Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure Extension and Key Management for DYMO Routing Protocol (Secure DYMO)

Mohammed Mokhtar HENOUNE[1], Kadda BENYAHIA[2], Sofiane BOUKLI-HACENE[3]
[1]*EEDIS Laboratory, University of Sidi Bel Abbes Djillali Liabess, Algeria, henoune@gmail.com*
[2]*Gecode Laboratory, University of Saida Dr. Moulay Tahar, Algeria, benyahiak@gmail.com*
[3]*EEDIS Laboratory, University of Sidi Bel Abbes Djillali liabess, Algeria, boukli@gmail.com*

ARTICLEINFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that communicate with each other without any infrastructure or central authority. The mobile nodes act as both hosts and routers. There are various ad hoc routing protocols, including Dynamic MANET On-demand (DYMO). The aim of this paper is to propose an extension, called "Secure DYMO", to this protocol in order to secure routing messages. This is achieved by encrypting and decrypting routing messages to ensure authentication, integrity, and confidentiality of routing information. To accomplish this, the protocol operates in two phases. The first phase is triggered when a node joins the network and is used to exchange keys with its immediate neighbors. The second phase consists of securing the routing messages used for route discovery and maintenance. This modification impacts network performance. Our objective is to measure the effect of this cryptographic processing on DYMO's behavior under varying network density and mobility conditions.

Keywords: Dymo, Secure dymo, Power consumption, Route Overhead, Average route discovery delay.

INTRODUCTION

In MANET, the mobile nodes act as both hosts and routers, and they can join or leave the network arbitrarily. These characteristics prevent the implementation of centralized mechanisms to organize and control the behavior of the nodes, since all nodes are involved in the routing process [1]. Routing requires the participation of multiple nodes for route discovery and maintenance. The processes involved in routing are generally carried out end-to-end. However, there is no guarantee that a malicious intermediate node will not alter routing messages in order to cause routing issues (e.g., Blackhole, Wormhole, etc.). To secure the routing protocol, control messages must be protected throughout the entire routing process.

MANETS

A MANET is wireless ad hoc network; it consists of a collection of mobile nodes which self-organize using communication based on radio propagation, since there is no pre-existing infrastructure [2].

2.1 Characteristics of MANET:

- Infrastructure less Architecture: MANETs operate without any fixed infrastructure or centralized administration. Each node acts autonomously as both a host and a router, meaning it can transmit, receive, and even forward messages between two distant nodes.
- Management is distributed: Due to the absence of a central entity, network management is distributed among the nodes. Each node participates in various network management processes.
- Topology is dynamic: Nodes join and leave the network arbitrarily and move randomly. Therefore, connections between nodes are sporadic [2].

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Nodes with limited resources: In general, nodes have limited computing power and energy, which necessitates the use of optimized (resource-efficient) processing methods.
- Nodes are Self-Configurable: Nodes can automatically configure themselves without any manual intervention, making the network highly adaptable.
- Vulnerability to Attacks: Due to the open wireless medium and lack of centralized security mechanisms, MANETs are more susceptible to various attacks (e.g., eavesdropping, spoofing, and routing attacks).
- Scalability: Performance can degrade significantly as the number of nodes increases, due to overhead in routing and coordination.

2.2 Security Requirements in MANETs

The security of communications between nodes is essential to protect the network [3]. It can apply to connection establishment, routing, data transmission, and data transfer. The security requirements include, among others:

- Confidentiality: Data must only be accessible to the intended nodes. Encryption techniques are used to prevent eavesdropping and data leakage.
- Integrity: Messages must remain unchanged during their transmission between nodes. Techniques such as cryptographic hash functions (e.g., HMAC) are employed to detect tampering
- Non-repudiation: The sender cannot deny having sent the message, and the recipient cannot deny having received it.
- Authentication: It is essential to verify the identity of participants in order to prevent malicious nodes from taking part in the communication.

2.3 Major Attacks in MANETs

- Blackhole Attack: A malicious node behaves like a "black hole" by absorbing all packets that pass through it without forwarding them [4].
- Greyhole Attack: A variant of the blackhole attack, where the malicious node selectively drops packets instead of dropping all of them, making the attack more difficult to detect [5].
- Wormhole Attack: Two colluding malicious nodes establish a private link (tunnel) to secretly forward packets between distant parts of the network, effectively splitting the network into two parts and forcing traffic through their tunnel [4].
- Man-in-the-Middle Attack: A malicious node positions itself between two communicating nodes to eavesdrop on the data being transmitted. It may also impersonate either the sender or the receiver to manipulate the communication [6].
- Sybil/Spoofing Attacks: A malicious node creates multiple fake identities in order to take control of the network or disrupt its operations. It can also inject false information and impersonate legitimate nodes [7].

2.4 Routing Protocols in MANETs

Routing involves several processes based on protocols and algorithms. Its main goal is to provide the necessary information to the routing algorithm in order to select the optimal path [8]. Routing protocols in MANETs can be classified into three categories (Figure 1), based on their operational mode [9]:

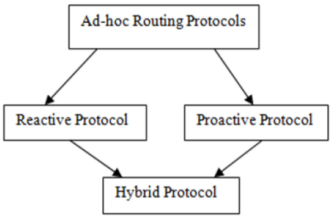

Fig. 1. MANET routing protocols [9]

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Each category offers specific mechanisms for route discovery and maintenance, with trade-offs in terms of latency, overhead, and adaptability to network changes.

2.4.1 Proactive Routing Protocols

Also known as table-driven protocols, this type of routing requires each node to maintain one or more lists called routing tables. These tables are periodically updated. When a topology change occurs, the node broadcasts a message containing the update information to all its neighbors.
However, this immediate dissemination of updates incurs a high bandwidth cost, which can negatively affect overall network performance. Despite this, it ensures accurate and up-to-date information about the network topology at any given moment [10].
These protocols provide routing paths to nodes in advance, so the route is immediately available when needed, reducing latency. One well-known protocol in this category is Destination-Sequenced Distance Vector (DSDV) [11].

2.4.2 Reactive Routing Protocols

Also known as on-demand protocols, these routing protocols establish routes only when needed. They are more efficient in terms of bandwidth usage, as they avoid creating unnecessary links. Reactive protocols typically involve two essential processes:

1. **Route Discovery:** Each node creates a table containing its direct neighbors and the cost of the links. When communication is required, it broadcasts a Route Request (RREQ) message, to which neighboring nodes respond with a Route Reply (RREP) [12].
2. **Route Maintenance:** If a link failure is detected, a Route Error (RERR) message is sent to notify other nodes, which then initiate a new route discovery process if the route is still needed [13].

Examples of Reactive Protocols:

- **DSR (Dynamic Source Routing):** The complete route is included in the packet header, eliminating the need for routing tables or periodic updates. This saves bandwidth and simplifies route management [14].
- **AODV (Ad hoc On-Demand Distance Vector**): An improvement over DSR, AODV stores the path in a routing table, avoiding the need to include the route in each data packet header (see Figure 2). It uses HELLO messages to periodically check local connectivity. Sequence numbers are used to ensure route freshness and prevent loops [15].

