TABLE 3 THROUGHPUT COMPARISON OF SEZMRPR WITH AODV AND AOMDV

PACKET SIZE	50	75	100	AVERAGE/ OVERALL
SEZMRPR compared to AODV	46.95%	61.06%	64.49%	59.60%
SEZMRPR compared to AOMDV	45.90%	59.85%	41.71%	49.22%

The evaluation of SEZMRPR's throughput across varying node counts showcases its efficiency and resilience. It delivers exceptional throughput even with increased nodes, establishing it as a prime option for secure and energy-efficient routing in mobile ad hoc networks. The integration of proactive and reactive routing mechanisms, coupled with advanced security features, confirms the efficacy of SEZMRPR for diverse applications, including military and security-sensitive operations.

5.2.2 End to End Delay

End-to-end network delay includes queuing delay, transmission delay, processing delay, and propagation delay. Average End-to-End Delay is determined using a specific formula.

$$\sum_{i=1}^{m} \frac{ZD_{q,i} + ZD_{t,i} + ZD_{cpu,i} + ZD_{p,i}}{m}$$

Where

$ZD_{q,i}$ = queuing delay at node i.

$ZD_{t,i}$ = transmission delay at node i.

$ZD_{cpu,i}$ = processing delay at node i.

$ZD_{p,i}$ = propagation delay at node i.

m = total number of nodes.

Delay is a very important performance metric of any network. Minimum is the delay better is the performance of the network.

Analysis of End-to-End Delay on Varied Number of Nodes

The end-to-end delay analysis of SEZMRPR on networks with varying node counts demonstrates its efficiency compared to AODV and AOMDV routing protocols. SEZMRPR consistently achieves lower delays even as the number of nodes increases. This is attributed to SEZMRPR's integration of proactive and reactive routing, along with zone-based optimization, which significantly reduces delays during data transmission. Importantly, the security measures of SEZMRPR have minimal impact on end-to-end delays, ensuring both efficient and secure communication

PROTOCOLS	NUMBER OF NODES VS END TO END DELAY		
	50	75	100
AODV	479.44	757.079	907.463
AOMDV	451.778	841.936	962.646
SEZMRPR	295.526	301.801	395.19

TABLE 4 END TO END DELAY OF AODV, AOMDV AND SEZMRPR WITH DIFFERENT NUMBER OF NODES

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

Table 5 shows that SEZMRPR outperforms AODV and AOMDV in terms of end-to-end delay for different node counts. SEZMRPR consistently achieves lower delay percentages across all scenarios, indicating its superior efficiency in data delivery compared to the other two protocols.

TABLE 5 END TO END DELAY COMPARISON OF SEZMRPR WITH AODV AND AOMDV

NUMBER OF NODES	50	75	100	AVERAGE/ OVERALL
SEZMRPR compared to AODV	38.36%	60.13 %	56.45%	53.70%
SEZMRPR compared to AOMDV	34.58%	64.15 %	58.94%	56.01%

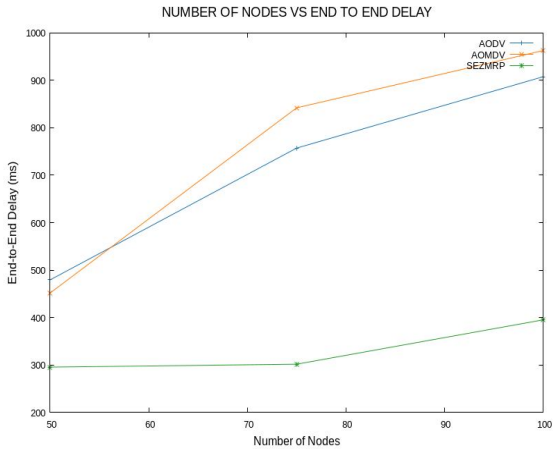

Fig. 6 End to End Delay comparison based on Scenario 4

The examination of end-to-end delay underscores SEZMRPR's prowess in sustaining minimal delays amid escalating node densities. This can be credited to its fusion of proactive and reactive routing approaches, zone-based optimization, and energy-efficient mechanisms. SEZMRPR's adeptness in fulfilling security demands without compromising performance renders it applicable across diverse domains, including military and security-sensitive operations. The research findings corroborate SEZMRPR as a resilient and effective routing protocol purpose-built for mobile ad hoc networks.

