**CHAPTER I**

# **Introduction**

## **Background**

MANET is a highly decentralized wireless network consisting of mobile devices, or nodes that communicate with each other without relying on a fixed infrastructure. MANETs are mostly known for their high mobility, self-configuring and self-organizing characteristics. It can adapt to changes its positions of individual devices, as well as varying channel error rates and link disruptions. MANETS are constructed by dynamic mobile nodes and used dynamic topology, which allows for frequent changes as devices move in and out of the network. This flexibility is critical when supporting communication during disaster scenarios and military operations where traditional infrastructures may not be available. Mobile nodes join in, on the fly, and create a network on their own, each node carrying out basic operations like routing and packet forwarding without the help of an established infrastructure [1]

AODV is a routing protocol based on the DSDV algorithm, operates reactively by establishing routes only when necessary. It ensures a single path without loops, when a source wants to send data to an unknown destination, it initiates a Route Request (RREQ) to discover the route. Intermediate nodes receiving the RREQ established a route if needed to the destination route and if it is the destination then it replays message (RREP) is sent back to the source by the destination or nodes with a route. Nodes without the route rebroadcast the RREQ if this has the route or the destination. The shortest path is chosen if multiple RREPs is received. Data transmission follows the established route. In case of route failure, a RERR is sent to the source, Prompting route cancellation and recovery. The main problem in AODV is link failure problem, because it discovers only one best route based on on-demand distance vector. If the path become vulnerable by a malicious node the whole link may be failed.

The AOMDV routing protocol is as like the AODV in most of the cases including distance vector concept instead of it finds multipaths. It overcomes the link failure problem in ad hoc network. AOMDV shares nodes instead of finding the destination routes from beginning by RREQ. It works with efficient node switching which allows AOMDV to find next best routes when it fails in one link.

Dynamic Source Routing (DSR) is a routing protocol used in wireless mesh networks and mobile ad hoc networks (MANETs) to establish efficient communication paths between nodes. Unlike traditional routing protocols that rely on fixed routing tables, DSR is based on the concept of source routing, where each packet contains complete information about its route through the network. It remains a valuable routing protocol in scenarios where traditional infrastructure-based routing is impractical, such as in mobile ad hoc networks and certain types of wireless mesh networks. Its reliance on source routing and dynamic updates makes it well-suited for dynamic and resource-constrained environments.

## **Requirements**

In a MANET, there is a sender who sends data and also a receiver who receives the data with several dynamic nodes which forwarding the data. AOMDV routing protocols find multiple routes from source to destination and transmits packets using the route with the minimum hop-count. The multiple paths are considered to be disjoint and active. Homomorphic Encryption is the cryptographic technique allowing computations on encrypted data without decryption. The homomorphic encryption has several techniques, It can be done by adding, Multiplying or both on the encrypted data. Another technique is called the mixed technique where, performing decryption on the product of one ciphertext plaintext is the same as multiplication of two plaintexts.

## **Problem Statements**

The security in MANETs has become an active area of research because of various applications. Security concerns arise due to highly decentralized nature, making them more vulnerable to unauthorized access, eavesdropping, and various attacks.

In Multipath routing protocol like AODV, source node at first selects the best routes to the destination nodes and send packets through the routes. But these routes may consist of malicious nodes. The malicious nodes behave like other nodes as other nodes forward packets. A malicious node forward the control packets but drop the data packets so they do not reach the destination.

The entire data is sent via a single path and dropped by the malicious node. However, the data is encrypted but lost so, it makes no sense of the encryption. As entire data is dropped so the attacker gains full knowledge about the data. The goal of the proposed scheme is to deliver the whole data reliably even though there is malicious node in the paths which are not working.

Blackhole Attack means a malicious node falsely claims to have the shortest route to a destination and attracts traffic to itself, subsequently dropping or misrouting the received data packets. In AOMDV, as it supports multiple paths to a destination, however a blackhole node claims to have the shortest path to various destinations, it can lure traffic onto those paths, disrupting the communication by dropping or manipulating packets. A blackhole node can falsely exploit the on-demand nature of AOMDV’s route discovery. When a source node seeks a route, a blackhole node might respond with fake routes that seems optimal. This can divert traffic towards it, leading to potential data loss or compromise.

Wormhole attacks means when attacker receives packets at one location in the network and tunnels them to another location in the network, where the packets are resent into the network. It is a security threat in wireless networks, particularly prevalent in ad hoc and sensor networks. In this attack, malicious nodes create a virtual tunnel or shortcut between two distant parts of the network, allowing them to bypass normal routing protocols and gain unauthorized access to sensitive information. The wormhole is established by colluding nodes that capture packets at one location, tunnel them to another location through a high-speed, possibly wired or direct wireless link, and then replay them into the network. This attack can disrupt network operations, compromise data integrity, and lead to various security breaches, including man-in-the-middle attacks and traffic analysis. Wormhole attacks are challenging to detect and mitigate since they exploit vulnerabilities in the underlying communication protocols rather than targeting individual devices or cryptographic mechanisms. To counter wormhole attacks, network designers and security experts employ techniques such as secure routing protocols, cryptographic authentication mechanisms, and anomaly detection algorithms to identify and prevent the formation of unauthorized tunnels within the network. Overall, understanding and mitigating the risks associated with wormhole attacks are crucial for ensuring the security and reliability of

