Applied Computer Science, vol.19, no. 3, pp. 133–159
doi:10.35784/acs-2023-29

Submitted: 2023-04-04 | Revised: 2023-08-23 | Accepted: 2023-08-28

Keywords: MANETs, ZRP, DoS, Encryption, Hashing

Md. Torikur RAHMAN [0000-0003-2173-6458]*, Mohammad ALAUDDIN*,
Uttam Kumar DEY*, Dr. A.H.M. Saifullah SADI*

ADAPTIVE, SECURE AND EFFICIENT ROUTING PROTOCOL TO ENHANCE THE PERFORMANCE OF MOBILE AD HOC NETWORK (MANET)

Abstract

Nowadays Mobile Ad Hoc Network (MANET) is an emerging area of research to provide various communication services to end users. Mobile Ad Hoc Networks (MANETs) are self-organizing wireless networks where nodes communicate with each other without a fixed infrastructure. Due to their unique characteristics, such as mobility, autonomy, and ad hoc connectivity, MANETs have become increasingly popular in various applications, including military, emergency response, and disaster management. However, the lack of infrastructure and dynamic topology of MANETs pose significant challenges to designing a secure and efficient routing protocol. This paper proposes an adaptive, secure, and efficient routing protocol that can enhance the performance of MANET. The proposed protocol incorporates various security mechanisms, including authentication, encryption, key management, and intrusion detection, to ensure secure routing. Additionally, the protocol considers energy consumption, network load, packet delivery fraction, route acquisition latency, packets dropped and Quality of Service (QoS) requirements of the applications to optimize network performance. Overall, the secure routing protocol for MANET should provide a reliable and secure communication environment that can adapt to the dynamic nature of the network. The protocol should ensure that messages are delivered securely and efficiently to the intended destination, while minimizing the risk of attacks and preserving the network resources Simulation results demonstrate that the proposed protocol outperforms existing routing protocols in terms of network performance and security. The proposed protocol can facilitate the deployment of various applications in MANET while maintaining security and efficiency.

* Uttara University, Department of Computer Science & Engineering, Dhaka, Bangladesh,
torikurrahman@gmail.com, md.alauddin@uttarauniversity.edu.bd, uttam@uttarauniversity.edu.bd,
saifullah.cse@uttarauniversity.edu.bd

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have gained significant attention in recent years due to their flexibility and ability to operate without a fixed infrastructure. Mobile Ad Hoc Networks are characterized by their dynamic topology, autonomous node behaviour, and limited resources, which pose unique challenges for designing efficient and secure routing protocols. Routing in a MANET is a critical task that directly affects network performance and security (Aroulanandam, V. V., Latchoumi, T. P., Balamurugan, K., & Yookesh, T. L., 2020; Ramphull, D., Mungur, A., Armoogum, S., & Pudaruth, S., 2021). Several routing protocols have been proposed to address the challenges of a MANET, such as Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) (Ramphull, D., Mungur, A., Armoogum, S., & Pudaruth, S., 2021). These protocols utilize various techniques to discover and maintain routes between nodes. However, these protocols suffer from various security vulnerabilities, such as packet dropping, node impersonation, and blackhole attacks, that can severely compromise the network's security. To address the security challenges of a MANET, several secure routing protocols have been proposed, such as Secure Ad Hoc On-Demand Distance Vector (SAODV) and Secure Efficient Ad Hoc Distance Vector (SEAD) (Sirajuddin, M., Rupa, C., Iwendi, C., & Biamba, C., 2021). These protocols utilize various security mechanisms, such as authentication, encryption, and key management, to ensure secure routing. However, these protocols do not consider the dynamic nature of a MANET, which can result in suboptimal network performance. This paper proposes an adaptive, secure, and efficient routing protocol for a MANET that considers the dynamic nature of a MANET to enhance network performance while maintaining security (Saminathan, K., & Thangavel, R., 2022). The proposed protocol incorporates various security mechanisms, such as authentication, encryption, key management, and intrusion detection, to ensure secure routing. Additionally, the protocol considers energy consumption, network load, and Quality of Service (QoS) requirements of the applications to optimize network performance (Vinoth Kumar, V., Deepa, R., Ranjith, D., Balamurugan, M., & Balajee, J. M., 2022). Simulation results demonstrate that the proposed protocol outperforms existing routing protocols in terms of network performance and security.

2. AD HOC NETWORKING

Ad hoc networking refers to the formation of a network on the fly, without the need for any pre-existing infrastructure or centralized control. In other words, it is a decentralized form of networking in which each node in the network acts as both a transmitter and a receiver of data packets. Ad hoc networks are typically formed by wireless devices such as smartphones, laptops, and tablets, which communicate directly with each other over short distances using Wi-Fi or Bluetooth technology (Sk, K. B., Vellela, S. S., Yakubreddy, K., & Rao, M. V., 2023). Because these networks are formed spontaneously and without any centralized control, they are often used in situations where traditional networks are unavailable, such as in disaster zones or remote areas. One of the key challenges of ad hoc networking is ensuring reliable communication in a dynamic and often unpredictable environment. To overcome this challenge, various protocols and algorithms have been developed that allow nodes to discover and connect with each other, exchange data, and adapt to changes in the network topology (Agrawal, R., Faujdar, N., Romero, C. A. T., Sharma, O., Abdulsahib, G. M., Khalaf, O. I., ... & Ghoneim, O. A., 2022). Ad hoc networks have a wide range of applications, from military and emergency communications to collaborative work and social networking. As wireless technology continues to advance, the potential for ad hoc networking to transform the way we communicate and interact with each other is only increasing.