5.2.3 Packet Delivery Ratio

It is the ratio of a number of packets that got at the destination and packets sent by a sender. The packet delivery ratio is determined by utilizing the following equation:

$$\text{PDR}\frac{ZTR_{pd}}{ZTS_{ps}}$$

Where,

ZTR_{pd} = total packets received at the destination (in bytes)

ZTS_{ps}= total packets sent by the sender (in bytes)

Analysis of Packet Delivery Ratio (PDR) on Varied Number of Nodes

In this section, the Packet Delivery Ratio (PDR) of SEZMRPR is scrutinized across networks with varying node counts. SEZMRPR consistently outperforms AODV and AOMDV, exhibiting higher PDR even as node counts increase. This underscores its efficacy in facilitating successful data delivery. The protocol's resilience, adaptability, employment of multipath routing, and zone-based optimizations collectively contribute to its elevated PDR. SEZMRPR swiftly detects link failures and adapts to network dynamics, thereby ensuring reliable data delivery. Importantly, the incorporation of security mechanisms within SEZMRPR does not compromise PDR, thereby safeguarding data integrity and confidentiality.

TABLE 6 PDR OF AODV, AOMDV AND SEZMRPR WITH DIFFERENT NUMBER OF NODES

PROTOCOLS	NUMBER OF NODES VS PACKET DELIVERY RATIO		
	50	75	100
AODV	49.5544	50.2045	54.3859
AOMDV	48.9817	52.7977	60.9714
SEZMRPR	60.5352	75.82134	78.4531

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

Table 7 illustrates SEZMRPR's superior performance in terms of Packet Delivery Ratio (PDR) compared to AODV and AOMDV across various node counts. SEZMRPR consistently attains higher PDR percentages in all scenarios, underscoring its heightened effectiveness and reliability in ensuring successful data delivery in comparison to the other two protocols.

TABLE 7 PDR COMPARISON OF SEZMRPR WITH AODV AND AOMDV

PACKET SIZE	50	75	100	AVERAGE/ OVERALL
SEZMRPR compared to AODV	18.13%	33.78%	30.67 %	28.24 %
SEZMRPR compared to AOMDV	19.08%	30.36%	22.28 %	24.23 %

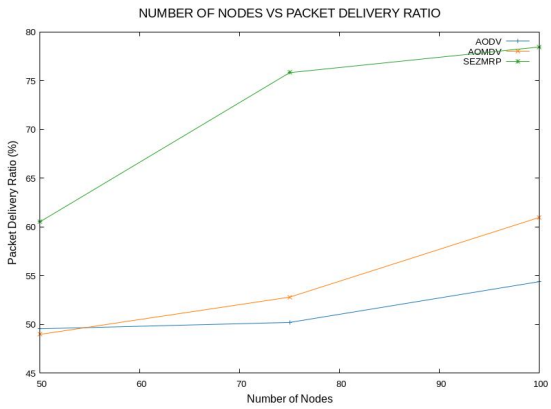

Fig. 7 Packet Delivery Ratio comparison based on Scenario 4

In conclusion, SEZMRPR demonstrates a remarkable Packet Delivery Ratio (PDR) across networks with diverse node counts. Its proactive and reactive routing strategies, zone-based optimization, and implementation of multipath routing significantly contribute to its superior PDR. SEZMRPR's adeptness in managing security demands while maintaining reliable data delivery renders it applicable across a spectrum of applications, including military and security-sensitive operations. The outcomes affirm SEZMRPR as a resilient and dependable routing protocol tailored for mobile ad hoc networks.