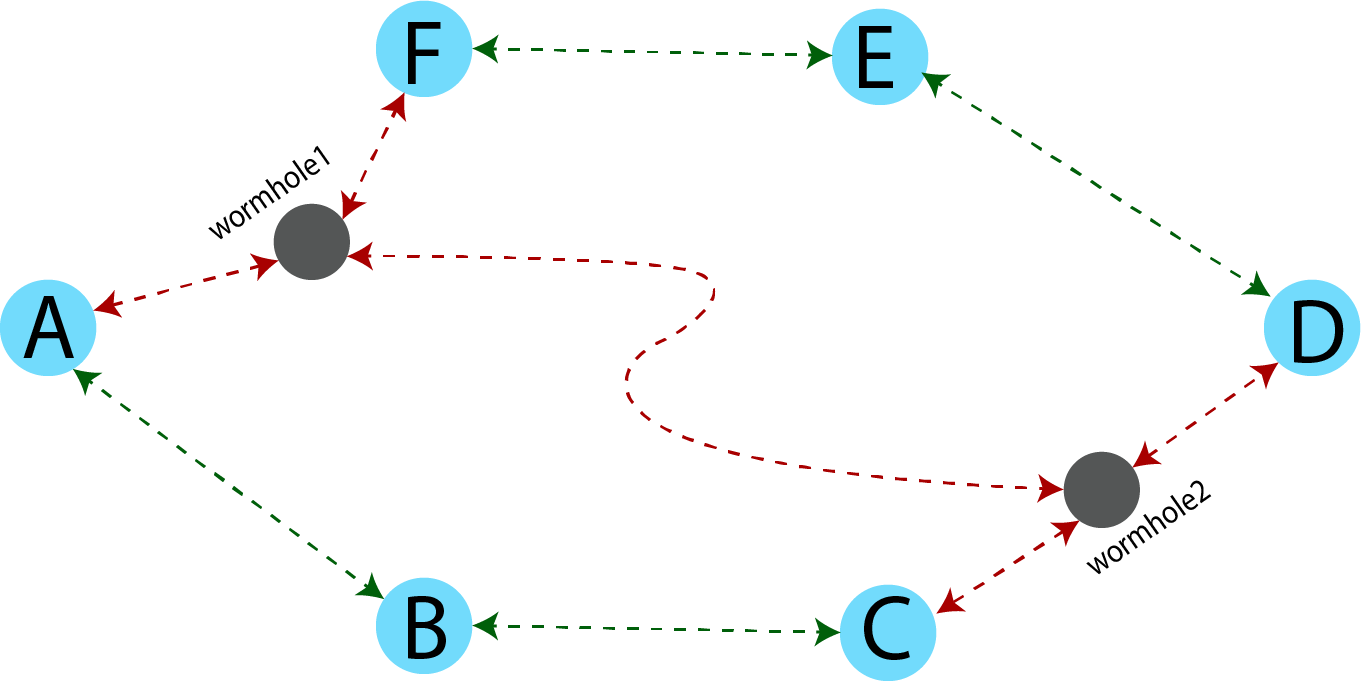


Fig: 1.1 Wormhole attacks

wireless communication networks in various applications, including IoT, military operations, and critical infrastructure. Amore subtle type of routing disruption attack is the creation of a wormhole in the network [2], using a pair of at tacker nodes wormhole1 and wormhole2 linked via a private network connection. Every packet (or selected packets) that wormhole1 receives from the ad hoc network, wormhole1 forwards through the wormhole to wormhole2, to then be rebroadcast by wormhole2; similarly, wormhole2 may send all packets to wormhole1.

**1.4 Objectives**

* The provide a reliable and secure AOMDV routing protocol for data transmission**.**
* Secure data transmission by assuming that routing between sender and receiver is already established.
* To make AOMDV routing protocol more efficient.
* To send data securely from blackhole and wormhole attacks

**1.5 Unfamiliarity of the Problem**

Malicious nodes may be contained in the route and may make blackhole attacks. In this proposed scheme multiple paths are found using AOMDV protocol and sent data by multiple paths dividing the main data into multiple parts and encrypted them by Enhanced homomorphic encryption cryptosystem. The proposed scheme is not intrusion detection algorithm, but it is intrusion avoidance system for malicious nodes. The idea behind the scheme is to allocate disjoint paths into distinct groups and each group consists of several paths. All the disjoint paths are interconnected between sender and receiver. The message is divided into multiple fragments and each fragment is encrypted using homomorphic encryption. One group is owned one parts of the encrypted message and deliver it to the destination. If one of the nodes is malicious then the message is still able to reach the destination by another safe path. This proposed scheme is able to send the whole message without any attacks or modifications by blackhole attacks.

**1.6 Project Planning**

The plan for this project is organized using a Gantt chart shown in figure 1.2. As the topic is quite new in the arena of research, review of necessary literatures took some time, then to find out some limitations and modifications of the proposed scheme by previous research is still on planning. After that implementation of previous approach as well as newly proposed scheme will be done for comparative study. This comparative study will provide a better

view of previous results and success rate with the newly proposed idea’s result and success rate.

**1.7 Organization**

This thesis progress report is organized as follows. Sections 2 explains closely related work. Section 3 introduces methodology. The problem to be solved in this paper is mentioned in Section 4. The proposed scheme is described in Section 5. Section 6 shows the simulation results. Conclusion with future work is mentioned in Section 7.

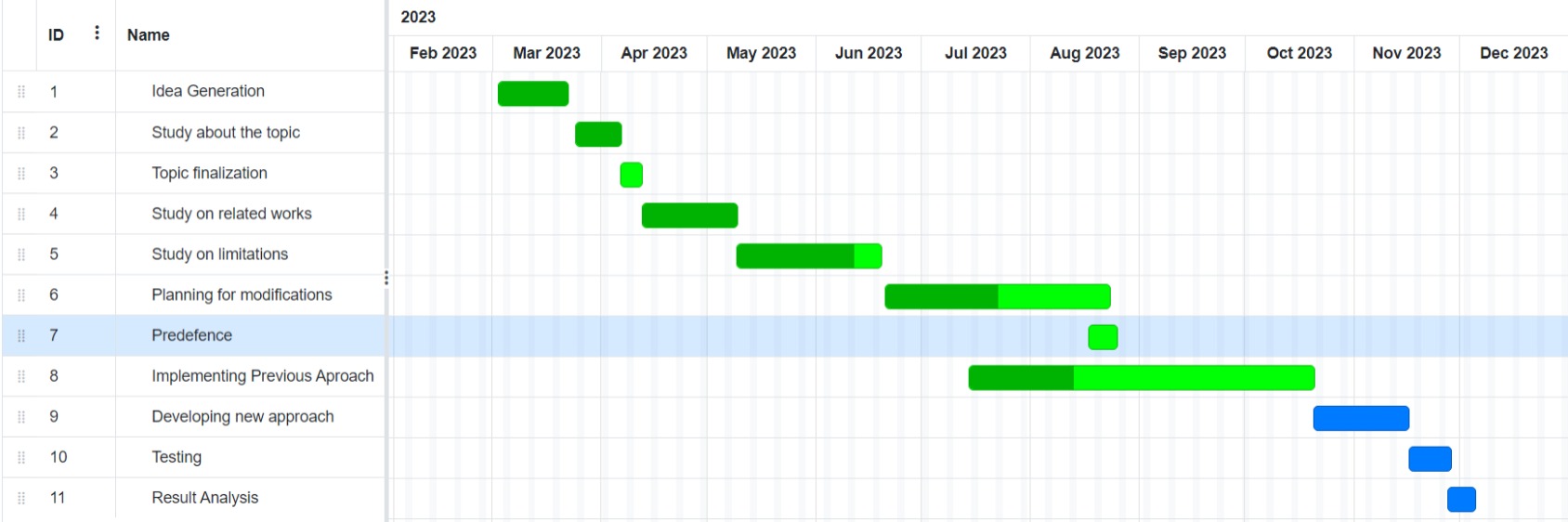


Fig. 1.2. Gantt chart for thesis plan

**CHAPTER II**

**Related works**

In this chapter, previous related works are discussed. Most of the works are done about secure and reliable MANET routing. A few works are done for securing data forwarding in MANETs. Although some proposal was interesting and effective in data forwarding or data communication on mobile ad-hoc network.

Papadimitratos and Haas [3] proposed a data transmission securing technique in MANETs and the proposed secure data transmission scheme for Mobile Ad Hoc Networks (MANETs) functions exclusively through an end-to-end process. It capitalizes on the redundancy provided by multipath routing and ensures its functionality remains robust and efficient even in challenging conditions. The scheme operates independently of constrained knowledge about security associations and network trust. It also accommodates potential data loss while dynamically adapting its operations to the prevailing network conditions.

