Design And Evaluation Of Secure Routing Schemes In Ad Hoc Wireless Networks

[1]Jagadish, [2]Rukmini S
[1]Lecturer, [2]Lecturer
[1]Department of Computer Science &Engineering, [2]Department of Computer Science &Engineering
[1]Government Women's Polytechnic, [2]Government Women's Polytechnic, Kalaburagi, India

Abstract:

Mobile Ad-Hoc Networks (MANETs) are decentralized, self-configuring wireless networks that rely on dynamic topologies and collaborative node-to-node communication without fixed infrastructure. While MANETs offer flexibility and ease of deployment, they are highly vulnerable to various security threats due to their open nature, limited resources, and lack of centralized control. Secure routing becomes a critical concern to ensure the reliable transmission of data across the network.

This research investigates the core security challenges in MANET routing protocols and analyzes various secure routing mechanisms designed to mitigate attacks such as black hole, wormhole, and Sybil attacks. It provides a comparative study of notable secure routing protocols including SAODV, ARAN, SEAD, and SRP, highlighting their strengths, weaknesses, and performance trade-offs under different threat models. Key security requirements such as authentication, integrity, confidentiality, and availability are discussed in the context of routing strategies.

Simulation results (or theoretical analysis, if no simulation is done) demonstrate the effectiveness of these protocols in enhancing MANET security while maintaining acceptable performance metrics. The study further explores potential enhancements and emerging trends aimed at developing more robust and adaptive secure routing solutions for future MANET deployments.

Index Terms: ***Mobile Ad-Hoc Networks (MANETs), Secure Routing, Routing Protocols, Wireless Networks, Network Security, Cryptography, Attack Mitigation, SAODV, ARAN, Black Hole Attack, Wormhole Attack.***

I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) represent a class of wireless networks where mobile nodes communicate with each other without relying on any fixed infrastructure or centralized administration. These networks are highly dynamic and self-organizing, making them suitable for applications in military operations, disaster recovery, intelligent transportation systems, and remote sensing. Due to their flexibility, MANETs have gained significant attention in both academic research and real-world deployment.

However, the decentralized and open nature of MANETs introduces several security vulnerabilities. Nodes in a MANET are free to join or leave the network, and the topology changes frequently due to node mobility. These characteristics make traditional security mechanisms ineffective, and hence, securing routing protocols becomes a major concern. Routing protocols in MANETs are responsible for discovering and maintaining paths between nodes, but in the absence of robust security features, they can be easily exploited by malicious actors through attacks such as black hole, wormhole, Sybil, and denial-of-service (DoS) attacks.

To address these challenges, researchers have proposed a variety of secure routing protocols that integrate cryptographic techniques, trust management, and anomaly detection mechanisms. Protocols like SAODV (Secure AODV), ARAN, SEAD, and SRP have been developed to enhance the security of route discovery and maintenance processes in MANETs.

This research paper aims to explore and analyze the key secure routing protocols designed for MANETs, highlighting their architectural approaches, strengths, weaknesses, and effectiveness in mitigating known attacks. The study also discusses the essential security requirements for routing in MANETs and proposes directions for future research to develop more adaptive and intelligent security solutions.

II. LITERATURE SURVEY

Overview of Existing Routing Protocols

Mobile Ad-Hoc Networks (MANETs) rely on dynamic routing protocols that facilitate communication between mobile nodes without fixed infrastructure. Several traditional routing protocols have been developed to manage route discovery and maintenance in such environments:

- **Destination-Sequenced Distance Vector (DSDV):** A proactive protocol that uses table-driven routing, where each node maintains a routing table with the shortest path to all known destinations. While DSDV ensures low-latency communication, it incurs high overhead due to frequent table updates.
- **Ad-hoc On-Demand Distance Vector (AODV):** A reactive protocol that initiates route discovery only when data transmission is needed. It uses Route Request (RREQ) and Route Reply (RREP) messages, reducing overhead but introducing delay during route setup.
- **Dynamic Source Routing (DSR):** Another reactive protocol that relies on source routing. Each packet carries the complete route in its header. Although DSR is bandwidth-efficient in small networks, it becomes less scalable as the number of nodes increases.
- **Optimized Link State Routing (OLSR):** A proactive protocol that uses periodic control messages to update link-state information. It introduces multipoint relays (MPRs) to reduce redundant retransmissions, making it more scalable for large and dense networks.