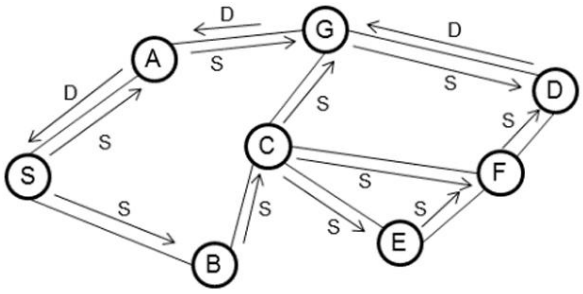

Fig. 2. Route discovery AODV [16]

- **DYMO (Dynamic MANET On-demand): A successor to AODV, DYMO combines characteristics** from both DSR and AODV. It does not use HELLO messages, relying solely on sequence numbers to ensure loop-free routes. Like all reactive routing protocols, DYMO operates based on two core processes: route discovery and route maintenance. DYMO's route discovery process (see Figure 3) is very similar to that of AODV, with the key difference being the path accumulation feature, which allows intermediate nodes to learn routes during the discovery process [17].

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

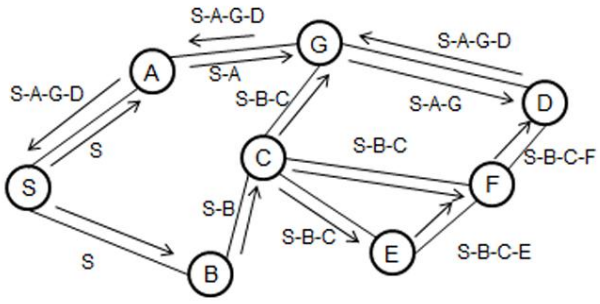

Fig. 3. Route discovery DYMO [16]

2.4.3 Hybrid Routing Protocols

Reactive and proactive routing protocols each have their own advantages and limitations. Hybrid protocols aim to combine the benefits of both approaches. They are particularly well suited to scenarios where the source and destination nodes can be efficiently located. These protocols typically divide the network into zones: If the source and destination are located within the same zone, a proactive approach is applied. If they are in different zones, the protocol switches to a reactive mechanism [18]. This adaptive strategy helps improve routing efficiency while maintaining scalability and reducing unnecessary control overhead.

SECURITY TECHNIQUES

In MANET, the mobile nodes act as both hosts and routers, and they can join or leave the network arbitrarily. These characteristics prevent the implementation of centralized mechanisms to organize and control the behavior of the nodes, since all nodes are involved in the routing process [2] Routing requires the participation of multiple nodes for route discovery and maintenance. The processes involved in routing are generally carried out end-to-end. However, there is no guarantee that a malicious intermediate node will not alter routing messages in order to cause routing issues (e.g., Blackhole, Wormhole, etc.). To secure the routing protocol, control messages must be protected throughout the entire routing process.

3.1 Authentication Techniques

Authentication is the process of verifying the identity of a node. It controls access to the network by validating the credentials of neighboring nodes stored in the routing tables. Given the absence of a central authority and the openness of wireless communication, MANETs are particularly vulnerable to impersonation, spoofing, and other identity-based attacks. One of the most widely used methods for authentication is hashing [19].
A hash algorithm is a mathematical function that transforms data of arbitrary length into a fixed-size digest, based on a secret key. This function is designed to be irreversible, meaning it is computationally infeasible to reconstruct the original message from its hash. If the recipient possesses the same key, they can verify both the authenticity and integrity of the message, thus protecting the network against tampering and spoofing attacks [20].
One commonly used hashing algorithm is MD5. It transforms variable-length messages into a fixed-size 128-bit digest. A message M is divided into 512-bit blocks. If the message length is not a multiple of 512 bits, padding is applied: a single '1' bit is added, followed by a sequence of '0' bits, and finally, the last 64 bits represent the length of original message M [21].
An alternative authentication technique involves the use of a secret key to generate a small fixed-size block of data, known as a cryptographic checksum or HMAC (Hashed Key Message Authentication Code) [22] that is appended to the message. HMAC combines the hashing algorithm (e.g., MD5 or SHA-1) with a secret key, providing a more robust method of ensuring both message integrity and authenticity.

$$HMAC(K, M) = H(K_1; (H(K_2, M)) \quad (1)$$

where: $K_1 = H(K \oplus ipad)$,

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

$$K_2 = H(K \oplus opad)$$

This technique assumes that two communicating parties, say A and B, share a common secret key K [20]. When A has a message to send to B, it calculates the HMAC as a function of the message and the key.
The message and HMAC are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new HMAC. The received HMAC is compared to the calculated HMAC (Figure 4).

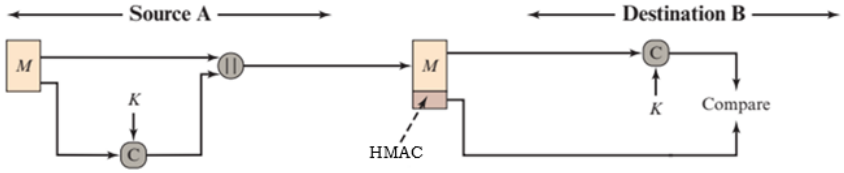

Fig. 4. Message authentication [20]

3.2 Encryption Techniques

Encryption is the process of transforming data into an unreadable form to ensure that it is only accessible to authorized parties. It requires the sharing of a secret key between the sender and the receiver. Common examples of symmetric encryption algorithms include AES (Advanced Encryption Standard) and DES (Data Encryption Standard). These algorithms are fast and efficient but rely on the prior exchange of a shared key exclusively between the source and the destination [20]. This key exchange requirement poses a significant challenge in MANETs, due to the lack of a trusted central authority to manage and distribute encryption keys securely. One widely used technique that does not require a centralized entity is the Diffie-Hellman key exchange. It allows two nodes to independently establish a shared secret key over an unsecured channel, based on mathematical operations using large prime numbers.

Algorithm:

1. Alice (A) and Bob (B) choose a prime number P et un generator G, $1 < G < P$
2. A chooses randomly a private key a, calculate $A = G^a \bmod P$.
3. B chooses randomly a private key b, calculate $B = G^b \bmod P$.
4. A and B exchange A et B.
5. A calculates shared key $K = B^a \bmod P$.
6. B calculates shared key $K = A^b \bmod P$.

Both nodes use the shared key K to encrypt and authenticate the message, ensuring that its content is recognized only by the two communicating parties. While the Diffie-Hellman exchange is theoretically vulnerable to brute-force attacks, this risk becomes negligible when sufficiently large prime numbers are used [20].

RELATED WORKS

The most crucial process in a MANET is the establishment of a route between a source node (S) and a destination node (D) to forward packets. This route should be as short as possible to reduce transmission time, and it must also be secure to prevent attacks from malicious nodes. Therefore, the optimal path is one that balances security and performance. To reduce the time required to discover the optimal path, several approaches have explored the use of authentication techniques to identify and select trusted nodes. These trusted nodes are prioritized during route discovery to minimize risk and increase efficiency. Here are some notable works:

- The work in [23], propose an authentication technique to provide secure communication by increasing the reliability of the nodes. Cluster structure is used for authentication technique of the proposed technique and cluster head acts as a certificate authority and is managed authentication information of member nodes. The performance of the proposed technique was confirmed by experiments.
- In [24], they propose an authentication technique without use of any trusted third party (TTP) or Certifying Authority (CA). Clustering provides an effective way to divide network to make the areas within which routing

is performed and overhead is also reduced. For mutual authentication of nodes, clustering is used with keys and unique identity numbers together provides authentication and the cluster heads will account for mobility. This will restrict the malicious nodes to enter into the network and thus reduces the chances of attack.