Lou et al. [4] introduced a security protocol aimed at bolstering data confidentiality in MANETs by ensuring dependable data delivery. The fundamental concept involves converting a confidential message into multiple shares using secret sharing schemes. These shares are subsequently conveyed via distinct, separate paths to the destination. This approach ensures that, even if a limited number of nodes are compromised, the entirety of the secret message remains secure. However, these schemes face a challenge: each node in the network must establish a security association with every other node, leading to increased overhead.

Wazid et al. [5] [6] introduced novel techniques for detecting and preventing multiple attacker nodes in Wireless Sensor Networks (WSNs). These methods involve dividing the entire WSN into clusters, with each cluster featuring a powerful sensor node known as a cluster head. These cluster heads are responsible for detecting potential attacker nodes within their respective clusters. Notably, these techniques are well-suited for resource-constrained sensor nodes due to their minimal computational and communication overheads.

Satav et al. [7] proposed a technique designed to enhance route selection security in challenging environments within Mobile Ad Hoc Networks (MANETs). This approach introduces a route reliability parameter to classify paths as reliable or unreliable in the routing table. However, this addition increases computational and storage overhead while diminishing packet delivery ratio and end-to-end delay. This method addresses security concerns during the route discovery phase, whereas our proposal focuses on addressing security issues during the data transmission stage.

Yang et al. [8] presented a self-organized network-layer security approach. Unlike crypto-graphic measures applied to messages in transit, this solution focuses on safeguarding the network against malicious nodes through the identification and response to suspicious behaviors. It constitutes a network-layer security strategy that shields routing and forwar-ding activities within a unified framework. However, a notable challenge of this scheme is its excessive energy consumption, which impacts its feasibility and effectiveness.

Chinthanai et al. [9] introduced an enhanced adaptive acknowledgment technique for intrusion detection. This method employs digital signatures to counteract the fabrication of acknowledgment packets by attackers. Notably, the scheme achieves improved detection rates for malicious behavior in specific scenarios without imposing any negative impact on network performance.

Tan et al. [10] introduced a mechanism that enhances data transmission security by employing the AES cryptographic primitive within the context of the AODV protocol. This approach focuses on countering blackhole attacks, emphasizing the enhancement of network parameters such as throughput and packet delivery ratio.

Ertaul et al. [11] utilized elliptic curve cryptography (ECC) and a threshold cryptosystem (TC) to ensure secure message delivery. Their method entails dividing the message into fragments, individually encrypting each fragment with ECC, and then transmitting these encrypted segments to the recipient. At the recipient's end, the secret shares are decrypted using ECC to reconstruct the original message. A key challenge faced by earlier approaches, however, is the introduction of additional routing overhead, particularly in situations involving a knowledgeable adversary.

**Table 2.1**: Comparison between the related works and the proposed scheme

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| work | Key focus | Approach and Features | Overhead | Packet loss | Security  Constrained | End-to-end delay |
| [1] | End-to-end secure data transmission  in MANET | Utilizes multipath routing for resilience and adaptability | yes | yes | yes | yes |
| [2] | Data confidentiality enhancement in MANETs | Secret sharing, safe-  guard against compromised nodes. | yes | no | no | yes |
| [3-4] | Detection and prevention of  Attacker nodes in WSNs | Divide WSNs in  clusters with power-  ful nodes. | no | yes | yes | yes |
| [5] | Route selection security enhancement  in MANETs | Adds route reliability to routing table | yes | yes | no | yes |
| [6] | Self-organized  Network-layer  security in MANETs | Detects malicious nodes, shields routing  and forwarding. | yes | no | no | yes |
| [7] | Enhanced ada-  ptive acknowl-edgement for  intrusion detect | Utilizes digital signa-tures for packet auth-enticity | yes | no | yes | yes |
| [8] | Data transmis-sion security  enhancement  using AES | Implement AES wit-  hin AODV for black-hole defence | yes | no | yes | no |
| Proposed | High reliability  security in da-ta transmission | Using Homomorphic  cryptosystem with AOMDV protocol | no | no | no | yes |

In overview, the majority of prior endeavors to secure the AOMDV protocol in MANETs struggle to effectively counter black hole attacks, as these attacks lead to data loss even if the data is encrypted. In contrast, our proposed scheme appears to offer a higher level of reliability and security by successfully delivering encrypted data to the intended destination.

**CHAPTER** **III**

**Required tools**

**3.1 Dynamic Routing Protocols**

Dynamic Source Routing (DSR) is a popular routing protocol used in mobile ad hoc networks (MANETs) and wireless mesh networks. It relies on the concept of source routing, where the entire route from source to destination is included in the packet header. DSR operates entirely on-demand and has been well studied through both simulation and real tested implementation [12] [13]. In DSR, when anode has a packet to send to some destination and does not currently have a route to that destination in its Route Cache, the node initiates Route Discovery to find a route.

**3.1.1 Route Discovery**

* When a source node (S) wants to send data to a destination node (D) and does not know a route to D, it initiates a route discovery process.
* Source S broadcasts a Route Request (RREQ) packet containing the address of the destination D.
* Each intermediate node receiving the RREQ either forwards it or responds if it has a route to D or is D itself.

**3.1.2 Route Reply**

* If the RREQ packet reaches node D or an intermediate node with a route to D, a Route Reply (RREP) packet is sent back to node S.
* The RREP packet contains the complete route information from S to D, accumulated during the propagation of the RREQ.

**3.1.3 Route Reply**

* Nodes along the established route cache the route information they learn.

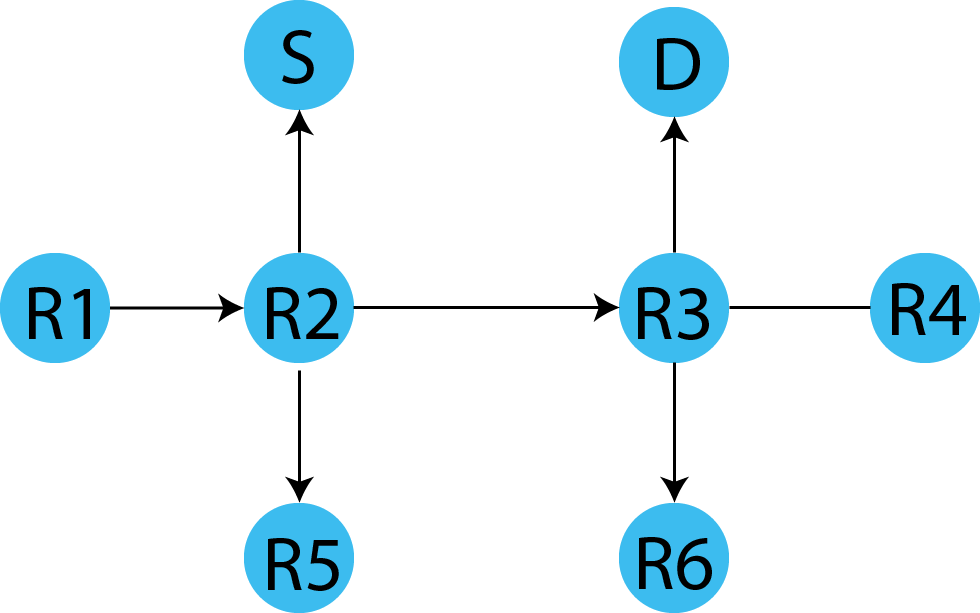


Fig 3.1: An example of Dynamic routing protocol

* If a link or node failure is detected, the affected node invalidates the route, and subsequent packets trigger new route discovery.