2.1. Mobile Ad Hoc Networks

A Mobile Ad Hoc Network (MANET) is a type of ad hoc network in which the nodes are mobile devices, such as smartphones or laptops, that can move freely and dynamically to form and break connections with other nodes (Aroulanandam, V. V., Latchoumi, T. P., Balamurugan, K., & Yookesh, T. L., 2020; Ramphull, D., Mungur, A., Armoogum, S., & Pudaruth, S., 2021). In a MANET, there is no fixed infrastructure or centralized control, and each node in the network acts as both a transmitter and a receiver of data packets. The dynamic nature of a MANET poses unique challenges for communication, such as limited bandwidth, high packet loss rates, and the need for efficient routing protocols that can adapt to changes in the network topology (Sirajuddin, M., Rupa, C., Iwendi, C., & Biamba, C., 2021; Saminathan, K., & Thangavel, R., 2022). To address these challenges, various routing protocols have been developed, including proactive, reactive, and hybrid protocols, that enable nodes to discover and communicate with each other. In Mobile Ad Hoc Networks (MANETs), bootstrapping refers to the process of discovering and joining the network. As MANETs lack a fixed infrastructure, the bootstrapping process plays a crucial role in enabling nodes to establish connectivity and participate in the network. In the context of bootstrapping, discovery involves the identification and detection of neighbouring nodes within the radio range. Nodes in MANETs typically employ techniques such as broadcasting or probing to discover other nodes in their vicinity. This process allows nodes to create an initial network topology and establish communication links with neighbouring nodes. Once the discovery process is complete, the joining phase begins, where a node seeks to become an active member of the MANET.

Joining involves obtaining necessary network parameters, such as routing information and security credentials, to effectively participate in network operations. This phase often includes exchanging control messages with existing network nodes and acquiring the required configuration details. Overall, bootstrapping in a MANET involves the discovery and joining phases, where nodes identify neighbouring nodes and acquire the necessary network parameters to participate in the network. While there is potential for a central point of control or specialized nodes, it is essential to strike a balance between centralized coordination and distributed control to ensure robustness and adaptability in MANETs bootstrapping mechanisms. Mobile Ad Hoc Networks have a wide range of potential applications, including military and emergency communications, disaster response, and personal and social networking. They can also be used in scenarios where traditional network infrastructure is unavailable or impractical, such as in remote or underdeveloped areas (Saminathan, K., & Thangavel, R., 2022; Vinoth Kumar, V., Deepa, R., Ranjith, D., Balamurugan, M., & Balajee, J. M., 2022). However, MANETs also pose security challenges, such as the risk of attacks from malicious nodes, the difficulty of securing routing protocols, and the lack of a centralized authority for network management. As a result, ensuring the security of a MANET is an ongoing research challenge. As shown in Figure 1, an ad hoc network might consist of several home-computing devices, including laptops, cellular phones, and so on. Each node will be able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop.

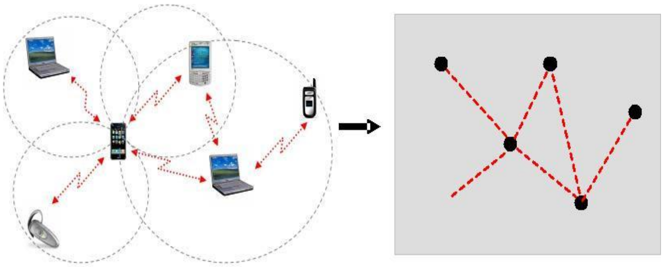


Fig. 1. A Typical Mobile Ad Hoc Network

2.2. MANET Applications

Mobile Ad Hoc Networks (MANETs) have a wide range of potential applications in various fields. Some of the common MANET applications are:

- Military and emergency communications: MANETs are often used in military operations and emergency response situations, where traditional communication infrastructures may be unavailable or damaged. MANETs provide a quick and efficient way for troops or emergency responders to communicate with each other in real-time, even in remote or disaster-stricken areas (Aroulanandam, V. V., Latchoumi, T. P., Balamurugan, K., & Yookesh, T. L., 2020).

- Disaster response: In the aftermath of a natural disaster, communication networks may be severely damaged or destroyed. Mobile Ad Hoc Networks can be used to quickly establish communication links between rescue teams, volunteers, and affected communities, enabling the exchange of critical information, such as medical needs or locations of survivors.
- Personal and social networking: MANETs can be used to create ad hoc social networks or communities, where people can communicate and share information without relying on traditional social media platforms or internet connectivity. For example, groups of hikers or campers in remote areas can create a MANET to communicate with each other and share photos or videos of their experiences.
- Industrial and commercial applications: MANETs can be used in industrial and commercial settings, such as in warehouses, factories, or construction sites, where devices need to communicate with each other in real-time without relying on a fixed infrastructure.
- Internet of Things (IoT) and smart city applications: a MANET can be used to support the communication needs of IoT devices, such as sensors and actuators, in a smart city environment. Mobile Ad Hoc Networks can enable devices to communicate with each other and exchange data in real-time, without relying on a centralized control system.
- Overall, the potential applications of MANETs are vast, and as wireless technology continues to advance, the opportunities for their use in various fields will only continue to grow.