5.2.4 Energy Consumption

Energy Consumption in a network refers to the amount of energy consumed by each node during the simulation time. It is calculated by measuring the energy level of each node at the end of the simulation. The formula to calculate Energy Consumption is as follows:

$$TotalEnergyConsumption = \sum_{i=1}^{n} (ZEi - ZRi)$$

Where ZE_i denotes the initial energy of i^{th} node, ZRi denote ds he residual energy of i^{th} node and n number of nodes in the network.

Analysis of Energy Consumption on Varied Number of Nodes

In this section, the Energy Consumption performance of SEZMRPR is evaluated on networks with different node counts in a mobile ad hoc network. SEZMRPR exhibits energy-efficient behavior, even with an increasing number of nodes. Its zone-based approach and multipath routing optimization contribute to reduced energy consumption. SEZMRPR dynamically selects energy-efficient paths and incorporates power-aware node scheduling and sleep modes to further co

nserve energy. The secure communication mechanisms do not significantly impact energy consumption, making SEZMRPR an energy-efficient routing protocol for mobile ad hoc networks.

TABLE 8 ENERGY CONSUMPTION OF AODV, AOMDV AND SEZMRPR WITH DIFFERENT NUMBER OF NODE

PROTOCOLS	NUMBER OF NODES VS ENERGY CONSUMPTION		
	50	75	100
AODV	95.4259	157.634	196.709
AOMDV	95.6652	157.991	196.558
SEZMRPR	72.7573	153.871	173.805

Table 9 shows that SEZMRPR outperforms AODV and AOMDV in terms of energy efficiency for different node counts. SEZMRPR consistently achieves lower energy consumption percentages across all scenarios, indicating its superior performance in optimizing energy usage compared to the other two protocols.

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

TABLE 9 ENERGY CONSUMPTION COMPARISON OF SEZMRPR WITH AODV AND AOMDV

PACKET SIZE	50	75	100	AVERAGE/OVERALL
SEZMRPR compared to AODV	23.75%	2.38%	11.64%	10.96%
SEZMRPR compared to AOMDV	23.94%	2.60%	11.57%	11.057%

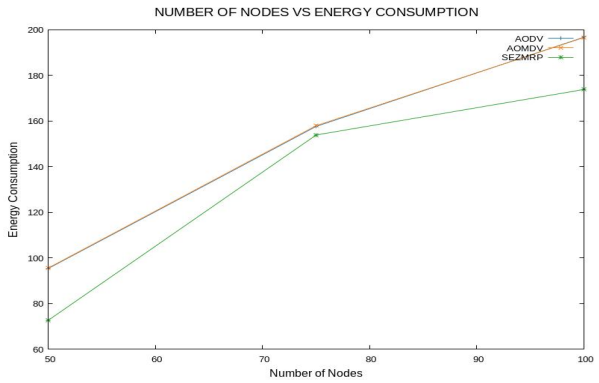

Fig. 8 Energy Consumption comparison based on Scenario 4

In conclusion, the analysis of Energy Consumption on networks with varying node counts confirms that SEZMRPR is an energy-efficient routing protocol. Its zone-based approach, multipath routing optimization, power-aware node scheduling, and sleep modes contribute to reduced energy consumption and prolonged network lifespan. SEZMRPR's ability to maintain energy efficiency while ensuring security makes it well-suited for resource-constrained mobile ad hoc networks. The results validate SEZMRPR as a reliable and energy-efficient routing protocol for diverse applications, including military and security-sensitive operations.

5.2.5 Network Lifetime

Network Lifetime shows how long nodes in the network continue active. The unit of Network Lifetime is a sec. It is a highly powerful metric since it shows the operational time of the network. It is determined to utilize the following equations:

$$NetworkLifetime = \sum_{i=1}^{m} (energy(i) = 0)$$

The proposed algorithm is implemented and simulation results based on the Scenarios are presented in this section.

Analysis of Network Lifetime on Varied Number of Nodes

The analysis of Network Lifetime shows that the Secure and Energy-efficient Zone-based Multipath Routing Protocol (SEZMRPR) effectively manages energy resources, leading to a prolonged Network Lifetime. SEZMRPR's zone-based approach, multipath routing optimization, and adaptive strategies contribute to its energy efficiency without compromising security. These results validate SEZMRPR as a reliable and energy-efficient routing protocol for mobile ad hoc networks, with extended Network Lifetime.