Security Challenges in These Protocols

While the above protocols are efficient in route management, they were not originally designed with security in mind. Consequently, they are highly vulnerable to various attacks due to their open medium, dynamic topology, and lack of centralized control:

- **AODV and DSR** are susceptible to **black hole and wormhole attacks**, where malicious nodes falsely advertise optimal paths to intercept or drop packets.
- **DSDV** can be affected by **routing table overflow and sequence number spoofing**, leading to incorrect or stale route advertisements.
- **OLSR**, being proactive, is vulnerable to **HELLO flood attacks** and **link spoofing**, which can result in false topology creation.

These vulnerabilities highlight the need for integrating robust security mechanisms into the routing process to ensure confidentiality, integrity, and availability of data.

Summary of Related Works and Research Gaps

Over the years, researchers have proposed several secure routing protocols to address these challenges. For instance:

- **Secure AODV (SAODV)** extends AODV by incorporating digital signatures and hash chains to protect RREQ and RREP messages from tampering.
- **Authenticated Routing for Ad Hoc Networks (ARAN)** uses cryptographic certificates for secure route authentication and verification.
- **Secure Efficient Ad hoc Distance vector (SEAD)** secures DSDV-like protocols using hash chains for authenticating updates.
- **Secure Routing Protocol (SRP)** secures route discovery by validating each step of the path using a security association between source and destination.

While these protocols improve resilience against specific attacks, most of them assume the availability of a trusted certificate authority or shared keys, which is often unrealistic in highly dynamic or hostile environments. Additionally, many secure routing solutions impose significant overhead in terms of computation and communication, reducing the efficiency of MANETs, especially in resource-constrained scenarios.

There is still a **notable gap** in designing lightweight, scalable, and fully adaptive secure routing protocols that can dynamically adjust to the nature of attacks and node mobility without compromising network performance. This research aims to analyze existing secure routing protocols and propose potential directions for more efficient and intelligent security frameworks in MANETs.

III. Security Threats in MANET’s

Due to their open wireless communication medium, lack of centralized control, and dynamic topology, Mobile Ad-Hoc Networks (MANETs) are highly vulnerable to various types of security threats. These threats can severely disrupt the network's functionality, leading to loss of data, degraded performance, and system instability. Security threats in MANETs are broadly classified into two categories: **passive** and **active** attacks.

3.1 Classification of Attacks

- **Passive Attacks:**
  In passive attacks, the attacker silently monitors and intercepts data without altering the communication. These attacks primarily focus on breaching **confidentiality** and **privacy**.
  - Example: Eavesdropping, traffic analysis.
  - Impact: Although not disruptive to communication, passive attacks can expose sensitive data such as encryption keys, routing paths, or user behavior.
- **Active Attacks:**
  Active attacks involve direct actions that alter, disrupt, or fabricate communication. These are **more dangerous** as they affect the **availability, integrity, and authenticity** of the data being transmitted.
  - Example: Injecting false routing information, dropping packets, impersonation.
  - Impact: These attacks can lead to denial of service, data loss, or manipulation of routing paths.

Specific Threats in MANETs

- **Black Hole Attack:**
  In this attack, a malicious node advertises itself as having the shortest path to all destinations. Once traffic is routed through it, the node drops all packets instead of forwarding them.
  - **Effect:** Complete data loss, denial of service.
  - **Targeted Protocols:** AODV, DSR.
- **Wormhole Attack:**
  Two or more malicious nodes create a tunnel (wormhole) between them to pass packets secretly. This shortcut can mislead nodes into selecting non-optimal or insecure routes.
  - **Effect:** Routing disruption, selective forwarding.
  - **Targeted Protocols:** All routing protocols.
- **Sybil Attack:**
  A single malicious node presents multiple fake identities (nodes) to the network. It can influence network operations such as routing, voting, or resource allocation.
  - **Effect:** Compromised trust models, routing confusion, and resource exhaustion.
  - **Mitigation:** Identity verification and cryptographic authentication.
- **Denial of Service (DoS):**
  DoS attacks aim to exhaust the resources of a node or the entire network by flooding it with unnecessary requests or data packets.
  - **Effect:** Network performance degradation, unavailability of services.
  - **Examples:** RREQ flooding, routing loops.