- The research of [25] presents a robust and secure mechanism for authentication of nodes in the MANET. The proposed authentication protocol is based on certificate exchange between the nodes. This protocol also uses digital signature with a hash function to maintain the authenticity of certificates. Simulation shows that this protocol shows better performance in terms of throughput, end-to-end delay and packet dropping in presence of malicious nodes in the MANET. In addition, it also has less computation and communication overhead, which makes it suitable for MANETs.
- The paper of [26] presents a robust and efficient key exchange protocol for nodes authentication in a MANET based on multi-path communication. Simulation results demonstrate that the protocol is effective even in presence of large fraction of malicious nodes in the network. Moreover, it has a minimal computation and communication overhead that makes it ideally suitable for MANETs.
- The paper by [27], focus on a system that uses a trust model and SHA-1 key encryption. The system is designed to detect and avoid malicious nodes in the network. The trust value is built based on the previous experiences and recommendations of other nodes in the network. The efficiency of trust system is enhanced by using SHA-1 encryption authentication mechanism when nodes enter into the network.
- In [28], they propose a lightweight authentication protocol, which utilizes one-way hash chain to provide effective and efficient authentication for communications between neighboring nodes in MANETs. The security properties and performance are also analyzed in the paper. The analysis shows that the protocol incurs low overhead penalty and achieves a tradeoff between security and performance.
- An efficient initial access authentication protocol proposed in [29] which realizes the authentications and key distribution through least roundtrip messages. They propose efficient initial access authentication mechanism over MANET that is more efficient than any message authentication method in the literature. The key idea behind the proposed method is to provide efficient initial authentication as well as to provide secure message passing between Mobile user and authentication server. Furthermore, a simple and practical method is presented to make compatible with MANET.
- The research by [19] aimed to develop a new model based on DYMO protocol where a modification was proposed to route discovery and route maintenance processes. In route discovery process they made an authentication process between the nodes by using MD5 hashing algorithm, then they used reinforcement learning to improve the route maintenance process based on machine learning approach. The results show improvement in the performance of MANETs, despite the little increased in the end-to-end delay in comparison with DYMO protocol.
- In [30] attempts to develop a mitigation algorithm to avoid and prevent genuine nodes from malicious attack. The complete experimental setup concludes that improvement in mobile node increase the network performance but also increase the black hole impact. Subsequently, improvement in node speed degrades the black hole impact.
- In [31], they proposed SEDYMO a new security protocol extension for DYMO that offers integrity, authenticity and non-repudiation. Its security mechanisms are based on digital signatures (simple, multiple or aggregate) and hash chains. They assume a distributed Certificate Authority (CA) that issues authorization certificates to control the access to the resources of the network.
- The authir of [32] exploits the fact that DYMO is based on AODV to adopt the security extension of that protocol SAODV to its data structure. However, SDYMO does not protect that part of DYMO protocol that differs from AODV (that is, routing information from intermediate nodes is not secured). Therefore, SDYMO can be considered equal to SAODV.

PROPOSED MODEL

The proposed protocol, Secure DYMO, is an extension of the DYMO routing protocol. It aims to secure the routing messages themselves and to manage encryption keys efficiently. Each node maintains, in addition to its routing table, three additional tables: a direct neighbor table, a trust table, and a revocation table. The neighbor table

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

contains the ID of each direct neighbor, the shared key, and the ID of the neighbor's guardian. The revocation table lists malicious nodes reported by their guardians. A guardian is a node responsible for attesting the authenticity of another node. In addition, a global key must be maintained across all nodes for network-wide operations.
The choice of symmetric cryptographic algorithms (AES for encryption and HMAC-MD5 for authentication) is motivated by their low computational cost, reduced energy consumption, and low memory usage, which makes them more suitable for resource-constrained MANET environments than asymmetric algorithms used in protocols like SDYMO or SEDYMO. It should be noted, however, that cryptographic processing introduces latency in packet transmission, depending on the complexity of the algorithm. Specifically, HMAC-MD5 adds 16 bytes to the size of each packet. While MD5 is known to have certain vulnerabilities, attacks on HMAC-MD5 have not been shown to pose practical threats when used as a message authentication code [22].
Our proposed Secure DYMO protocol operates in three main phases:

5.1 Joining Phase:

This phase is triggered when a new node joins the MANET. Its objective is to establish secure communication channels with direct neighbors.
Initially, the new node manually obtains the global network key from a neighboring node, referred to as its guardian. If the new node has not been previously revoked, the guardian broadcasts an encrypted and authenticated message (using the global key) indicating the presence of a legitimate new member and identifying itself as the node's guardian. Next, the new node broadcasts an encrypted HELLO message (using the global key) containing its ID to its neighbors. Upon receiving the HELLO message, neighboring nodes decrypt it to verify the authenticity of the new node. If the node is validated, each neighbor i responds with an $ECHO_i$ message, also encrypted with the global key, containing the identity of their own guardian. Through this "HELLO-ECHO" exchange, both the new node and its neighbors recognize and validate their mutual presence and trust.
Finally, the new node initiates a peer-to-peer Diffie–Hellman key exchange with each direct neighbor. This key exchange is encrypted and authenticated using the global key, and the resulting shared key is stored in the neighbor table. This key protects the direct channel between the new node and each neighbor. As a result, man-in-the-middle attacks are mitigated (see Figure 5). The HELLO-ECHO exchange is repeated every 10 seconds to account for node mobility and dynamic topology changes.

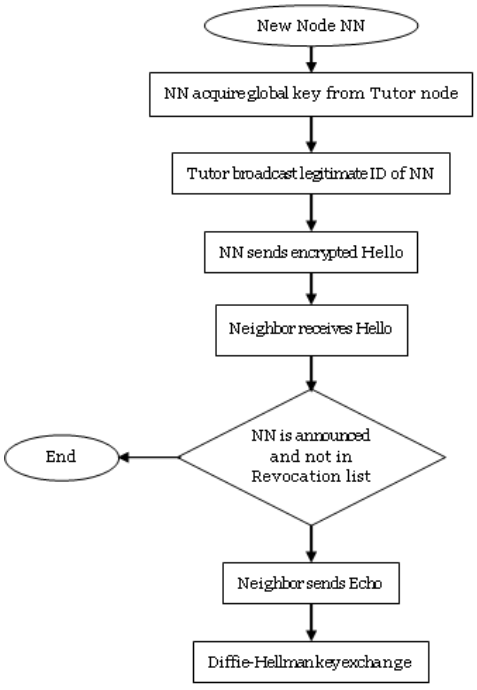

Fig. 5. New Node Joining Phase

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5.2 Routing Phase:

In this phase, all routing packets circulating within the MANET are protected. The DYMO protocol operates as specified in its standard [33], with the integration of an added security layer.
A point-to-point AES encryption (128-bit key) is applied to ensure the confidentiality of routing information, while an HMAC-MD5 hashing function is used to provide point-to-point authentication and integrity (see Figure 6). Each routing message (RREQ, RREP, and RERR) is thus encrypted and authenticated between every pair of neighboring nodes, preventing eavesdropping, tampering, and impersonation attacks during the route establishment process. During this phase, any packet coming from a node listed in the revocation table, is ignored and excluded from the routing path. As a result, if no secure path can be established, the discovery is aborted to prevent communication through untrusted nodes.