3. EXISTING ROUTING APPROACHES IN MANET

There are several routing approaches that are commonly used in Mobile Ad Hoc Networks (MANETs). These include:

- Proactive routing: This approach, also known as table-driven routing, is characterized by the maintenance of a complete routing table for each node in the network (Xu, K., Hong, X., & Gerla, M., 2002). This ensures that routes are always available, but it requires a significant amount of overhead for route discovery and maintenance. Examples of proactive routing protocols include Optimized Link State Routing (OLSR) and Destination-Sequenced Distance Vector (DSDV).
- Reactive routing: This approach, also known as on-demand routing, is characterized by the discovery of routes only when they are required. When a node wants to send a packet to a destination, it initiates a route discovery process to find a path to the

destination (Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y., 2022). This approach minimizes overhead, but it can lead to delays in packet delivery. Examples of reactive routing protocols include Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR).

- Hybrid routing: This approach is a combination of proactive and reactive routing. In hybrid routing, nodes maintain a partial routing table for frequently communicated destinations, while other routes are discovered on demand. This provides a good balance between overhead and delays (Shajin, F. H., & Rajesh, P., 2022). Examples of hybrid routing protocols include Zone Routing Protocol (ZRP) and Temporally Ordered Routing Algorithm (TORA).
- Geographic routing: This approach, also known as position-based routing, is characterized by the use of physical location information to make routing decisions. Nodes forward packets to the nearest neighbour that is closer to the destination. This approach is efficient and scalable, but it requires accurate location information for all nodes in the network. Examples of geographic routing protocols include Greedy Perimeter Stateless Routing (GPSR) and Geographic Distance Routing (GEDIR).

The choice of routing protocol depends on the specific application requirements and network characteristics. Proactive routing is more suitable for networks with high traffic loads, while reactive routing is more suitable for networks with low traffic loads. Hybrid routing is suitable for networks with a mixture of traffic loads, while geographic routing is suitable for networks with a relatively stable topology.

4. SECURITY IN MOBILE AD HOC NETWORKS

There are several security mechanisms that can be employed to enhance the security of a MANET. These include:

- Authentication: This mechanism is used to verify the identity of nodes in the network before allowing them to participate in network operations (Shantaf, A. M., Kurnaz, S., & Mohammed, A. H., 2020). It can prevent unauthorized access to the network and protect against impersonation attacks.
- Encryption: This mechanism is used to protect the confidentiality of data transmitted over the network. Encryption algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) can be used to encrypt the data and ensure that it can only be read by authorized recipients.
- Intrusion Detection and Prevention Systems (IDPS): IDPSs can be deployed in the network to monitor network traffic and detect potential security threats (Quy, V. K.,

Nam, V. H., Linh, D. M., & Ngoc, L. A., 2022). They can be used to prevent and mitigate attacks by identifying and blocking suspicious traffic.

- Secure Routing: Secure routing protocols can be used to prevent routing attacks such as blackhole and grayhole attacks. These protocols employ various techniques such as digital signatures and reputation-based mechanisms to ensure that only trusted nodes are involved in the routing process.
- Key Management: Key management protocols are used to generate, distribute, and manage encryption keys used in the network (Soomro, A. M., Fudzee, M. F. B. M., Hussain, M., Saim, H. M., Zaman, G., Atta-ur-Rahman, H. A., & Nabil, M., 2022). They can be used to ensure that only authorized nodes have access to the keys and prevent unauthorized access to network resources.
- Trust Management: Trust management protocols are used to evaluate the trustworthiness of nodes in the network. They can be used to ensure that only trusted nodes are involved in network operations and prevent malicious nodes from compromising the security of the network.

These security mechanisms can be used individually or in combination to enhance the security of a MANET. The choice of the mechanism depends on the specific application requirements and the level of security needed to protect the network and its resources.

4.1. Security Attacks

Mobile Ad Hoc Networks (MANETs) are vulnerable to various security attacks due to their dynamic and decentralized nature. These attacks can compromise the confidentiality, integrity, and availability of data and network resources, and can disrupt the normal functioning of the network (Pamarthi, S., & Narmadha, R., 2022). Some common security attacks in MANETs include:

- Eavesdropping: In this attack, an attacker intercepts and monitors the communication between two nodes in the network, thereby compromising the confidentiality of the data being transmitted.
- Jamming: This attack involves an attacker sending high-power interference signals to disrupt the wireless transmission between nodes, making it difficult for legitimate communication to take place.
- Denial of Service (DoS): This attack aims to prevent legitimate nodes from accessing the network by flooding the network with illegitimate traffic or consuming network resources such as bandwidth, processing power, or memory.
- Blackhole: In this attack, a malicious node advertises itself as having the shortest path to the destination, attracting all traffic to itself and dropping it, thereby disrupting the network.

- Wormhole: This attack involves two or more colluding attackers creating a tunnel in the network, allowing them to intercept and modify the traffic between nodes (Kariyannavar, S. S., Thakur, S., & Maheshwari, A., 2021).
- Sybil: In this attack, a single node creates multiple fake identities in the network, allowing it to launch further attacks or gain unauthorized access.
- Spoofing: This attack involves an attacker impersonating a legitimate node in the network to gain unauthorized access or inject false information into the network.