- **Impersonation Attack:**
  In this attack, a malicious node pretends to be another legitimate node to gain unauthorized access or disrupt communication.
  - **Effect:** Loss of confidentiality, integrity, and trust.
  - **Mitigation:** Strong authentication and digital certificates.
- **Routing Table Overflow:**
  An attacker attempts to overwhelm a node by sending a large number of fictitious routes to non-existent nodes. This fills up the routing table and prevents it from storing legitimate routes.
  - **Effect:** Route discovery failures, delayed transmissions, and resource wastage.
  - **Targeted Protocols:** DSDV, OLSR.

IV. Security Requirements for Routing in MANET'S

Securing routing protocols in Mobile Ad-Hoc Networks (MANETs) is essential due to their decentralized nature and vulnerability to a wide range of security threats. To ensure reliable and trustworthy communication, routing protocols must satisfy several fundamental security requirements:

Confidentiality

Confidentiality ensures that sensitive data and control messages are not disclosed to unauthorized entities. In MANETs, nodes communicate over wireless links, which are inherently prone to eavesdropping. Secure routing must protect data packets and routing information using encryption mechanisms to prevent passive attacks such as traffic snooping and information leakage.

Integrity

Integrity guarantees that routing information and data are not altered during transmission. Attackers may try to modify routing packets to mislead nodes, cause routing loops, or divert traffic. Techniques such as hash functions, message authentication codes (MACs), and digital signatures are commonly used to detect and prevent tampering.

Authentication

Authentication verifies the identity of nodes involved in routing. Without proper authentication, malicious nodes can impersonate legitimate nodes and launch attacks such as impersonation or Sybil attacks. Secure routing protocols should incorporate strong mutual authentication mechanisms to validate both the source and the destination of routing messages.

Availability

Availability ensures that routing services remain operational even under malicious conditions. MANETs must maintain uninterrupted communication and route discovery despite attempts to flood the network or cause resource exhaustion (e.g., through DoS attacks). Security mechanisms should be lightweight and resilient, ensuring that legitimate users can access the network at all times.

Non-repudiation

Non-repudiation prevents nodes from denying their participation in a routing transaction. This is particularly important for detecting and responding to malicious behavior. Techniques such as digital signatures and logging of message exchanges provide undeniable proof of communication, enabling accountability and trust management.

Secure Key Management

Secure key management is the backbone of all cryptographic operations in MANETs. Given the lack of centralized infrastructure and the dynamic nature of the network, managing encryption keys securely is a major challenge. Key distribution, revocation, and renewal must be handled in a decentralized, scalable, and efficient manner to support authentication, encryption, and data integrity.

Together, these security requirements form the foundation of a robust and secure routing protocol in MANETs. Failing to address even one of these aspects can leave the network vulnerable to a wide array of attacks, thereby compromising its performance, reliability, and trustworthiness.

V Secure Routing Protocol Overview

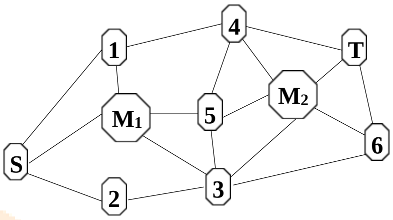

Figure 1. Example Topology: *S* wishes to discover a route to *T* in the presence of two malicious nodes, *M₁* and *M₂*.

To address the vulnerabilities of traditional MANET routing protocols, several secure routing protocols have been developed. These protocols are designed to ensure secure and reliable communication in the presence of various network threats. They differ based on routing strategies — **reactive**, **proactive**, and **hybrid** — and incorporate cryptographic and trust-based mechanisms to counter attacks.

Classification Based on Routing Behavior

- **Reactive Protocols (On-demand):**
  These establish routes only when needed, reducing overhead but increasing delay. Examples include **SAODV**, **SRP**, and **Ariadne**.
- **Proactive Protocols (Table-driven):**
  Maintain routing information at all times, ensuring low latency but at the cost of high control overhead. Examples include **SEAD** and **OLSR with IPSec**.
- **Hybrid Protocols:**
  Combine features of both reactive and proactive approaches to balance performance and efficiency. **GPSR with security enhancements** can be adapted in a hybrid manner.

Key Secure Routing Protocols

- **SAODV (Secure AODV):**
  Extension of AODV that uses digital signatures for authentication and hash chains to protect hop count. It ensures **integrity, authentication, and non-repudiation**, defending against spoofing and route manipulation.
- **ARAN (Authenticated Routing for Ad hoc Networks):**
  Uses **public key cryptography** and a trusted certificate authority (CA) to authenticate routing messages. It offers robust security against spoofing, replay attacks, and modification but incurs **high computational cost**.