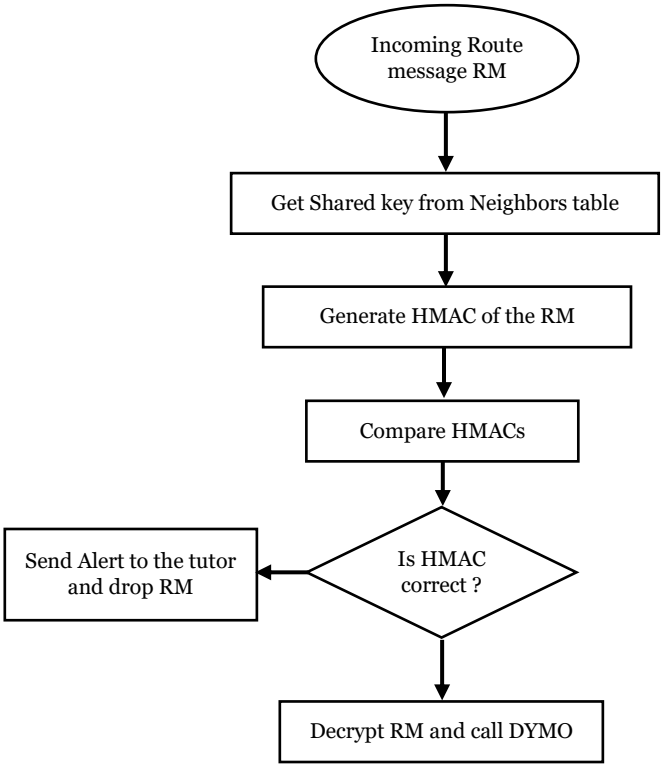

Fig. 6. Routing phase

5.3 Revocation Management

If a node detects an incorrect hash in a message received from a neighbor, it considers that neighbor suspicious and must send a report message to the guardian of the peer. The guardian then consults its trust table and decrements the trust counter (initially set to 3) associated with the suspicious node. This counter reflects the number of trusted nodes that have detected the misbehavior. If the counter reaches zero, the guardian broadcasts a revocation message indicating that the node is considered malicious. Upon receiving this revocation message, every node:

1. Terminates all current and future communication with the malicious node,
2. Adds it to the revocation table
3. Generates a Route Error (RERR) message to trigger the DYMO route maintenance process and reroute data away from the revoked node (see Figure 7).

This approach ensures that revocation is progressive and evidence-based, preventing false accusations while maintaining the integrity and security of the routing process.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

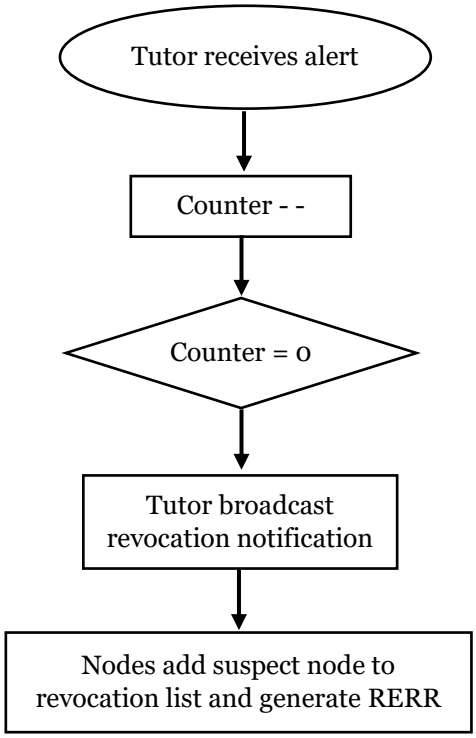

Fig. 7. Revocation process

PERFORMANCE EVALUATION

To evaluate the impact of the cryptographic processing introduced by Secure DYMO on network performance, we opted for simulation-based analysis.

6.1 Security analysis

The Secure DYMO protocol is built upon three complementary layers of security, each addressing a specific security requirement in mobile ad hoc networks:

- **Diffie–Hellman Key Exchange:** A robust and widely used mechanism for generating a shared secret key between two nodes without requiring a trusted third party. It enables the secure establishment of pairwise encryption keys, even in a decentralized and dynamic network such as a MANET.
- **AES (Advanced Encryption Standard):** Used to ensure the confidentiality of routing packets. With a 128-bit symmetric key, AES encrypts routing messages so that they cannot be intercepted or read by unauthorized nodes.
- **HMAC-MD5 (Hash-based Message Authentication Code):** Provides message authentication and integrity. Each routing message is accompanied by a 128-bit digest that allows receiving nodes to verify that the message has not been altered and that it originates from a legitimate source.

Together, these three mechanisms form a multi defense strategy against common attacks in MANETs, such as eavesdropping, message tampering, spoofing, and man-in-the-middle attacks:

- **Blackhole Attack:** In this attack, a malicious node advertises a false short route to attract all traffic, which it then discards or intercepts. Secure DYMO foil this attack because the attacker cannot forge a RREP since HMAC-MD5 validates the authenticity of the message; The routing message content (e.g., destination, metric) is encrypted using AES, making it unreadable without the key. Without access to the correct key or HMAC, the attacker cannot interpret or manipulate routing messages.
- **Wormhole Attack:** Two colluding attackers establish a private tunnel (wormhole) to falsely appear as a shortcut in the network. This attack is difficult because all packets are encrypted (AES), preventing attackers

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

from reading or modifying any useful fields. In addition, the HMAC validates message authenticity and integrity and any tampering is immediately detected. In consequence, fields like TTL or hop count cannot be falsified. Since packets are unreadable and unalterable, no routing data is usable by attackers to build a tunnel.

- **Spoofing Attack:** An attacker impersonates another node, by forging its address or identity. Secure DYMO elude this by HMAC as it is computed using a unique pairwise key between neighboring nodes. Without this key, the attacker cannot generate a valid HMAC. The node identity is cryptographically bound to its key, preventing identity spoofing or Sybil attacks.
- **Message Alteration / Route Forging:** An attacker modifies routing messages in transit (e.g., alters hop count or destination) to mislead route computation. In Secure DYMO all routing messages are AES-encrypted, making fields unreadable and inaccessible to attackers. Any modification invalidates the HMAC, causing the packet to be discarded. Message integrity is guaranteed, and tampering is detected immediately.
- **Replay Attack:** The attacker reuses a previously valid routing message (e.g., old RREQ or RREP) to disrupt the routing logic. Fields such as sequence numbers and TTL are protected by the HMAC. So Replayed messages are detected due to invalid or outdated HMACs and are rejected.
- **Man-in-the-Middle Attack:** An attacker intercepts, alters, and forwards messages to manipulate communication between nodes. Secure DYMO forestall this attack applying security mechanisms: AES ensures message confidentiality, so attackers cannot understand the payload. HMAC prevents undetected alterations to the message. The global key protects the Diffie-Hellman key exchange, preventing key interception. Thus, Secure DYMO blocks man-in-the-middle attempts entirely.
- **Eavesdropping (Sniffing):** Is the passive interception of routing packets to gain information about the network. Confidentiality is guaranteed, without the key, the intercepted data is unreadable. All routing packets are encrypted using AES.
- **Flooding Attack (Resource Exhaustion):** The attacker floods the network with fake routing messages to overwhelm nodes and links. In Secure DYMO, HMAC-MD5 authentication filters out unsigned or incorrectly signed packets. Thus, only legitimate nodes can inject valid routing messages into the network.

6.2 Experimentations and discussions

The simulation scenarios were conducted using OMNeT++ v6.1.0 with the INET Framework v4.5.4, on Ubuntu 22.04 LTS 64-bit system. The simulation parameters were varied according to network density and node mobility, in order to reflect real-world use cases:

- **Network densities** were set to: **10** nodes (sparse network), **20** nodes (medium density), and **30** nodes (high density).
- **Mobility scenarios** were chosen to match realistic operational contexts: **3** m/s, representing the average speed of a running soldier on foot, **17** m/s, corresponding to a combat tank on rough terrain, **25** m/s, representing an armored personnel carrier (APC).