**3.2 Ad Hoc On-demand Distance Vector Routing (AODV)**

An ad-hoc network involves mobile nodes cooperating without centralized control. [14] Each node acts as a router, acquiring routes on-demand rather than through regular ads. AODV ensures loop-free routes even when repairing broken links. The protocol's efficiency lies in avoiding constant global routing advertisements.

**3.3 Ad Hoc Multipath On-demand Distance Vector Routing (AOMDV)**

AOMDV is extension of AODV. It is a multi-path, disjoint path and also a loop free routing protocol. [15] It is proposed based on the existing single path routing protocol AODV to avoid frequent route discovery [16]. It also solves the route cutoff problem. Reactive routing protocol, which initiates route Computations only.

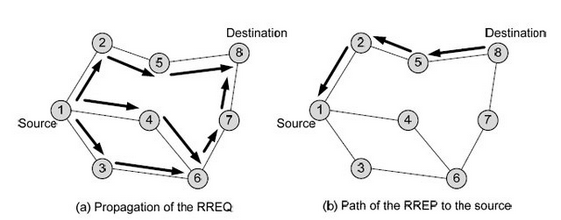


Fig 3.1: Ad hoc on demand distance vector routing scenario [17]

**3.4 Homomorphic Encryption:**

Homomorphic cryptosystems are cryptographic methods that allow performing operations on encrypted data without needing to decrypt it first, making it possible to compute on ciphertexts just like on plaintexts. There are two types: partially homomorphic, which can handle either addition or multiplication on ciphertexts, and fully homomorphic, which can handle both. Examples include RSA and the Paillier cryptosystem for partially homomorphic systems, while fully homomorphic systems originate from lattice-based cryptography, notably pioneered by Craig Gentry. These systems find applications in secure outsourced computation, private data analysis, and secure multi-party computation, enabling computations while keeping data encrypted for privacy and security. Challenges include computational overhead, managing keys securely, and relying on specific security assumptions. Nevertheless, ongoing research seeks to tackle these challenges as homomorphic cryptosystems remain crucial for protecting sensitive information and enabling secure computations across various fields.

**3.5 Enhanced Homomorphic Cryptosystem (EHC)**

In this proposed scheme EHC is used to encrypt the data. The encryption technique uses additive homomorphic encryption strategy. The computer will perform the computation on the encrypted data, hence without knowing anything of its real value. Finaly, it will send back the result and that will be decrypted. Here a large number m consists of two large prime numbers p and q. Here q is the shared secret key. That number m is also a secret key which is used to encrypt the data. Random number is used in this system. Random number makes the cryptosystem strong and impossible to breach. In the principle of the scheme there are three parts. They are: key generation, encryption and decryption.

**3.5.1 Secret Key Generation**

- p, q ↋ P, where P is prime, and m = p \* q.

- Generate a random number r.

- The set of original plaintext message p = = {x : x <= P}, = {x : x < m } has the set of ciphertext messages.

- Secret values r, m and q

- Shared key k = p.

**3.5.2 Encryption**

**-** x ↋

-The ciphertext C is calculated as:

y = (x) = (x + r × ) (mod m) = x + r \* p.

**3.5.3 Decryption**

**-** The Plaintext x is recovered as:

x = (y) = y mod p

= (x + r\*p) mod p

= x mod p + r \* p mod p

= x

**3.5.4 Homomorphic (additive) characteristic of EHC:**

Homomorphic encryption schemes allow operations to be performed on the encrypted data (ciphertext) as if the operation is performed on the plaintext. In additive homomorphism, decrypting the sum of two ciphertext is same as addition of two plaintext represented as:

E (x + y) = E(x) + E(y) [1].

Y ( + ) = +

= (+ \* P) + ( + \* P)

= + + ( + ) \* P

D ( + ) = ( + ) mod P

= ( + + ( + ) \* P) mod p

= +

**Real Life Example:**

= 7

= 3, = 4

= (3 + 2 \* )) mod 77 = 25

= (4 + 3 \* ) mod 77 = 37

= + = 25 + 37 = 62

D = 62 mod 11 = 7

**CHAPTER IV**

**Proposed Methodology**

**4.4 Proposed Scheme**

**4.4.1 Blackhole Attack Avoidance**

The proposed scheme is implemented by modifying the AOMDV protocol. The scheme is explained below:

* A collection of operational separate routes, denoted as n, is established between a sender and a receiver. In our network layout, n signifies the count of active routes present within the topology. This value is deliberately chosen and kept constant to create multiple routes linking a sender and a receiver, thereby facilitating the transmission of message components. The sender's routing table is then populated with crucial information necessary for data routing along each chosen path in the topology connecting the sender and the receiver.
* The paths are organized into groups labeled as G, achieved by dividing the total count of paths, n, by the specified quantity of paths intended for each group. This division is carried out with the condition that each group contains at least two active paths, which is represented as G = (n / 2 or more).
* Prior to transmitting the message (code), the sender designates a distinct and exclusive message identifier (msg-id) to the complete message. The message is then fragmented into parts equal to the number of groups, denoted as G. This division process generates individual segments labeled as M/G, wherein M signifies the complete message and G stands for the total count of merged active separate paths within groups.
* Additionally, every segment of the complete message, denoted as m, is linked to a distinct part message identifier. This identifier, represented as (msg-sp-id1, msg-sp-id2,…,etc.), is employed on the receiver's end to reassemble the complete message from its individual segments.

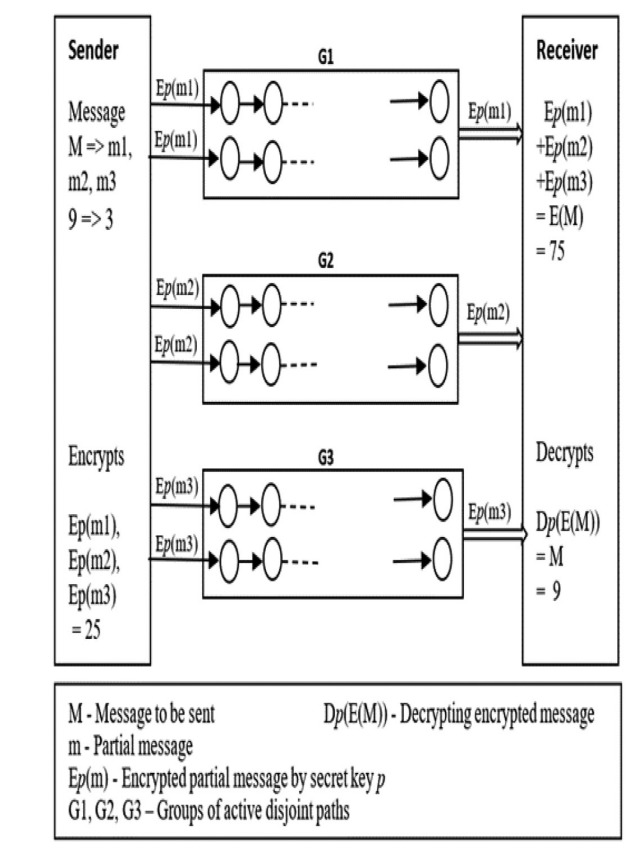


Fig. 4.1. An example of proposed scheme where n = 6 and G = 3

* Subsequently, the sender employs the Extended Homomorphic Cryptosystem (EHC) to encrypt all segments of the complete message: m1, m2, m3, …, etc. The encryption process yields corresponding encrypted parts: Ep(m1), Ep(m2), Ep(m3), …, etc. Here, 'p' signifies the secret key. The sender transmits these encrypted parts, along with the message identifier (msg-id), part message identifier (msg-sp-id), and the sum of part message identifiers (msg-sp-id-sum), through separate active paths within each group.