TABLE 10 NETWORK LIFETIME OF AODV, AOMDV AND SEZMRPR WITH DIFFERENT NUMBER OF NODE

PROTOCOLS	NUMBER OF NODES VS NETWORK LIFETIME		
	50	75	100
AODV	42.2749	42.3658	22.2908
AOMDV	42.2929	42.0088	22.4415
SEZMRPR	52.5456	46.2503	36.5234

SEZMRPR outperforms AODV and AOMDV in Network Lifetime, demonstrating its superior energy management and efficiency for mobile ad hoc networks. It prolongs the network's operational lifespan and is suitable for various applications, including military and security-sensitive operations.

NUMBER OF NODES	50	75	100	AVERAGE/OVERALL
SEZMRPR compared to AODV	19.54 %	8.39 %	38.96%	20.97%
SEZMRPR compared to AOMDV	19.51 %	9.17 %	38.55%	21.11%

TABLE 11 NETWORK LIFETIME COMPARISON OF SEZMRPR WITH AODV AND AOMDV

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

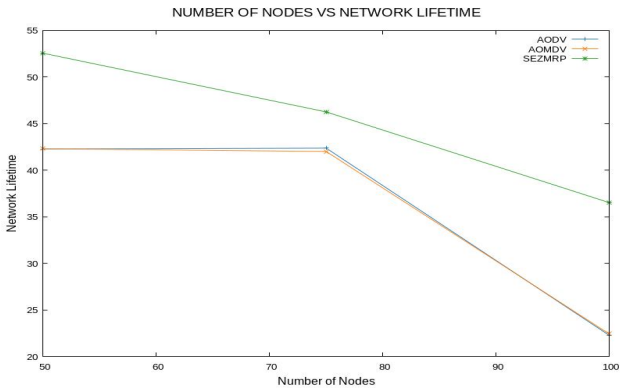

Fig. 9 Network Lifetime comparison based on Scenario 4

SEZMRPR efficiently manages energy, leading to a prolonged Network Lifetime. Its zone-based approach, multipath routing, and security measures contribute to reliability. Suitable for resource-constrained environments and security-sensitive scenarios. Robust and efficient routing protocol.

VI. CONCLUSION

The research introduces the Secure and Energy-efficient Zone-based Multipath Routing Protocol (SEZMRPR) as a holistic approach to securing routing in mobile ad hoc networks (MANETs). SEZMRPR combines proactive and reactive strategies, employing digital signatures and encryption to maintain message integrity and data confidentiality. Through extensive simulations, SEZMRPR demonstrates its effectiveness against security threats and showcases efficiency in throughput, end-to-end delay, and packet delivery ratio. The protocol not only ensures secure communication but also enhances energy efficiency, prolongs network lifetime, and outperforms traditional protocols like AODV and AOMDV. It proves to be a dependable and energy-efficient solution suitable for diverse applications, especially in military and security-sensitive contexts. Future research directions may involve optimizing performance, scalability, and energy efficiency to further enhance the protocol's capabilities. In summary, SEZMRPR emerges as a robust and effective routing solution for secure communication in ad hoc networks.

REFERENCES

[1]. Kaur, S. and R. Kait, An Overview of Ad Hoc Networks Routing Protocols and Its Design Effectiveness. Computer Vision and Robotics: Proceedings of CVR 2022, 2023: p. 421-430.

[2]. Vamshi Krishna, K. and K. Ganesh Reddy, Classification of Distributed Denial of Service Attacks in VANET: A Survey. Wireless Personal Communications, 2023: p. 1-32.

[3]. Kaddoura, S., et al., SDODV: A smart and adaptive on-demand distance vector routing protocol for MANETs. Peer-to-Peer Networking and Applications, 2023: p. 1-24.