6.2.1 Simulation Environment

The simulations were conducted to evaluate the performance impact of cryptographic mechanisms integrated into the Secure DYMO protocol, in comparison with standard DYMO. The hardware characteristics of the simulation environment are as follows:

- Hardware Specifications:
  - Processor: Intel Core i5 – 1035G1 @ 1.0 GHz
  - Memory: 8 GB RAM
  - Operating System: Ubuntu 22.04 LTS (64-bit)
- Simulation Scenarios:
  - Simulation area: 800 m × 800 m
  - Simulation time: 300 seconds
  - Node speed: 3 m/s, 17 m/s, 25 m/s
  - Number of nodes: 10, 20, 30

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Mobility model: Random Waypoint
- Traffic pattern: CBR (Constant Bit Rate) – 10 connections
- Bandwidth: 54 Mbps
- Transmission range: 200 meters
- Routing protocols evaluated: DYMO and Secure DYMO

6.2.2 Performance Metrics:

Three criteria are evaluated to compare the performance of DYMO and Secure Dymo based on the **density** (number of nodes) and **mobility** (node speed) of the MANET [34]:

- **ARDD (Average Route Discovery Delay)** to assess the impact on network latency;
- **PC (Power Consumption)** to determine the energy overhead caused by securing the packets
- **RO (Route Overhead)** to measure the routing overhead introduced by the secure routing protocol.

The results highlight the impact of implementing the previously discussed security mechanisms (AES, HMAC-MD5, and key management) on the overall network performance:

1. **Average Route Discovery Delay (ARDD):** This metric represents the average time required to establish a route between a source and a destination node. It reflects the responsiveness of the routing protocol in discovering valid paths.

$$ARDD = \sum \frac{\mathrm{RREP_i - RREQ_i}}{\mathrm{NRD}} \quad (2)$$

where: $RREQ_i$: Time at which the i-th Route Request was sent
$RREP_i$: Time at which the corresponding Route Reply was received
NRD: Total number of successful route discovery attempts

2. **Power Consumption:** This metric represents the total energy consumed by all nodes in the network during the simulation. It includes the energy used for packet transmission and reception, as well as the processing cost of cryptographic operations (AES encryption, HMAC-MD5 hashing). It is a critical factor in MANETs, where nodes often rely on limited battery resources. Higher energy consumption may indicate **inefficient protocol behavior** or the **computational cost** of security mechanisms such as encryption and hashing.

$$EC = \sum (Energy_i^{start} - Energy_i^{end}) \quad (3)$$

where: $Energy_i^{end}$: Remaining battery level of node i at the end of the simulation
$Energy_i^{start}$: Initial battery level of node i

3. **Routing Overhead:** This metric represents the amount of bandwidth consumed by control packets and cryptographic operations during route discovery and maintenance. It reflects the protocol's efficiency in managing the network topology and securing routing communications. A higher routing overhead indicates greater security cost, which can impact network performance.

$$RO = \sum RPacket_i + \sum KeyExchange_i \quad (4)$$

where: $\sum RPacket_i$: Remaining battery level of node i at the end of the simulation
$\sum KeyExchange_i$: Initial battery level of node i

6.2.3. Simulations results

Table 1 summarizes the average cryptographic processing time and energy consumption for a given packet size. These tests were conducted on a smartphone equipped with a mid-range processor (ARM Cortex-A55). The measured time and energy were integrated into the simulator to simulate the delay and power consumption

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

induced by cryptographic calculations with a fluctuation of 5%. For energy modeling; all nodes start the simulation with fully charged batteries.

Tab. 1. Cryptographic processing delay and energy consumption per packet size

Size (B)	AES delay (ns)	HMAC delay (ns)	AES and HMAC Energy (nJ)
32	51.81344261	688.8544715	0.31370225035158089133
48	61.73591389	695.0577686	0.32825544753283986132
64	77.75327434	801.7072685	0.61446832543093166112
80	95.56408752	811.9891632	0.62902152261219057561
96	113.97585310	846.1451714	0.64357471979344949009
112	132.54775530	879.0762711	0.65812791697470840457
128	150.94518800	1001.9970270	0.94434079487280031540
144	170.19257400	1016.2096800	0.95889399205405922988
160	188.35333960	1051.8497730	0.97344718923531814436
176	205.81289710	1096.1656150	0.98800038641657705885
192	224.92207060	1168.5741770	1.27421326431466885865

We applied the parameters (number and speed of nodes) to the MANET in order to compare the performance metrics (ARDD, Power Consumption, and Routing Overhead). The simulation was carried out across nine different scenarios, varying in network density and mobility. At the end, we calculated the overall degradation for each performance metric of the Secure Dymo protocol in comparison to the original DYMO protocol.

Scenarios of 10 nodes:

As shown in table 2 and figure 8: For low mobility, RO of Secure Dymo introduces only a slight increase of 0.47%. This indicates that the addition of 16 bytes per routing packet does not significantly impact the overall volume of routing data. In addition, routing packets has a limited propagation due to low density. However, we observe a 25.19% increase in the ARDD for Secure Dymo. This increase is mainly due to the cryptographic processing time (generation and verification of HMAC, AES encryption/decryption), in addition to route unavailability. Even in a relatively stable topology, route discovery delay is noticeably affected. Regarding EC, there is only a minimal increase of 0.27%, showing that the energy impact of encryption remains negligible at low speed. In this type of topology, Secure Dymo proves to be energy-efficient. Overall, Secure Dymo adds a security layer with very low energy cost and a moderate delay overhead, making it suitable for low-mobility networks (such as IoT or static sensor environments).

Tab. 2. Simulation results in low node density

Speed	Protocol	RO	ARDD	EC	Penalty (RO)	Penalty (ARDD)	Penalty (EC)
3	Dymo	4562848	1.58772184787100	6.47298418513275	0.47%	25.19%	0.27%
	Secure Dymo	4584124	1.98772184787100	6.49038170392009			
17	Dymo	15701096	1.34357754264000	7.81314101195762	30.00%	14.22%	1.25%
	Secure Dymo	20412108	1.53466958146299	7.91047721430713			
25	Dymo	29458394	1.57029698055599	7.33652640131409	16.71%	8.18%	1.39%
	Secure Dymo	34381984	1.69870831569899	7.43883636579188			

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

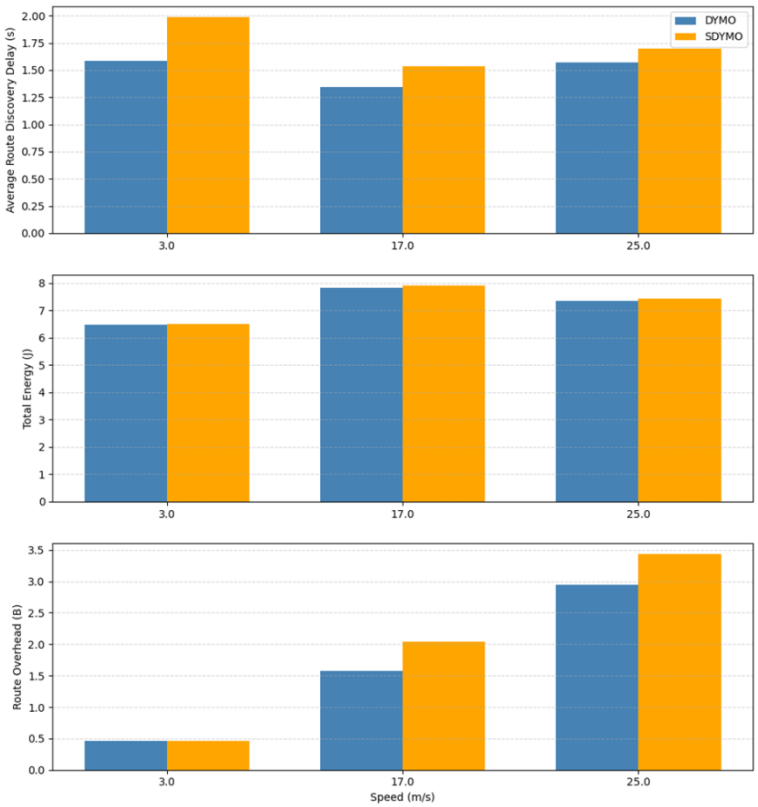

Fig. 8. DYMO vs SecureDYMO - 10 nodes

At a medium speed (17 m/s), RO experiences a significant increase of 30%. The unstable topology forces Secure Dymo to send more routing messages (secured RREQ and RREP), and the accumulation of security extensions in the packets considerably increases control traffic. For the ARDD, there is a 14.22% increase, reflecting a double penalty due to cryptographic processing and the frequent reconstruction of routes. The secured network loses responsiveness, which can be critical for real-time applications. However, EC increases by only 1.25%. While cryptographic processing begins to have a slight impact, Secure Dymo remains energy-efficient, even with the additional control traffic. In summary, Secure Dymo becomes more costly in terms of bandwidth and delay at medium mobility, but it still maintains better energy efficiency.