As a result of this transmission, each group is equipped with only one encrypted part under the same message identifier and part message identifier.

* On the recipient's end, the total count of encrypted segments in the complete message is determined using the summation of part message identifiers (msg-sp-id-sum) embedded within the encrypted parts.

**4.4.2 Wormhole Attack Avoidance**

The TESLA [18] [19] broadcast authentication protocol, efficiently authenticates message-s by adding just one message authentication code (MAC) to the message for broadcast authentication purposes [20]. In point-to-point communication, adding a Message Authentication Code (MAC) with a shared key ensures secure authentication. However, in broadcast communication, multiple receivers needing the MAC key can lead to packet forging and impersonation. Secure broadcast authentication requires an asymmetric primitive, where the sender generates authentication information, but receivers only verify it. TESLA achieves this through clock synchronization and delayed key disclosure, instead of relying on computationally expensive one-way trapdoor functions like RSA [21].

* Each sender chooses a random initial key .

generates a one-way key chain by repeatedly computing a one-way hash function H on this starting value: = H [], = H [], . . . .

* In general, = H [= [].
* To compute any previous Key from key j < I, a node uses the equation:

[]

* To authenticate any received value on the one-way chain, a node applies this equation to the received value to determine if the computed value matches a previous known authentic key on the chain. Coppersmith and Jakobsson present efficient mechanisms for storing and generating values of hash chains [22].
* In TESLA, senders prearrange a schedule to reveal keys from their one-way key chain in reverse order from their creation. That is, a sender publishes its keys in the order ,,...,. For example, they might disclose key at time plus i multiplied by the key publication interval I, where is the initial key publication time and I is the interval between key disclosures.

**4.5 Example Scenario**

* The number of disjoint paths n = 6 between the sender and receiver.
* Number of groups is G = n / two or more paths in each group G = 6 / 2 = 3
* The entire message M = 9.
* Parts of the entire message m = M / G = 9 / 3 = 3 where m is m 1 = m2 = m3
* The message’s id for the entire message M is msg − id = 1.
* The message part ids for the message parts are msg − sp − id1 = 1, msg − sp − id2 = 2, and msg − sp − id3 = 3.
* So, the message part id’s sum is msg − sp − id − sum = msg − sp − id1 + msg − sp − id2 + msg −sp − id3 = 1 + 2 + 3 = 6
* Encrypted the message parts m1, m2, m3 using EHC at the sender before sending them to the destination: We have M = 9 and m1 = m2 = m3 = 9/3 = 3

**CHAPTER V**

**Implementation**

In this section, our proposed algorithm is subjected to numerical analysis. When conside-ring that a source node possesses n separate routes to the destination, each route is modelled as a queue denoted as Qi. Each queue has an arrival rate λ from the source node and a service rate μi, as depicted in Figure 5.1. Given that a route consists of multiple nodes, the collective buffer capacity for each route equals the sum of buffers across all nodes. As such, we employ the M/M/1 queue model, assuming unlimited buffers for traffic and First-Come-First-Served (FCFS) service discipline. The structure of the queue model used for our analysis is illustrated in Figure 5.1.

**5.1 Encryption Process**

Select p = 11, q = 7 and r (random) = 2

Then m = p × q = 11 × 7 = 77

Ep (m1) = (m1 + r ∗ ) (mod m) = (3 + 2∗) (mod 77)

Ep (m1) = 25

And so on for m2 and m3

Ep (m2) = 25 and Ep (m3) = 25

E (m1) + E (m2) + E (m3) = 25 + 25 + 25 = 75 = Y

* Decrypt the sum of the encrypted parts of entire message to get the original message at the receiver using EHC.

**5.2 Decryption Process**

Y = E (m1) + E (m2) + E (m3) = 75 and shared key

p = 11 Dp (Y) = Y mod p

= 75 mod 11 = 9 = M (The original message)

**5.3 Algorithm**

**5.3.1 The Sender Procedure**

**Input:** message M, number of active disjoint paths n

**Output:** Encryptedpart of message E(m)

1: Read M, n // read the entire message and number of active

paths between source and destination.

2: Set r // number of required

disjoint active paths in each group.

3: Set G to n / r // G is the number of groups of disjoint paths.

4: Set m = M / G // splitting the original message.

5: Set msg-id to 1 // assign ‘message id’ value for the whole message.

6: msg-sp-id-sum = 0 // initiate value of the sum of message parts.

7: for (i = 1; i ≤ G; i++)

8: Set msg-sp-id to i // assign ‘id’ to part of the message.

9: Set E(m) to encrypt m // encrypt part of the message.

10: msg-sp-id-sum + = msg-sp-id // add to get the sum of message split ids.

11: Write msg-id, msg-sp-id, E(m) // buffer output data.

12: end for

13: Write msg-sp-id-sum // attend sum of message split ids to the buffer of outputs.

14: Send msg-id, msg-sp-id, msg-sp-id-sum, E(m) //send output data to destination

**5.3.2 The Receiver Procedure**

**Input**: msg-id, msg-sp-ids, msg-sp-id-sum, encrypted message E(m)

**Output**: the original message M

1: Set sum = 0, E(M) = 0

2: While (sum != msg-sp-id-sum) do

3: if (msg-sp-id is duplicated) then // msg-sp-id of encrypted message is already received. 4: drop E(m) // drop the duplicate encrypted message.

5: else

6: add E(M)=E(M)+E(m) // add encrypted parts of message.

7: sum = sum+ msg-sp-id // add message split ids of the encrypted parts.

8: end while

9: M = decrypt E(M) // decrypt sum of the encrypted parts to get the original Message.

The time complexity of the proposed scheme is analyzed. In the Encryption Homomorphic Cryptosystem (EHC), key operations run in polynomial time, denoted as λ. Encryption time is T. The scheme's overhead is T × θ(G), where G is the number of path groups and n is active paths.

For the sender, initialization (steps 1-5) takes θ (1), encryption (steps 6-12) takes T × θ(G), and communication (step 14) is θ(G). Storage for variables takes θ(G) and θ(1) times. The sender's computational time is T × θ(G). For the receiver, initialization (step 1) is θ(1), addition (steps 2-8) is θ(G), and decryption (step 9) is O(T). Receiver's computation is less than sender. Receiver's storage is also smaller.