These attacks can be prevented and mitigated by employing various security mechanisms such as authentication, encryption, secure routing, intrusion detection, prevention systems and trust management. The choice of security mechanism depends on the specific requirements and the level of security needed to protect the network and its resources.

4.2. Security Mechanisms and Solutions

Some common security mechanisms and solutions in MANETs include:

- Authentication: This mechanism involves verifying the identity of nodes in the network to prevent unauthorized access. Various authentication protocols can be used, such as password-based authentication, public-key cryptography, and digital certificates.

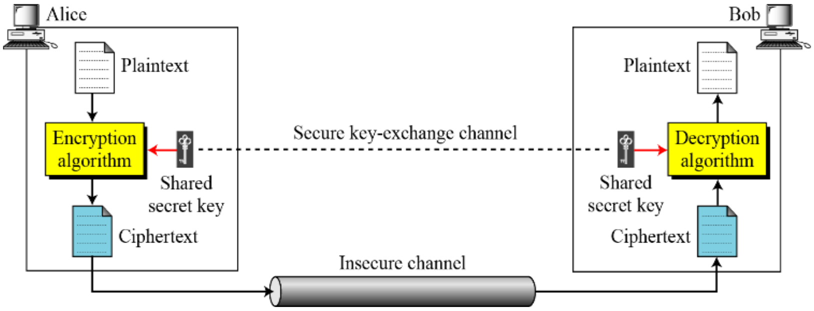


Fig. 2. General idea of symmetric-key cryptosystem

- Encryption: This mechanism involves transforming plaintext into ciphertext to ensure confidentiality (Navaneethan, T., & Lalli, M., 2014). Various encryption algorithms can be used, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA).
- Secure Routing: This mechanism involves designing routing protocols that can resist various attacks such as blackhole, wormhole, and Sybil attacks. Examples of secure routing protocols include Ad hoc On-Demand Distance Vector (AODV),

Secure Efficient Ad hoc Distance Vector (SEAD), and Zone Routing Protocol (ZRP).

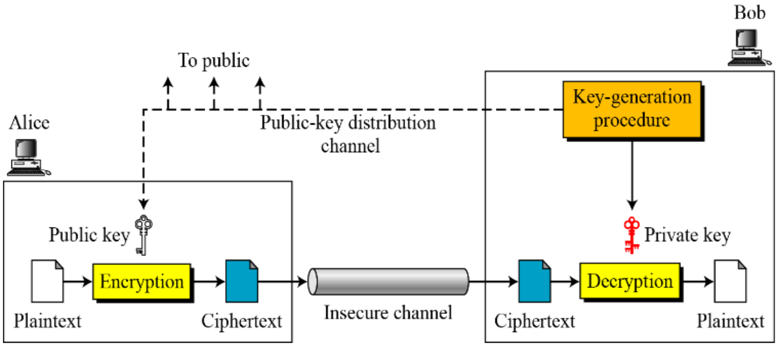


Fig. 3. General idea of asymmetric-key cryptosystem

- Intrusion Detection and Prevention Systems (IDPS): These systems aim to detect and prevent attacks by monitoring the network traffic and identifying suspicious behaviour. Examples of IDPSs in MANETs include anomaly-based detection and signature-based detection.
- Trust Management: This mechanism involves establishing and maintaining trust relationships among nodes in the network to prevent attacks such as Sybil and spoofing attacks (Tsao, K. Y., Girdler, T., & Vassilakis, V. G., 2022). Examples of trust management protocols in MANETs include the EigenTrust algorithm and the Trust-Based Secure Routing protocol (TSRP).
- Key Management: This mechanism involves managing cryptographic keys used for authentication and encryption. Various key management protocols can be used, such as the Simple Key-management for Internet Protocol (SKIP) protocol and the Public Key Infrastructure (PKI) protocol.

These security mechanisms and solutions can be used individually or in combination to provide a robust and secure environment for MANETs. The choice of the mechanism depends on the specific requirements and the level of security needed to protect the network and its resources.

4.3. Digital signature and Hashing

Digital signature and hashing are two important security mechanisms used in Mobile Ad Hoc Networks (MANETs).

Digital Signature: Digital signature is a cryptographic mechanism used to verify the authenticity and integrity of messages in MANETs (Tsao, K. Y., Girdler, T., & Vassilakis,

V. G., 2022). A digital signature is a mathematical scheme that provides a mechanism to verify the authenticity of digital documents or messages. It provides the recipient with proof that the message was sent by the sender and that the message has not been tampered with during transmission. The digital signature is created using the sender's private key and can be verified using the sender's public key (Pamarthi, S., & Narmadha, R., 2022). In MANETs, the digital signature is commonly used for authentication and non-repudiation of messages. It ensures that the message comes from a legitimate sender and cannot be denied later by the sender.