At high speed (25 m/s): the RO increases by 16.71%, which is lower than at 17m/s. This can be explained by the higher instability of the topology, leading to more frequent route re-establishments, but fewer routing messages overall. Although the overhead remains significant, it is relatively controlled. The ARDD rises by only 8.18%, much lower than the increase observed at 17 m/s. This suggests that the rapid topological changes actually help reduce route discovery time. At high mobility, Secure Dymo becomes more competitive in terms of responsiveness. Finally, EC increases by 1.39%, remaining stable even under extreme mobility conditions. This demonstrates good energy resilience despite high node speeds. Overall, Secure Dymo shows better balance at high mobility, where the cost of security is offset by shorter route durations. The security-performance trade-off becomes more acceptable as mobility increases.

In such a topology, Secure Dymo is a strong candidate for MANETs where security is critical, provided that a slight increase in latency and a moderate overhead in bandwidth, are acceptable, in exchange for excellent energy efficiency.

Scenarios of 20 nodes:

The table 9 and figure 3, show result in scenarios under low mobility, Secure Dymo generates 33.36% more routing traffic than standard DYMO. This sharp increase in RO stems from the higher node density, which leads to a

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

greater number of possible paths to secure, and thus more routing control messages to process. The cryptographic layer introduces a significant overhead.

Tab. 3. Simulation results in medium node density

Speed	Protocol	RO	ARDD	EC	Penalty (RO)	Penalty (ARDD)	Penalty (EC)
3	Dymo	28766668	2.03895831570899	15.77095741456520	33.36%	16.41%	0.45%
	Secure Dymo	38364502	2.37363870265099	15.84262917480810			
17	Dymo	112340066	2.45380643202100	18.92727024306320	15.11%	7.45%	6.40%
	Secure Dymo	129316974	2.63650597953800	20.13827891061790			
25	Dymo	149526984	2.14359330333399	19.91067286811490	35.07%	8.53%	6.40%
	Secure Dymo	201972484	2.32652515379699	21.18568488190410			

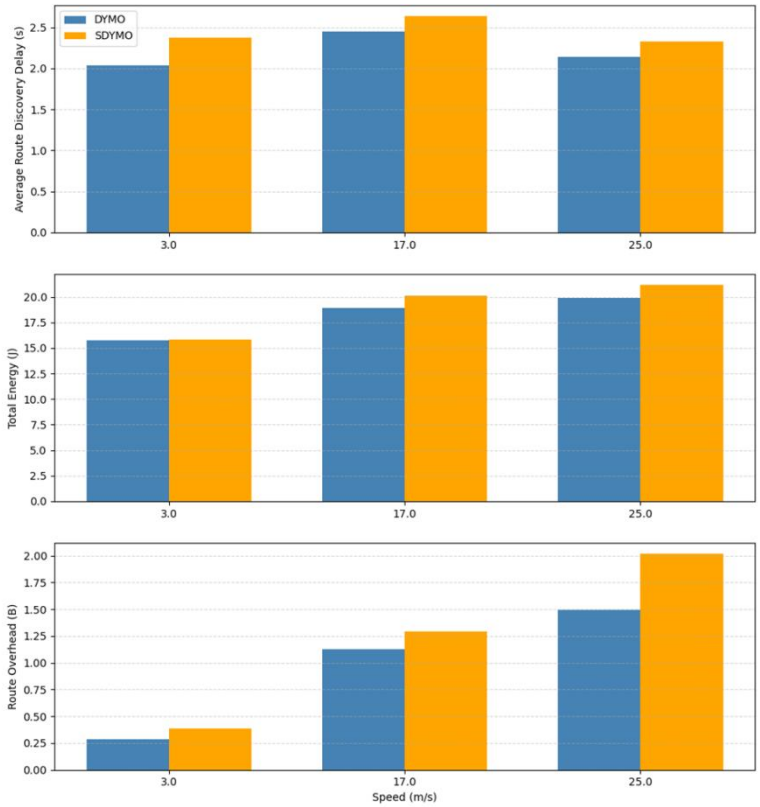

Fig. 9. DYMO vs SecureDYMO - 20 nodes

The ARDD increases by 16.41%, which is consistent with the 10-node scenario. The delay is mainly caused by cryptographic processing (AES encryption and HMAC generation), though the stable topology helps contain the impact. This performance penalty remains manageable in low-mobility environments.The EC increases by only 0.45%, indicating that the added security is still energy-efficient, even as the network scales up. Secure Dymo demonstrates good energy scalability in denser but static networks.

At moderate speed (17 m/s), the RO increases by 15.11%, which is lower than the increase observed at 3 m/s. This is due to more unstable routes leading to shallower propagation of control packets, reducing accumulated traffic. However, Secure Dymo still incurs higher overhead than DYMO.For ARDD, there's a moderate increase of 7.45%, which is lower than in the 10-node setup. The performance gain can be attributed to increased route redundancy,

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

which reduces the need for route recalculation. Secure Dymo starts to show better adaptability to moderate mobility. The EC increases by 6.40%, a noticeable rise due to more frequent cryptographic verifications. This marks the first significant energy penalty, driven by both the higher node count and increased mobility.
In high mobility scenarios (25 m/s), RO jumps by 35.07%. The combination of high node density and speed causes frequent route breaks, resulting in a flood of encrypted routing messages (RREQ, RREP, RERR). The overhead is high but expected in such dynamic topologies. Despite the instability, ARDD only increases by 8.53%, suggesting that Secure Dymo maintains a delay close to DYMO, benefiting from route redundancy that accelerates recovery.EC rises again by 6.40%, identical to the 17 m/s case. This shows that energy consumption remains stable, and encryption does not become exponentially more expensive under high mobility.
Overall, Secure Dymo remains energetically robust even in unstable conditions. However, the routing overhead becomes considerably heavy—especially in static topologies—making it crucial to justify the added security, particularly in bandwidth-sensitive applications.

Scenarios of 30 nodes: This scenario simulates a high-density MANET, and the results are summarized in table 4 and figure 10.