- **SRP (Secure Routing Protocol):**
  Designed to work with DSR and assumes a security association between source and destination. It uses **MACs** for integrity and authenticity. SRP is lightweight but limited by the **assumption of a pre-established trust**.
- **SEAD (Secure Efficient Ad hoc Distance Vector):**
  A proactive protocol based on DSDV that uses one-way hash chains to secure sequence numbers and metrics. It is designed for environments with **limited processing resources**.
- **Ariadne:**
  Based on DSR, Ariadne uses **TESLA (Timed Efficient Stream Loss-Tolerant Authentication)** and symmetric cryptography to provide secure route discovery. It prevents various attacks like **wormholes, black holes, and tampering**.
- **OLSR with IPSec:**
  Enhances the Optimized Link State Routing protocol with IPSec to ensure **confidentiality, integrity, and authentication**. Suitable for infrastructure-based MANETs or hybrid models, though it **increases packet size and processing overhead**.
- **GPSR with Security Enhancements:**
  GPSR (Greedy Perimeter Stateless Routing) when combined with secure neighbor authentication and encryption can defend against location spoofing, Sybil attacks, and route falsification. Useful for **position-based routing** in location-aware networks.

Summary of Secure Routing Protocol Characteristics

Protocol	**Routing Type**	**Security Mechanisms**	**Strengths**	**Limitations**
SAODV	Reactive	Digital signatures, hash chains	Strong authentication and integrity	High processing cost
ARAN	Reactive	Public key infrastructure (PKI)	Strong security against spoofing	Requires CA, high overhead
SRP	Reactive	Message Authentication Codes (MACs)	Lightweight, source-destination trust	Needs prior trust, not fully scalable
SEAD	Proactive	Hash chains	Efficient for low-power devices	Limited scalability
Ariadne	Reactive	TESLA, symmetric encryption	Prevents multiple attack types	Requires time synchronization
OLSR + IPSec	Proactive	IPSec (ESP/AH)	High security in structured setups	Increases delay and header size
GPSR + Security	Hybrid	Secure location verification	Good for location-aware MANETs	GPS dependency, additional overhead

This overview highlights the diversity of secure routing strategies in MANETs, offering insights into their trade-offs between **security level, computational cost, scalability, and latency**. Selecting an appropriate protocol depends on the network's **application domain**, **threat model**, and **resource constraints**.

VI. COMPARATIVE ANALYSIS OF SECURE ROUTING PROTOCOLS

Secure routing protocols in MANETs must be evaluated based on their effectiveness and efficiency across various performance and security parameters. The following analysis compares key secure routing protocols based on **Packet Delivery Ratio (PDR)**, **End-to-End Delay**, **Throughput**, **Routing Overhead**, and **Security Level**.

Key Evaluation Parameters

- **Packet Delivery Ratio (PDR):** Ratio of packets successfully delivered to the destination.
- **End-to-End Delay:** Time taken for a data packet to reach from source to destination.
- **Throughput:** Amount of data successfully delivered over the network per unit time.
- **Routing Overhead:** Extra control packets generated by the routing protocol.
- **Security Level:** Capability to defend against various routing attacks.

Comparative Table

Protocol	PDR	End-to-End Delay	Throughput	Routing Overhead	Security Level
SAODV	High	Medium	High	High	Strong (hash, signature)
ARAN	High	High	Medium	High	Very Strong (PKI)
SRP	Medium	Low	Medium	Low	Moderate (MAC-based)
SEAD	Medium	Low	Low	Low	Moderate (hash chains)
Ariadne	High	Medium	High	Medium	Strong (TESLA, symmetric)
OLSR + IPSec	High	High	Medium	High	Strong (IPSec)
GPSR + Sec	Medium	Low	Medium	Medium	Strong (location auth)

Block Diagram: Secure Routing Protocol Comparison

```
+------------------------------+
|   Secure Routing Protocols   |
+------------------------------+
/       |       \
/        |        \
[Reactive] [Proactive] [Hybrid]
|           |         |
+--------------+     +------+     +---+------------+
|                    |                |            |
[SAODV]            [SEAD, OLSR+IPSec]    [GPSR+Sec]    ...
|                    |                |
+------------+------------+       |                |
|     Evaluation Parameters       |                |
|                                 |                |
|  -> High PDR                   |-> Low Delay     |
|  -> Medium Delay               |-> Low Throughput|
|  -> High Security (Hash + Sig)|-> Low Overhead   |
                  +--------------------------------+-----------------+
```

VI. Proposed Model

existing secure routing protocols in MANETs — such as high routing overhead, latency, and inadequate protection against coordinated attacks — we propose an enhanced secure routing protocol named **H-SAODV+ (Hybrid Secure AODV Plus)**. This model builds upon the foundation of the well-established SAODV protocol and integrates features from trust-based and cryptographic schemes to enhance **security, scalability, and efficiency**.