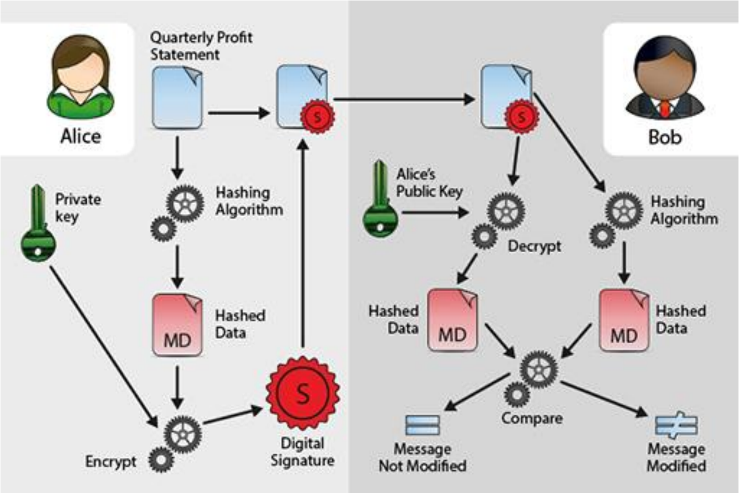


Fig. 4. Illustration of the digital signature process

4.4. Hashing

Hashing is a technique used to generate a unique and fixed-length value (called hash) from a variable-length input message. Hashing ensures the integrity of data by detecting any changes made to the message during transmission. Even a small change in the message will result in a completely different hash value (Shekhar, S., Mahajan, M., & Kaur, S., 2022). Hashing algorithms are one-way functions, meaning that it is practically impossible to derive the original message from the hash value.

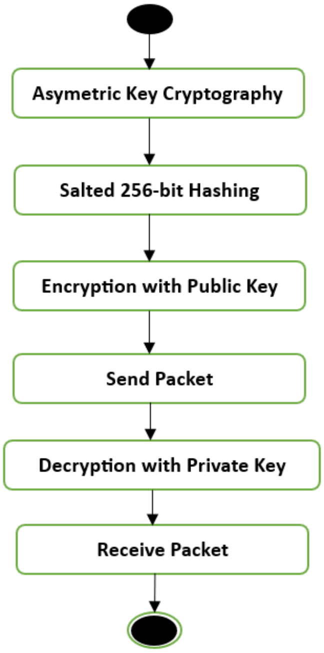

Asymetric Key Cryptography
Salted 256-bit Hashing
Encryption with Public Key
Send Packet
Decryption with Private Key
Receive Packet

Fig. 5. Flowchart of overall Security Mechanisms

In MANETs, hashing is used to ensure that messages are not altered during transmission. It is commonly used in combination with digital signatures to ensure the authenticity and integrity of messages. Overall, digital signature and hashing are important security mechanisms used in MANETs to ensure the authenticity, integrity, and confidentiality of messages. They help to provide a secure and reliable communication environment for MANETs.

4.5. Requirements for a Secure Routing Protocol

A secure routing protocol for Mobile Ad Hoc Networks (MANETs) must meet the following requirements:

- Correctness: The routing protocol must be able to find a correct path to the destination node. It should be able to select a path that avoids any malicious nodes that may attempt to disrupt the communication.
- Availability: The routing protocol must be able to maintain network connectivity in the presence of node failures, mobility, and other network disruptions.
- Efficiency: The routing protocol should use network resources efficiently, including bandwidth, power, and processing time. It should minimize the overhead of message exchanges and computation (Nagpal, S., Aggarwal, A., & Gaba, S., 2022).

- Scalability: The routing protocol must be scalable, meaning that it can handle a large number of nodes without compromising performance or security.
- Security: The routing protocol must be resistant to various security threats, including black hole, gray hole, wormhole, and Sybil attacks. It should also provide mechanisms for authentication, confidentiality, and integrity of routing messages.
- Self-organizing: The routing protocol should be able to adapt to changes in the network topology and traffic patterns without any central coordination (Schaumann, J., 2002). It should be able to self-organize and self-heal in response to node mobility, failures, and network partitioning.
- Compatibility: The routing protocol should be compatible with existing network infrastructure, standards, and protocols. It should be able to coexist with other routing protocols and support interoperability with other networks (Tripathy, B. K., Jena, S. K., Bera, P., & Das, S., 2020).

Overall, a secure routing protocol for MANETs should provide a reliable and safe communication environment that can adapt to the dynamic nature of the network. The protocol should ensure that messages are delivered steadily and efficiently to the intended destination while minimizing the risk of attacks and preserving the network resources.

5. PROPOSED PROTOCOL OVERVIEW

Neither a pure proactive nor a purely reactive approach provides a full solution for secure ad hoc routing that performs efficiently across a wide range of operational requisites and network configurations. A complete, efficient and implementable solution for secure routing is highly desirable that can operate well on diverse applications of mobile ad hoc networks. We use the hash function in MANETs. The proposed protocol is developed on the concept of Zone Routing Protocol (ZRP) (Hinds, A., Ngulube, M., Zhu, S., & Al-Aqrabi, H., 2013). It is a hybrid routing protocol that is comprised of the best features of both proactive and reactive approaches and adds its own security mechanisms to perform secure routing. The reasons for selecting ZRP as the basis of my protocol are as follows: ZRP is based on the concept of routing zones, a restricted area, and it is more feasible to apply the security mechanisms within a restricted area than in a broader area of the whole network (Bagwari, A., Jee, R., Joshi, P., & Bisht, S., 2012). Since the concept of zones separates the communicating nodes in terms of the interior (nodes within the zone) and exterior (nodes outside the zone) nodes, certain information like network topology and neighbourhood information etc. can be hidden from the exterior nodes, in case of a failure, it can be restricted to a zone. Like ZRP the proposed protocol performs routing in terms of intra-zone and inter-zone routing. However, it differs from ZRP (Sirmollo, C. Z., & Bitew, M. A., 2021) in security aspects. In ZRP where there is no security consideration, the proposed protocol is designed to address all measure security concerns like end-to-end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing.