Tab. 4. Simulation results in high node density

Speed	Protocol	RO	ARDD	EC	Penalty (RO)	Penalty (ARDD)	Penalty (EC)
3	Dymo	77292826	4.52627452628699	28.2668407167861	32.66%	4.26%	3.86%
	Secure Dymo	102535200	4.71893697682000	29.3572210178066			
17	Dymo	267570864	4.13575412027400	35.3201744013556	11.52%	1.87%	1.92%
	Secure Dymo	298407086	4.21296805072600	35.9979333472397			
25	Dymo	455621366	3.96603249107799	37.7237944387632	14.37%	12.35%	1.94%
	Secure Dymo	521107160	4.45584461883800	38.4552706992439			

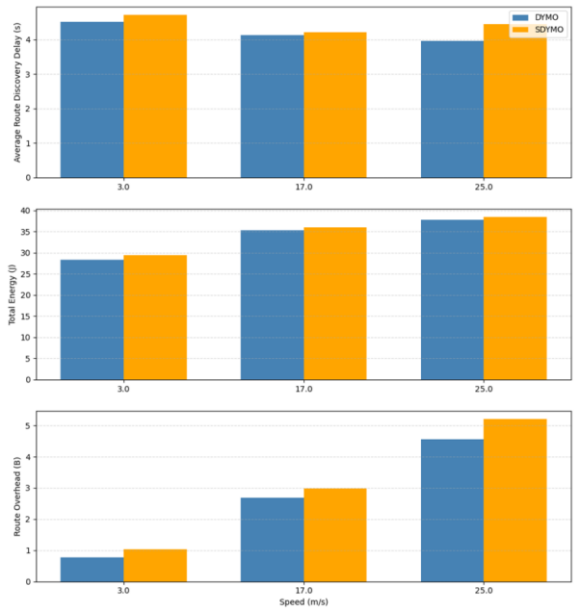

Fig. 10. DYMO vs SecureDYMO - 30 nodes

In the case of low mobility, Secure Dymo incurs a 32.66% overhead in RO. The dense and low-mobility network leads to many secure control messages (due to HMAC accumulation on each route). The impact is comparable to

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the 20-node topology at low speed. For ARDD, the overhead is only 4.26%, which is significantly lower than with 10 or 20 nodes. This can be explained by the wide availability of alternative paths, compensating for delays caused by encryption. This reflects good resilience of the secure protocol in high-density, low-mobility scenarios. For EC, the overhead is 3.86%, which is higher than in previous topologies since each node processes more messages and cryptographic operations. The energy penalty becomes noticeable, yet remains acceptable.

With medium mobility, RO increases moderately by 11.52%. While mobility disrupts routes, the protocol avoids a traffic explosion, showing improved efficiency at this mobility level. ARDD is only slightly penalized (+1.87%), thanks to path redundancy and dense mesh connectivity, which help offset cryptographic delays. Secure Dymo becomes nearly as fast as DYMO. The most favorable result is in EC, with only a 1.92% increase. This indicates that the energy cost of encryption is absorbed thanks to stable network dynamic and effective packet diffusion. This reflects a very good security/energy tradeoff.

At high mobility (25 m/s), RO overhead is 14.37%, consistent with previous results. The highly unstable routes require frequent rediscoveries, but Secure Dymo remains within reasonable bounds, showing good adaptability in highly mobile environments. For ARDD, there is a significant overhead of 12.35%. At this speed, cryptographic processing combined with topological instability causes cumulative delays. While there is a noticeable degradation in latency, it remains acceptable in certain use cases. EC shows a steady overhead of 1.94% (same as at 17 m/s), indicating that cryptographic processing is energy-efficient regardless of speed. Secure Dymo is robust in terms of energy consumption even under high mobility.

In summary, Secure Dymo remains effective in dense networks despite the increase in control traffic. It provides strong security with limited impact on energy and moderate impact on latency, especially at medium speed. However, the RO penalty remains significant at low speed and should be considered when bandwidth is limited.

6.2.4 Results synthesis

Based on the results, it can be observed that the Secure Dymo protocol consistently penalizes network performance compared to standard Dymo, with variations depending on node speed and network density. The Average Route Discovery Delay and energy consumption increase because routing packets undergo cryptographic processing, and their size is extended by 16 bytes due to the HMAC-MD5. This requires more transmission time and energy. The Routing Overhead also increases as a result of the larger packet size introduced by the authentication tag (HMAC-MD5).

Security vs. Cost Trade-off: Secure Dymo introduces strong protection against blackhole, wormhole, spoofing, and packet modification attacks, thanks to the use of HMAC-MD5 and AES cryptography. This security enhancement:

- Increases Routing Overhead significantly, by up to 35% depending on network density and node speed,
- Moderately impacts ARDD, as HMAC-MD5 and AES require additional CPU processing time, except in low-speed or low-density scenarios,
- Remains highly energy-efficient, with less than 6.5% increase in power consumption in all cases.

Impact of Node Density:

- Secure Dymo adapts better to denser networks (20–30 nodes), where the latency penalties decrease significantly.
- Starting from 30 nodes, route redundancy helps compensate for the delays caused by cryptographic processing.

Impact of Mobility:

- At low mobility, the accumulation of secure routing messages leads to high routing overhead.
- At medium to high speeds, Secure Dymo remains efficient, as the routes are short-lived and unstable; this limits the accumulation of overhead.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6.2.5 Overall Performance Degradation: Globally, the performance degradation of Secure Dymo compared to the standard Dymo protocol is:

- Average Route Discovery Delay (ARDD): +9.17%
- Power Consumption (PC): +2.97%
- Routing Overhead (RO): +18.43%

CONCLUSION

This study aimed to evaluate the performance of the Secure Dymo protocol, a secured extension of the DYMO protocol, through three network topologies (10, 20, and 30 nodes) and various mobility speeds (3, 17, and 25 m/s). Three key performance metrics were analyzed:

- RO (Routing Overhead): control traffic generated for routing (in bytes)
- ARDD (Average Route Discovery Delay): average delay in establishing a route
- EC (Energy Consumption): total energy consumed

Secure Dymo represents a robust and efficient solution for securing communications in MANETs while maintaining moderate energy consumption. Despite a predictable increase in control traffic, its performance remains satisfactory starting from 20 nodes, and especially stable under medium to high mobility conditions. Thus, Secure Dymo is particularly recommended in scenarios:

- With high security requirements (e.g., military or emergency networks)
- In reasonably dense node environments
- Where energy consumption is a critical constraint

Secure Dymo provides a balanced and effective approach to secure routing in mobile ad hoc networks. Although it introduces a control traffic overhead of 20.10%, this is offset by enhanced robustness against attacks, low energy overhead (2.97%), and a moderate latency increase (10.85%). Its stability improves significantly in dense topologies, especially under medium or high mobility conditions.

Therefore, Secure Dymo is a relevant choice for critical applications where security and energy efficiency are essential, such as emergency response, military operations, or decentralized IoT networks.

REFRENCES

[1] Gupta, A., Verma, P., &Sambyal, R. (2018). An overview of MANET: features, challenges and applications. Proceedings of the National Conference on recent advancement in Computer science and IT, 4(1), 122–126. https://doi.org/10.32628/IJSRCSEIT

[2] Naghshegar, A., Darehshoorzadeh, A., & Dana, A. (2008). Dynamic topology control scheme in MANETs for AODV routing. Australasian Telecommunication Networks and Applications Conference, IEEE, Australia. 246–251. https://dx.doi.org/10.1109/ATNAC.2008.4783331

[3] Hongmei, D., Wei Li, & Dharma P. A. (2002). Routing Security in wireless Ad Hoc Networks. IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks,40(10), 70–75. http://dx.doi.org/10.1109/MCOM.2002.1039859

[4] Dhanke J., Rastogi, S., Singh, K., Saxena, K., Kumar, K., & Mishra, P. (2024). An Efficient Approach for Prevention of Blackhole Attack in MANET. International Journal of Intelligent Systems and Applications in Engineering. 12(12s), 743–752.