The initial AOMDV scheme requires θ(n) storage for n paths, with computational complexity of O(n) due to absence of encryption or decryption. Communication complexity is also O(n) in worst case. A comparison of time complexity between the proposed scheme and original AOMDV scheme is provided in Table 4.1.

**5.4 Key Exchange Algorithm**

Elliptic Curve Cryptography (ECC) was initially introduced by Victor Miller and independently by Neal Koblitz in the mid-1980s and has since developed into a robust public-key encryption system. ECC offers equivalent security to traditional methods but with significantly smaller key sizes, resulting in faster computations and reduced memory, power, and bandwidth requirements, especially beneficial in resource-constrained environments. Its advantages become more pronounced as security demands grow.

**Table 5.1**: Comparison of time complexity between proposed scheme and the AOMDV scheme

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Scheme | Memory | Encryption | Decryption | Computation | Communication |
| Proposed | θ(n) + θ(G) | T × θ(G) | T × θ(1) | T × θ(G) | θ(n) |
| AOMDV | - | - | - | θ(1) | 0(n) |

Recently, the National Institute of Standards and Technology (NIST) endorsed ECC for U.S. government use, and various standards organizations like the IEEE, ANSI, OMA, and IETF are actively working to incorporate ECC as either a required or recommended

security measure. In this context, we introduce a novel algorithm utilizing the Diffie-Hellman key exchange for web browsers, ensuring forward secrecy [18].

An elliptic curve E which is over the finite field is given through an equation. An equation will be of the form:

= + a + b,

a, b ε , and − ( + 27) ≠ 0

Let (, ) be the private-public key pair of A and (dB, QB) be the private-public key of B.

1. The end A Computes = (, ) = \*
2. The end B Computes = (, ) = \*
3. Since \* = G = G = \* .
4. Therefore = and hence , =
5. (Where G is generator point)
6. Hence the shared secret is .

Since it is practically impossible to find the private key or dB from the public key .

**5.5 Financial Analysis and Budgets**

* **Hardware Costs:** In this thesis implementation normal daily used personal computer is needed. So, there is no extra cost for hardware.
* **Software Costs:** All The software used for this work is totally free. Linux operating system is used, which is free.
* **Labor Costs:** No labour cost.
* **Training Costs:** No labour is needed.
* **Operating Costs:** NO operating costs.

**5.1 Analytical Model of the Example Scenario**

λ = 1 packet/second, μ = 2 packets/second and packet size = 512 bytes. Waiting time W1 in Q1 just for one packet is the mean response time.

Wi = (1/μ)/ (1 − ρ) = (1/2) / (1 − 0.5) = 1 sec

From our proposal, dividing the first packet for sending it into M/M/1 queues and the capacity of each queue is one packet per second, so the source sends three packets to utilize the whole size of the queue. 4, 096 bits / 3 (# of groups) = 1, 365 bits

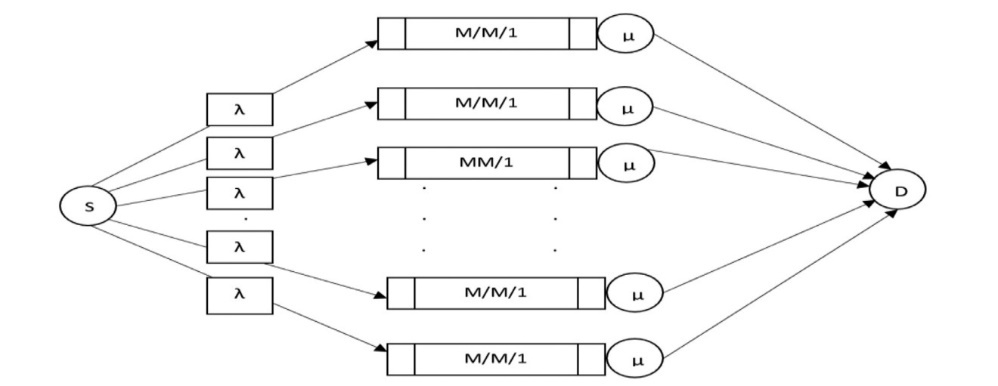
****

Fig. 5.1. Queue model for proposed protocol

**Table 5.1**. Comparing the throughput from the simulation

|  |  |  |
| --- | --- | --- |
| Number of malicious nodes | Numerical results | Simulation results |
| 0 | 24.57 | 71 |
| 1 | 20.47 | 61 |
| 2 | 16.38 | 59 |
| 3 | 12.28 | 38 |
| 4 | 8.19 | 34 |

**Table 5.2**. Simulation parameters

|  |  |
| --- | --- |
| Simulator | Network Simulator 2.35 |
| Number of nodes | 100 |
| Malicious nodes | 0, 1, 2, 3, 4 |
| Area | 1100 m × 1100 m |
| Communication range | 250 m |
| Packet size | 512 bytes |
| Interface type | Phy/Wireless phy |
| MAC type | IEEE 802.11 |
| Queue length | 50 packets |
| Propagation type | TwoRayGround |
| Routing protocol | AOMDV |
| Transport agent | UDP |
| Application agent | CBR |
| Traffic rate | 1 kbps |
| Simulation time | 900 s |

Analyzing the M/M/1 queue model with Poisson arrivals (exponential inter-arrival times) and exponential service times requires two key parameters: the mean arrival rate λ and the mean service rate μ. The ratio λ/μ is referred to as the utilization factor or traffic intensity, denoted as ρ. The queue remains stable when ρ is less than 1. Here are the fundamental properties of the M/M/1 queue model.

**CHAPTER VI**

**Performance evaluation**

This section presents simulation results for performance evaluation. It starts by explaining the simulation methodology and performance metrics. Subsequently, the obtained simula-tion results are provided below:

**6.1 Performance Methodology And Performance Metrics**

We conducted a simulation using the NS-2 network simulator. The AOMDV protocol was adapted to simulate our proposed scheme while introducing malicious nodes. Our simulation consisted of 100 nodes, with some of them behaving as blackhole nodes. Each node's initial position was defined within a 1100 × 1100 m simulation area. Packets were generated using Constant Bit Rate (CBR) with a uniform size of 512 bytes for all mobile nodes. The nodes exhibited a mobility rate of 10 meters per second, and the simulation was run for a duration of 900 seconds. The IEEE 802.11 MAC protocol was employed.