Tab. 1. Notations Used in the Proposed Protocol

Notation	Description
SK_X	Signature Key of node X (A private key used by X for signing)
VK_X	Signature verification key for node X. (A public key provided by X to verify its signature done with SK_X)
EK_X	Encryption Key for node X (A public key supplied by node X for encrypting any message to be sent to X)
DK_X	Decryption Key of node X (A private key used by X for decrypting any message which is encrypted with EK_X)
[d] SK_X	Packet 'd' signed with SK_X, this can be only verified using VK_X
{d}EK_X	Message 'd' encrypted with EK_X, this can be only decrypted with DK_X
[d] | b	b is appended to the packet containing d
$cert_X$	Public key certificate of X.
IP_X	IP address of X
t	Time stamp
e	Certificate expiration time
N_X	Nonce issued by node X
SKREQ	Session Key Request packet identifier
SKREP	Session Key Reply packet identifier
SRD	Secure Route Discovery packet identifier
SRR	Secure Route Reply packet identifier
ERR	Error packet identifier

5.1. Certification Process

The proposed Protocol requires the presence of trusted certification servers called certification authorities (CAs) in the network. The CAs are assumed to be safe, whose public keys are known to all valid CNs. Keys are generated a priori and exchanged through an existing, perhaps out-of-band, relationship between CA and each CN. Before entering the ad hoc network, each node requests a certificate from its nearest CA. Each node receives exactly one certificate after securely authenticating its identity to the CA. The idea is depicted in Figure 6. The methods for secure authentication to the certificate server are numerous and hence it is left to the developers; a significant list is provided by.

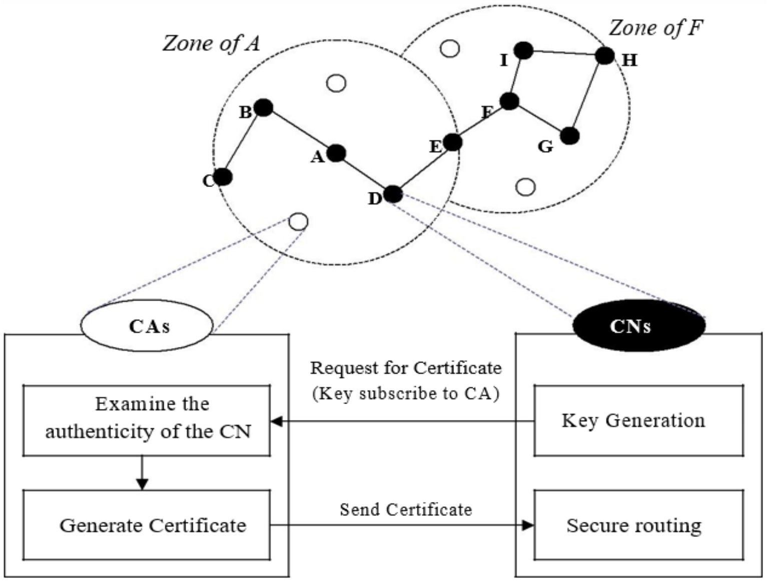


Fig. 6. Certification Process in SZ

5.2. The Secure Routing Algorithm

This section describes the secure intra-zone and inter-zone routing in detail. For illustration, the network shown in Figure 7 is considered.

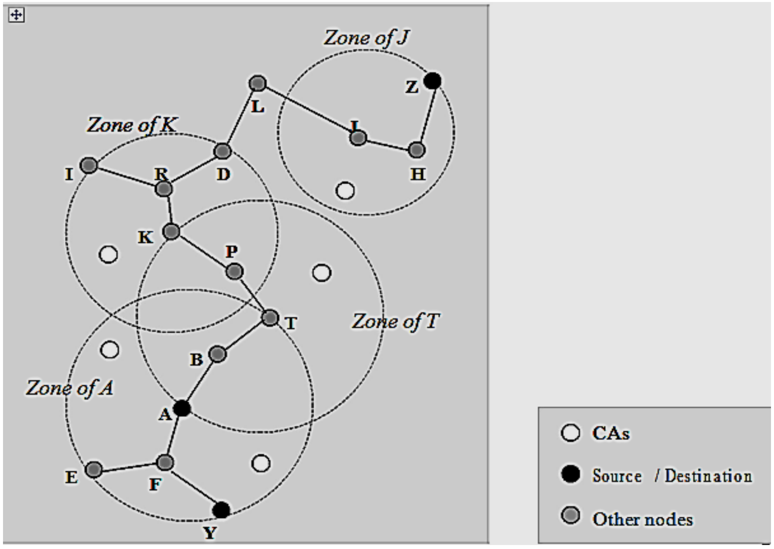


Fig. 7. Intra-zone and Inter-zone destinations of node A (zone radius = 2)