[4]. Basurra, S.S., et al., Energy efficient zone based routing protocol for MANETs. Ad Hoc Networks, 2015. 25: p. 16-37.

[5]. Theresa, W.G., A. Gayathri, and P. Rama, A Collaborative Approach for Secured Routing in Mobile Ad-Hoc Network. Intelligent Automation & Soft Computing, 2023. 35(2).

[6]. Sathiyavathi, V., et al., Clustering based secure error report fault tolerant routing in mobile adhoc networks. Journal of Intelligent & Fuzzy Systems, 2023(Preprint): p. 1-10.

[7]. Yi, S., P. Naldurg, and R. Kravets. A security-aware routing protocol for wireless ad hoc networks. in Proceedings of ACM MobiHoc. 2001. Citeseer.

[8]. Simpson, S.V. and G. Nagarajan. SEAL—security-aware list-based routing protocol for mobile ad hoc network. in Advances in Power Systems and Energy Management: Select Proceedings of ETAEERE 2020. 2021. Springer.

[9]. Kumar, A.V. and S.K. Mohideen, Security aware routing protocol for hybrid wireless network (SARP-HWNs) via trust enhanced mechanism. International Journal of Business Data Communications and Networking (IJBDCN), 2019. 15(1): p. 34-57.

[10]. Ilakkiya, N. and A. Rajaram, Blockchain-assisted Secure Routing Protocol for Cluster-based Mobile-ad Hoc Networks. INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL, 2023. 18(2).

[11]. Sharma, S. and S.Z. Hussain. A survey of trust based secure routing protocol used in mobile ad hoc networks. in ITM Web of Conferences. 2023. EDP Sciences.

[12]. Roshini, A. and K. Kiran, Hierarchical energy efficient secure routing protocol for optimal route selection in wireless body area networks. International Journal of Intelligent Networks, 2023. 4: p. 19-28.

Volume: 15 Issue: 06 Pages: 6182 – 6193 (2024) ISSN: 0975-0290

[13]. Prasad, R., Enhanced energy efficient secure routing protocol for mobile ad-hoc network. Global Transitions Proceedings, 2022. 3(2): p. 412-423.
[14]. Srilakshmi, U., et al., A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access, 2022. 10: p. 14260-14269.
[15]. Suresh Kumar, R., et al., Cluster Head Selection and Energy Efficient Multicast Routing Protocol-Based Optimal Route Selection for Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing, 2022. 2022.
[16]. Fatemidokht, H., et al., Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 2021. 22(7): p. 4757-4769.
[17]. Argyroudis, P.G. and D. O'mahony, Secure routing for mobile ad hoc networks. IEEE Commun. Surv. Tutorials, 2005. 7(1-4): p. 2-21.
[18]. Bhardwaj, V., et al., SecRIP: Secure and reliable intercluster routing protocol for efficient data transmission in flying ad hoc networks. Transactions on Emerging Telecommunications Technologies, 2021. 32(6): p. e4068.
[19]. Mahmood, S., et al., Digital certificate verification scheme for smart grid using fog computing (FONICA). Sustainability, 2021. 13(5): p. 2549.
[20]. Devi, B.R., J.R. Murthy, and G. Narasimha. Secure zone based routing protocol for mobile adhoc networks. in 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s). 2013. IEEE.
[21]. Jubair, M. and R. Muniyandi, NS2 simulator to evaluate the effective of nodes number and simulation time on the reactive routing protocols in MANET. International Journal of Applied Engineering Research, 2016. 11(23): p. 11394-11399.
[22]. Sahu, Manju, and Sanjeev Gour. "INTSM: A Novel Approach for Load Balancing in MANET Route Discovery." Int. J. Advanced Networking and Applications 15.02 (2023): 5837-5852.
[23]. Sahu, Vinay, Neetu Sahu, and Rani Sahu. "A Comparative Study on Routing Protocols: RIPng, OSPFv3 and EIGRPv6 and Their Analysis Using GNS-3." International Journal of Advanced Networking and Applications (2023): 5775-5780.