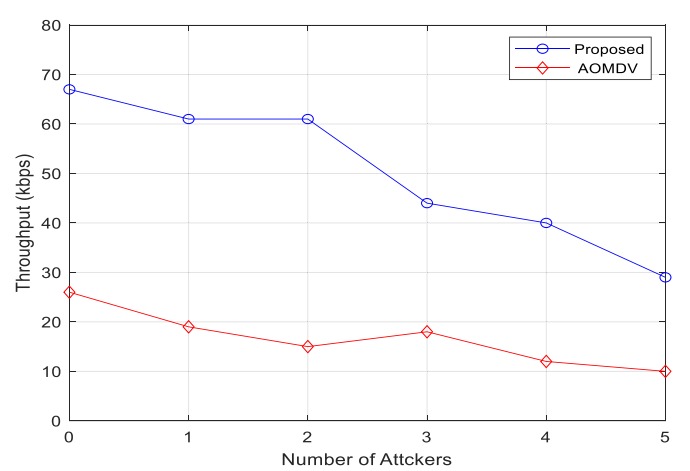
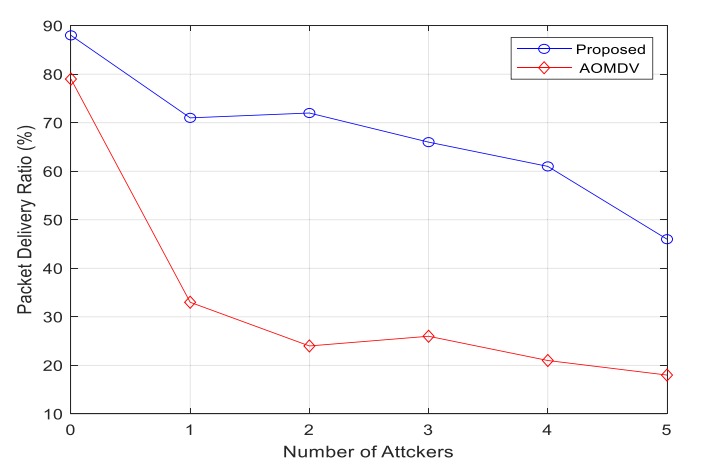
****

Fig. 6.1. Packet delivery ratio (%) Fig. 6.2. Throughput as a function of nodes

Details of the simulation parameters can be found in Table 3. To evaluate the simulation of the original AOMDV and the proposed scheme four metrices have been considered.

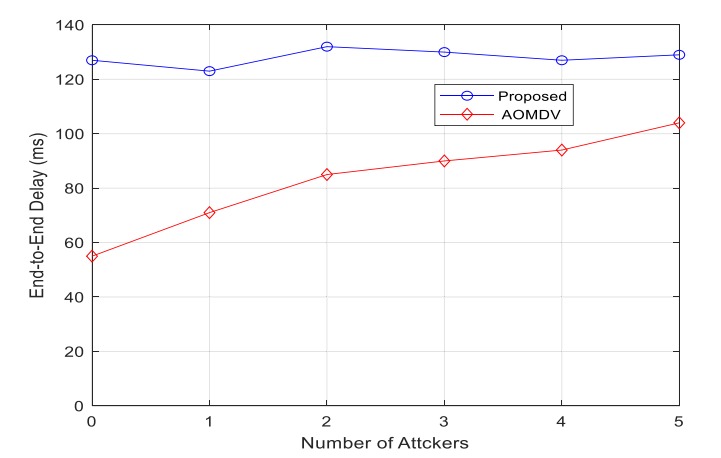
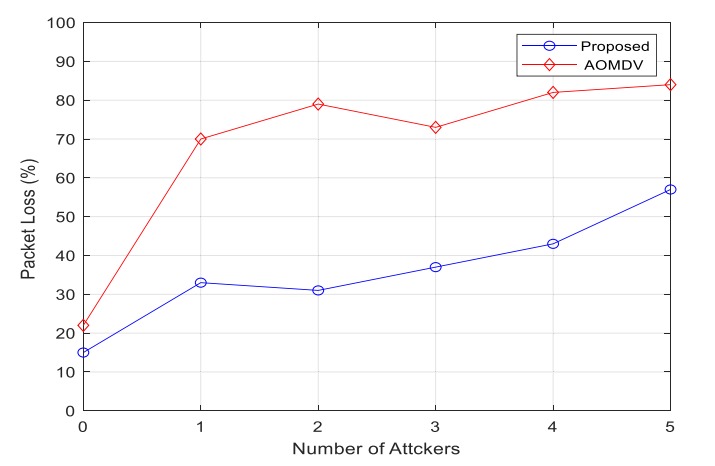


Fig. 6.3. Packet loss as a function Fig. 6.4. End-to-end delay

* Packet delivery ratio (%): the proportion of the total number of packets reached the destination over the number of packets sent by the source.
* Throughput (bits/sec): the amount of data successfully received at the destination per second.
* Packet loss (%): the average number of lost packets during the data transmission process.
* Average end-to-end delay (sec): the time taken for a packet to reach the destination from the source node

**6.2 Results**

**6.2.1 Packet Delivery Ratio**

Referring to Figure 6.1, a comparison is made between our proposed scheme and the original AOMDV protocol regarding packet delivery ratio (PDR) in the presence of malicious nodes (blackhole attackers). As the number of attackers increases, the PDR decreases in the original AOMDV scheme. However, in AOMDV, beyond the first attacker, additional attackers have limited impact due to the use of a single path at a time. In contrast, our proposed scheme maintains PDR by ensuring that the original data is received through any available path from the group. This preserves data integrity even in the presence of malicious nodes. Notably, the PDR significantly decreases in the original AOMDV when malicious nodes are introduced, while our proposed scheme manages to maintain a relatively high PDR even with malicious nodes. The effectiveness of our proposed method in preserving packet delivery performance is evident when compared to the original approach.

**6.2.2 Throughput**

In Figure 6.2, a comparison of throughput between the schemes is shown in relation to the presence of malicious nodes (blackhole attackers). Both schemes experience a reduction in data successfully received at the destination per second when an active attacker exists, given the prolonged data transmission duration. Despite this, our proposed scheme maintains a higher throughput compared to the original AOMDV scheme due to its superior packet delivery ratio (PDR) when the number of attackers rises. While our proposed scheme might take longer for packet delivery, its increased reliability in delivering packets with an elevated number of malicious nodes is evident. The observed trend reveals that our proposed scheme consistently achieves higher throughput compared to the original scheme for packet transmission.

**6.2.3 Packet loss**

Figure 6.3 illustrates a comparison of packet loss between the schemes concerning the quantity of blackhole attackers. Generally, in multipath routing protocols, an increase in active attackers corresponds to amplified packet loss. In the original AOMDV protocol, the effect on packet loss is minimal when attackers exceed one for a single data trans-mission. This is due to the scheme employing just a single path at a time. Consequently, the initial attacker in the path has a substantial impact, and subsequent attackers do not significantly influence it, as the encrypted message is already dropped. Conversely, the proposed protocol experiences the impact of multiple attackers, given its simultaneous utilization of multiple paths. While our proposed scheme does exhibit increased data loss with more malicious nodes, it still delivers nearly the entire packet to the destination by distributing it across numerous paths. This approach ensures complete delivery through secure paths, even in the presence of multiple attackers.

**6.2.4 End-to-end Delay**

Figure 6.4 depicts a comparison of end-to-end delay between the two schemes with respect to the number of blackhole attackers. The delay is observed to be greater in our proposed scheme in comparison to the original AOMDV scheme as the count of malicious nodes rises. This is attributed to the more intricate procedures and security mechanisms embedded in the proposed scheme. While our proposed scheme achieves improved data delivery compared to alternative methods with an increased number of malicious nodes.