5.3. Secure Intra-Zone Routing (IARP)

Secure Intra-Zone Routing Protocol (IARP) is a secure routing protocol designed for Mobile Ad Hoc Networks (MANETs). IARP is designed to provide secure and efficient routing within a predefined security zone in the network. The security zone is defined as a group of nodes that share a common security policy, such as a group of nodes that belong to a particular organization or department. The security zone is established using a key management scheme, where each node in the zone shares a secret key with other nodes in the zone. IARP provides a secure and efficient routing mechanism within the security zone by using a combination of cryptographic techniques, including digital signatures, message authentication codes (MACs), and hop-by-hop encryption. Each node in the security zone maintains a routing table that contains information about the destination nodes and the next-hop nodes to reach them. When a node wants to send a message to a destination node, it first consults its routing table to find the next-hop node for the destination. The node then creates a packet that contains the message and attaches a digital signature and a MAC to the packet. The digital signature and MAC ensure the authenticity and integrity of the packet. The packet is then encrypted using hop-by-hop encryption and sent to the next-hop node. The next-hop node repeats the same process until the packet reaches the destination node. Overall, Secure Intra-Zone Routing Protocol (IARP) provides a secure and efficient routing mechanism within a predefined security zone in Mobile Ad Hoc Networks (MANETs). It ensures the authenticity, integrity, and confidentiality of messages while minimizing the risk of attacks.

A typical SIARP routing table at maintained at node *A* is shown in Table 2.

Tab. 2. SIARP routing table maintained at node *A*

Destination Address	Routes	Route metrics
Y	A-F-Y	....
T	A-B-T	....
E	A-F-E	....
F	A-F	....
B	A-B	....

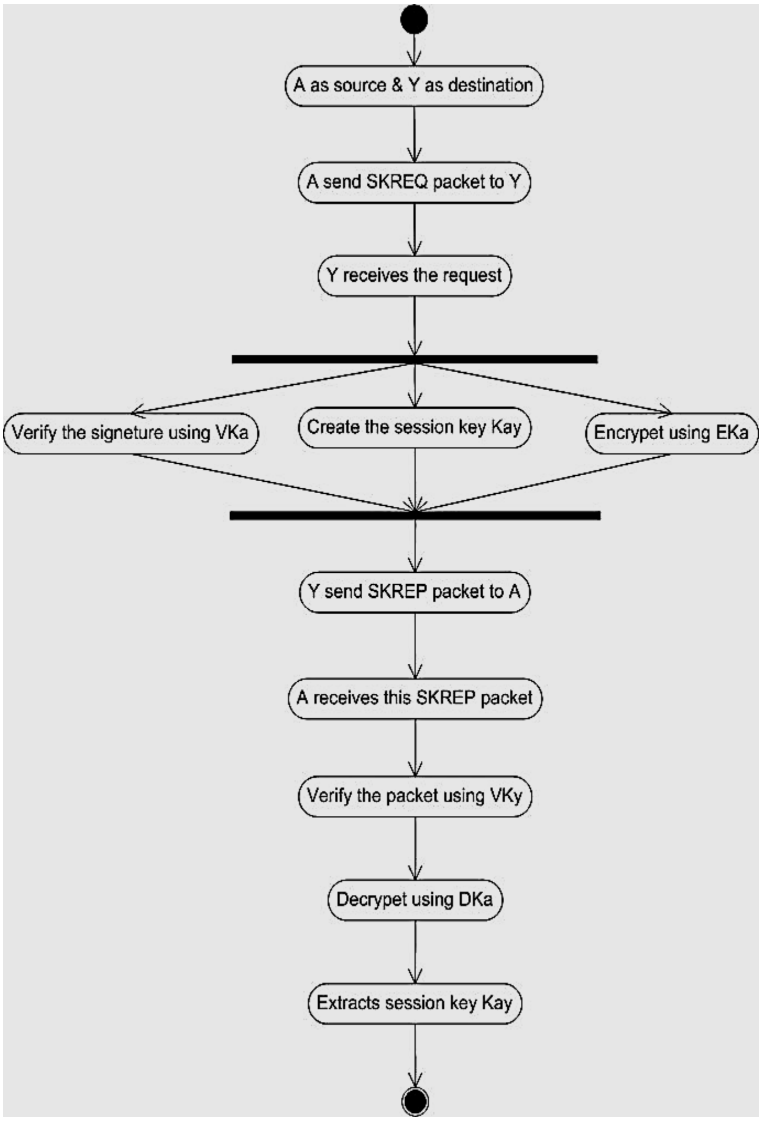

A as source & Y as destination
A send SKREQ packet to Y
Y receives the request
Verify the signeture using VKa
Create the session key Kay
Encrypet using EKa
Y send SKREP packet to A
A receives this SKREP packet
Verify the packet using VKy
Decrypet using DKa
Extracts session key Kay