[5] Dhende, S. L., Shirbahadurkar, S. D., Musale, S. S., &Galande, S. K. (2018). A survey on black hole attack in mobile adhoc networks. Proceedings of the 4th International Conference on Recent Advances in Information Technology (RAIT), IEEE, India, 1–7. http://dx.doi.org/10.1109/RAIT.2018.8389073

[6] Sowah, R., Kwadwo B., Mills, G., & Koumadi, K. (2019). Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in artificial neural networks (ANN). Journal of Computer Networks and Communications, 2019(1), 1–14. https://doi.org/10.1155/2019/4683982

[7] Douceur, J.R. (2002). The sybil attack, in Peer-to-peer Systems. IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, 251–260. https://doi.org/10.1007/3-540-45748-8_24

[8] Ferdaus, J., &Salihi, R. (2014). Routing: internet routing protocols and algorithms. Academic Paper, 1–20. http://dx.doi.org/10.13140/RG.2.1.4341.1680
[9] Agrawal, K., Jain, S. (2014). Simulation Based Performance Comparison of Ad hoc Routing Protocols. International Journal of Engineering Research and Applications (IJERA), AET-2014, 10–15.
[10] Venkatesan, T.P., Rajakumar, P. &Pitchaikkannu, A. (2014). Overview of proactive routing protocols in MANET. Proceedings of the 4th International Conference on Communication Systems and Network Technologies, IEEE, India, 173–177. http://dx.doi.org/10.1109/CSNT.2014.42
[11] Mahdipour, E., Rahmani, A. M., &Aminian, E. (2009). Performance evaluation of destination-sequenced distance-vector (DSDV) routing protocol. Proceedings of the International Conference on Future Networks, IEEE, Thailand. 186–190. http://dx.doi.org/10.1109/ICFN.2009.51
[12] Johnson, D.B., & Maltz, D.A. (1996). Mobile Computing. Dynamic Source Routing in Ad Hoc Wireless Networks. Tomasz Imielinski, Henry F. Korth. The Kluwer. International Series in Engineering and Computer Science (353). Springer, Boston, MA. https://doi.org/10.1007/978-0-585-29603-6_5
[13] Khatri, P., Rajput, M., Shastri, A. &Solanki, K. (2010). Performance Study of Ad-Hoc Reactive Routing Protocols. Journal of Computer Science, 6(10), 1159–1163. https://doi.org/10.3844/jcssp.2010.1159.1163
[14] Alaparthi, S., Parvataneni, S., Vaishnavi, C., Sathvika, P., Chandrika, M., & Sharanya, P. (2019). Dynamic source routing protocol – a comparative analysis with AODV and DYMO in ZigBee based wireless personal area network. Proceedings of the 6thInternational Conference on Signal Processing and Integrated Networks (SPIN), IEEE, India, 1042–1046. http://dx.doi.org/10.1109/SPIN.2019.8711689
[15] Liu, S., Yang, Y., & Wang, W. (2013). Research of AODV routing protocol for ad hoc networks. Proceedings of the AASRI Conference on Parallel and Distributed Computing and Systems, 5, 21–31. https://doi.org/10.1016/j.aasri.2013.10.054
[16] Hamamreh, R. A., Ayyad, M., Jamoos, M. (2019). RAD: Reinforcement Authentication DYMO Protocol for MANET. International Conference on Promising Electronic Technologies (ICPET 2019) Gaza, Palestine, 136–141. http://dx.doi.org/10.1109/ICPET.2019.00032
[17] Hamamreh, R. & Salah, O. (2018). An intelligent routing protocol based on DYMO for MANET. International Journal of Digital Information and Wireless Communications, 8(3), 195–202. http://dx.doi.org/10.17781/P002452
[18] Al-Dhief, F., Sabri, N., Salim, M., Fouad, S., &Aljunid, S. (2018). MANET routing protocols evaluation: AODV, DSR and DSDV perspective. MATEC Web of Conferences, 150(2), 1–6. http://dx.doi.org/10.1051/matecconf/201815006024
[19] Hamamreh, R.A., Ayyad, M.R., &Abutaha, M. (2023). RAD: reinforcement authentication model based on DYMO protocol for MANET. International Journal of Internet Protocol Technology, 16(1), 46–57. http://dx.doi.org/10.1504/IJIPT.2023.10054906
[20] Stallings, W. (2023). Cryptography and Network Security: Principles and Practice, 8th edition. Prentice Hall.
[21] Shakya, A., & Karna, N. (2019). Enhancing MD5 hash algorithm using symmetric key encryption. Proceedings of the 3rdInternational Conference on Cryptography, Security and Privacy, 18–22. https://doi.org/10.1145/3309074.3309087
[22] Turner, S., & Chen, L. (2011). Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms. Internet Engineering Task Force (IETF). https://www.rfc-editor.org/info/rfc6151.
[23] Yang, H.S., & Yoo, S.J. (2014). Authentication Techniques for Improving the Reliability of the Nodes in the MANET. Proceedings of the International Conference on IT Convergence and Security, IEEE, China, 1–3. https://doi.org/10.1109/ICITCS.2014.7021743
[24] Sharma, N., Gangal, A. (2016). Mobile node authentication in MANET using enhanced cluster based AUCRES algorithm. Far East Journal of Electronics and Communications, 3(1), 1–12. http://dx.doi.org/10.17654/ECSV3PI16001
[25] Verma, U., Kumar, S., & Sinha, D. (2016). A secure and efficient certificate-based authentication protocol for MANET. Proceedings of the International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2016(3), 1–7. https://doi.org/10.1109/ICCPCT.2016.7530346

[26] Sen, J. (2010). A robust and efficient node authentication protocol for mobile ad hoc networks. Proceedings of the 2nd International Conference on Computational Intelligence, Modeling and Simulation, IEEE, Indonesia, 476–481. http://dx.doi.org/10.1109/CIMSiM.2010.12
[27] Subu, N., Jayapal, S., & Sridharan, D. (2012). A trust system in manet with secure key authentication mechanism. Proceedings of the International Conference on Recent Trends in Information Technology, IEEE, India, 261–265. http://dx.doi.org/10.1109/ICRTIT.2012.6206818
[28] Lu, B., & Pooch, U. (2005). A lightweight authentication protocol for mobile ad hoc networks. Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE, USA, 2, 546–551. https://doi.org/10.1109/ITCC.2005.13
[29] Tembhurkar, M., &Singare, Y. (2015). Design of an efficient initial access authentication over MANET. Proceedings of the International Conference on Industrial Instrumentation and Control (ICIC), IEEE, India, 1614–1619, http://dx.doi.org/10.1109/IIC.2015.7151008
[30] Nitnaware, D., & Thakur, A. (2016). Black hole attack detection and prevention strategy in DYMO for MANET. Proceedings of the3rd International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, India, 279–284, https://doi.org/10.1109/SPIN.2016.7566704
[31] Rifa, H., & Herrera, J. (2007). Secure Dynamic MANET On-demand (SEDYMO) Routing Protocol. Fifth Annual Conference on Communication Networks and Services Research (CNSR07) IEEE Xplore Press, 372–380. http://dx.doi.org/10.1109/CNSR.2007.57
[32] Zapata, M. G. (2006). Secure Dynamic MANET On-Demand (SDYMO) Routing Protocol. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-guerrero-manet-sdymo/00/.
[33] Perkins, C. E., Chakeres, I. (2013). Dynamic MANET On-demand (AODVv2) Routing-draft-ietf-manet-dymo-24. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-ietf-manet-dymo-24.
[34] Salleh, N. M., Mahiddin, N. A. (2020). MANET Performance Measurement of DYMO Routing Protocol by Varying Density and Mobility Speed. International Journal of Engineering Trends and Technology. 11–18. http://dx.doi.org/10.14445/22315381/CATI3P202