**CHAPTER VII**

**Societal, Health, Environment, Safety, Ethical, Legal and Cultural Issues**

**4.9 Socio-Economic Impact and Sustainability**

**4.9. 1. Socio-Economic Impact:**

* **Positive Impacts:**
  + **Enhanced Security:** The thesis addresses a critical security concern (blackhole attacks) in mobile ad hoc networks, leading to increased data integrity and network reliability.
  + **Privacy Protection:** The use of homomorphic encryption contributes to protecting users' privacy and sensitive data during communication.
  + **Trust Building:** By mitigating blackhole attacks, users can build greater trust in the network, fostering increased adoption and usage.
* **Community Empowerment:**
  + The research empowers network users by providing them with a secure and reliable communication framework, which in turn enhances their digital experience.
* **Policy and Industry Implications:**
* The findings can influence network security policies and guidelines,
* leading to better regulatory practices.

**4.9.2. Economic Impact Assessment:**

 **Scalability:** The improved data forwarding technique using homomorphic encryption could potentially be scaled to larger network deployments, ensuring its relevance in broader contexts.

 **Adaptability:** The encryption technique is based on a well-established cryptographic concept. It could be adapted to other security challenges, contributing to its long-term viability.

**CHAPTER VII**

**Conclusion**

This paper introduces an enhanced AOMDV scheme designed to enhance the reliability and security of data transmission within Mobile Ad Hoc Networks (MANETs) in the presence of malicious nodes. The proposed approach achieves this by distributing message components across multiple paths and employing homomorphic encryption for cryptog-raphic protection. Simulation results demonstrate the superiority of the proposed scheme, yielding higher packet delivery ratios and throughput. These advancements are particularly valuable for critical applications in MANETs, especially in emergency scenarios. Further-more, the proposed scheme demonstrates a high success rate in ensuring packet delivery to the intended destination, primarily due to the utilization of numerous active paths within each network group.

Future research will focus on reducing the end-to-end delay of this scheme, with the aim of implementing it effectively in emergency applications within Mobile Ad Hoc Networks (MANETs).

# **References**

|  |  |
| --- | --- |
| [1] | Levent Ertaul and Vaidehi, “Implementation of Homomorphic Encryption Schemes for Secure Packet Forwarding in Mobile Ad Hoc Networks (MANETs),” *IJCSNS International Journal of Computer Science and Network Security,* vol. VOL.7, no. No.11, 2007. |
| [2] | A. P. a. D. J. Y.-C. Hu, “ Efficient security mechanisms for routing protocols.,” *Annual Network and Distributed System Security Symposium,* p. 57–73, 2003. |
| [3] | H. Z. Papadimitratos P, “Secure message transmission in mobile ad hoc networks,” *Ad Hoc Netw,* vol. 193–209, no. doi:10.1016/S1570-8705(03)00018-0., p. 1, 2003. |
| [4] | L. W. F. Y. S. Lou W, “ enhancing data confidentiality in mobile ad hoc networks,” *Proc IEEE INFOCOM,* Vols. 2404-13, no. doi:10.1109/INFCOM.2004., p. 4, 2004. |
| [5] | K. A. Wazid M, “ A secure group-based blackhole node detection scheme for hierachical wireless sensor networks,” *wirel pers commun,* Vols. 1165-91, no. doi:10.1007/s11277-016-3676-z., p. 94, 2017. |
| [6] | K. A. Wazid M, “An efficient hybrid anomaly detection scheme using K-means clustering for wireless sensor networks,” *Wirel Pers Commun,* Vols. 1971-2000, no. doi:10.1007/s11277-016-3433-3., p. 90, 2016. |
| [7] | J. P. T. V. Satav P, “Secure route selection mechanism in the presence of blackhole attack with aomdv routing algorithm,” *fourth international conference on computing communication control and automation.,* 2018. |
| [8] | S. J. M. X. S. S. Yang H, “Self-Organized network-layer security in mobile ad hoc networks,” *IEEE J sel Areas Commun,* Vols. 261-73, p. 24, 2006. |
| [9] | S. T. P. V. S. D. Chelvan KC, “EAACK-A secure intrusion detection system for,” *Int J Innov Res Comput Commun Eng,* Vols. 3860-6, p. 1, 2014. |
| [10] | T. S., “Using cryptographic technique for securing route discovery and data transmission from blackhole attack on AODV-based MANET,” *Int J Netw Distrib comput ,* Vols. 100-7, no. doi:10.2991/ijndc.2014.2.2.4., 2014. |
| [11] | C. N. Ertaul L, “Elliptic curve cryptography based threshold cryptography (ecc-tc) implementation for manets,” *IJCSNS Int J Comput Sci Netw Secur,* Vols. 48-61, no. http://paper.ijcsns.org/07\_book/200704/20070407.pdf., p. 7, 2007. |
| [12] | J. B. J. J. a. D. J. D.A. Maltz, “The effects of on-demand behavior in routing protocols for multi-hop wireless ad hoc networks,” *IEEE Journal on Selected Areas in Communications,* Vols. 1439-1453, p. 17(8), 1999. |
| [13] | D. M. D. J. Y.-C. H. a. J. J. J. Broch, “A performance comparison of multi-hop wireless ad hoc network routing protocols.,” *ACM/IEEE International Conference on mobile computing and Networking.,* Vols. 85-97, 1998. |
| [14] | C. E. P. a. E. M. Royer, “Ad-hoc on-demand distance vector routing,” *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA,,* 1999. |
| [15] | YuHua Yuan, HuiMin Chen and Min Jia, “YuHua Yuan, ; HuiMin Chen, ; Min Jia, (2005). [IEEE 2005 Asia-Pacific Conference on Communications - Perth, Western Austral An Optimized Ad-hoc On-demand Multipath Distance Vector(AOMDV,” *YuHua Yuan, ; HuiMin Chen, ; Min Jia, (2005). [IEEE 2005 Asia-Pacific Conference on Communications - Perth, Western Australia (0IEEE 2005 Asia-Pacific Conference on Communications - Perth, Weste2005,* 2005. |
| [16] | P. Sarao, “Ad Hoc On-Demand Multipath Distance Vector Based Routing in Ad-Hoc Networks.,” *Wireless Personal Communications,,* no. doi:10.1007/s11277-020-07511-y , 2020. |
| [17] | [Online]. Available: https://www.researchgate.net/publication/279464781\_To\_find\_cost\_effective\_routes\_that\_are\_able\_to\_meet\_the\_fueltime\_constraints\_using\_the\_Intelligent\_Transportation\_Systems\_in\_VANETS. |
| [18] | M. A. Ram Ratan Ahirrwal, “Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network,” *(IJCSIT) International Journal of Computer Science and Information Technologies,* vol. Vol. 4 (2), no. 363 - 368, 2013. |
| [19] | L. E. a. Vaidehi, “Implementation of Homomorphic Encryption Schemes for Secure Packet Forwarding in Mobile Ad Hoc Networks (MANETs),” *IJCSNS International Journal of Computer Science and Network Security,* vol. VOL.7, no. No.11, 2007. |
| [20] | “Research Gate,” [Online]. Available: https://www.researchgate.net/publication/279464781\_To\_find\_cost\_effective\_routes\_that\_are\_able\_to\_meet\_the\_fueltime\_constraints\_using\_the\_Intelligent\_Transportation\_Systems\_in\_VANETS. |