Overview of H-SAODV+ Protocol

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	Reserved
Query Identifier	
Query Sequence Number	
SRP MAC	

The H-SAODV+ protocol is a **hybrid secure routing approach** that combines:

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

IP Header
Basis Routing Protocol Packet
SRP Header

- **On-demand routing (from AODV)** for efficient bandwidth usage,
- **Trust-based node evaluation**, and
- **Lightweight cryptographic mechanisms** to improve real-time routing decisions under threat scenarios.

Architecture and Design

- **Routing Table Manager:** Maintains up-to-date routes with trust ratings.
- **Trust Evaluation Engine:** Assigns dynamic trust scores to nodes based on packet forwarding behavior, route reply authenticity, and historical consistency.
- **Security Module:** Implements digital signatures and hash chaining to ensure the authenticity and integrity of routing messages.
- **Intrusion Detection System (IDS):** Optional module to detect anomalies like packet dropping, fake RREQ flooding, or suspicious route alterations.

Security Mechanisms Used

- **Digital Signatures:**
  Applied to Route Request (RREQ) and Route Reply (RREP) messages to ensure authentication and non-repudiation.
- **Hash Chaining:**
  Protects hop count and prevents manipulation of routing metrics by malicious nodes.
- **Dynamic Trust Scoring:**
  Each node evaluates its neighbors based on packet delivery success, behavior over time, and consistency in routing participation. Nodes below a defined trust threshold are excluded from routing paths.
- **Timestamping & Nonce Mechanism:**
  Prevents replay attacks and ensures the freshness of routing messages.

Benefits of the Proposed Model

- **Improved Security:**
  Resistant to black hole, wormhole, and Sybil attacks through trust-based filtering and cryptographic verification.
- **Reduced Routing Overhead:**
  By using a hybrid approach and selective trust paths, the number of control messages is optimized.
- **Better Scalability:**
  Adaptable to larger and more dynamic MANET environments due to the lightweight nature of the trust computation.
- **Low Computational Load:**
  Use of symmetric cryptography and hash functions reduces the energy and processing demands on mobile nodes.

References

1. Perkins, C. E., & Royer, E. M. (1999). *Ad-hoc On-Demand Distance Vector Routing*. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (pp. 90–100). IEEE. https://doi.org/10.1109/MCSA.1999.749281
2. Johnson, D. B., Maltz, D. A., & Broch, J. (2001). *DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks*. Ad Hoc Networking, 5, 139–172.
3. Perkins, C. E., & Bhagwat, P. (1994). *Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers*. In Proceedings of the ACM SIGCOMM (pp. 234–244). https://doi.org/10.1145/190809.190336
4. Hu, Y. C., Perrig, A., & Johnson, D. B. (2002). *Ariadne: A secure on-demand routing protocol for ad hoc networks*. Wireless Networks, 11(1–2), 21–38. https://doi.org/10.1007/s11276-004-4753-6
5. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2002). *A secure routing protocol for ad hoc networks*. In Proceedings of the 10th IEEE International Conference on Network Protocols (pp. 78–87). IEEE.
6. Zapata, M. G., & Asokan, N. (2002). *Securing ad hoc routing protocols*. In Proceedings of the 1st ACM Workshop on Wireless Security (pp. 1–10). https://doi.org/10.1145/570681.570682
7. Lou, W., & Kwon, Y. (2006). *H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks*. IEEE Transactions on Vehicular Technology, 55(4), 1320–1330. https://doi.org/10.1109/TVT.2006.877445
8. Papadimitratos, P., & Haas, Z. J. (2006). *Secure message transmission in mobile ad hoc networks*. Ad Hoc Networks, 1(1), 193–209. https://doi.org/10.1016/S1570-8705(03)00017-1
9. Al-Roubaiey, A., Sheikh, R. A., & Ahmad, R. (2017). *A survey on secure routing protocols in mobile ad hoc networks*. Journal of Network and Computer Applications, 95, 50–76. https://doi.org/10.1016/j.jnca.2017.06.011