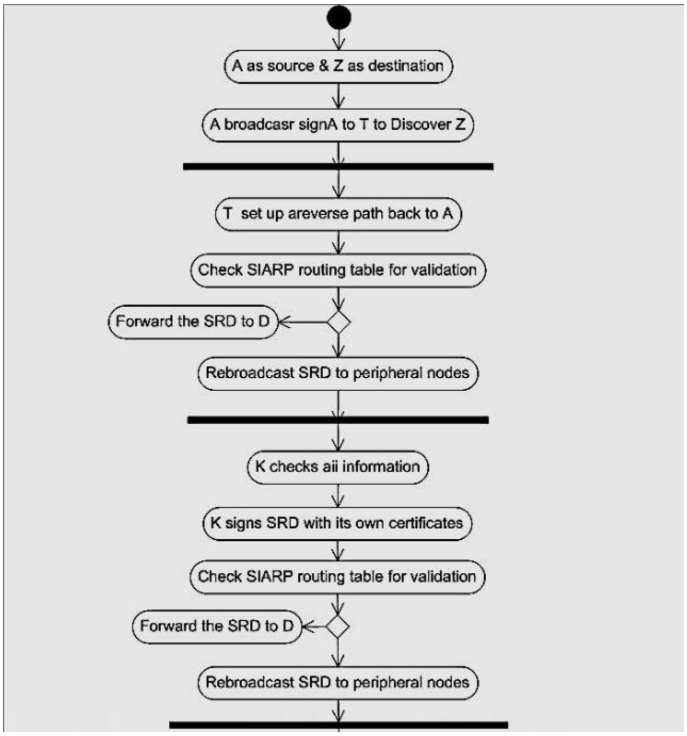
Fig. 8. Basic activity diagram of Secure Intra-zone routing

5.4. Secure Inter-Zone Routing (IERP)

Secure Inter-Zone Routing (IERP) is a secure routing protocol for Mobile Ad Hoc Networks (MANETs) that is designed to provide secure communication between different security zones. IERP allows for communication between nodes in different zones while maintaining the security and confidentiality of the communication. IERP is designed to work in conjunction with the Secure Intra-Zone Routing (IARP) protocol, which provides secure communication within a predefined security zone. IERP extends IARP's security mechanisms to allow for secure communication between different security zones. IERP uses a proactive routing approach and a hierarchical architecture similar to IARP. Each security zone has a designated zone leader responsible for managing the routing information and security within the zone. In addition, IERP also has a designated inter-zone coordinator responsible for managing the communication between different zones. The main goal of IERP is to provide secure and efficient routing between different security zones while minimizing the risk of attacks and preserving the confidentiality of communication. To achieve this goal, IERP uses several security mechanisms, including:

- Authentication: IERP uses digital signatures to authenticate the routing messages between the nodes in different security zones. Each node has a unique public/private key pair, and messages are signed using the sender's private key and verified using the sender's public key.
- Authorization: IERP uses access control mechanisms to ensure that only authorized nodes can participate in the routing process between different security zones. Each node has a set of security credentials that determine its level of access and authority between different zones.
- Encryption: IERP uses encryption to ensure the confidentiality of routing messages between different security zones. Each message is encrypted using the receiver's public key, and only the receiver with the corresponding private key can decrypt the message.
- Key Management: IERP uses a key management system to manage the public/private key pairs used for authentication and encryption. The key management system ensures that the keys are distributed securely and that they are updated periodically to maintain their effectiveness.

Overall, Secure Inter-Zone Routing (IERP) provides a secure and efficient routing protocol for Mobile Ad Hoc Networks (MANETs) between different security zones. It ensures the confidentiality, authenticity, and integrity of routing messages while minimizing the risk of attacks and preserving network resources.


A as source & Z as destination
A broadcasr signA to T to Discover Z
T set up areverse path back to A
Check SIARP routing table for validation
Forward the SRD to D
Rebroadcast SRD to peripheral nodes
K checks aii information
K signs SRD with its own certificates
Check SIARP routing table for validation
Forward the SRD to D
Rebroadcast SRD to peripheral nodes

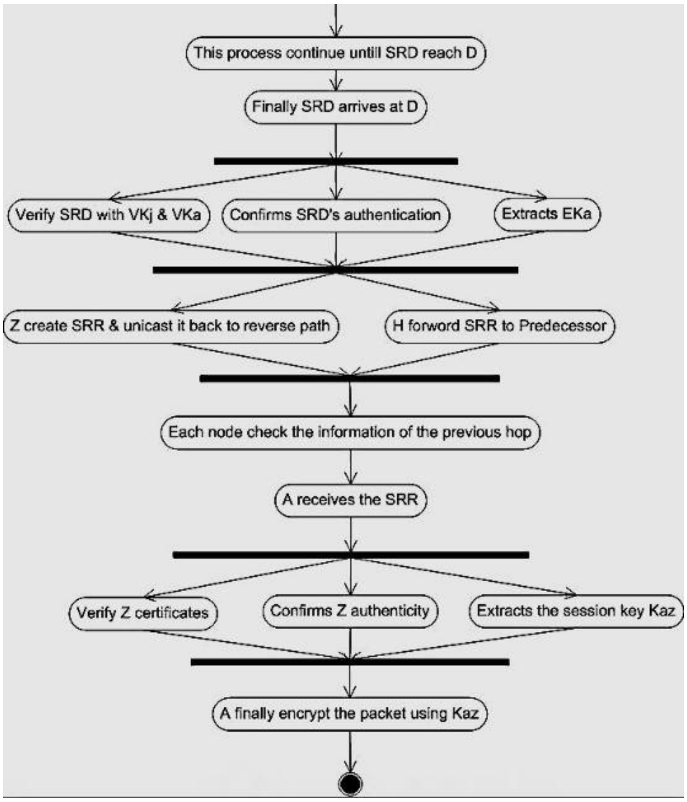

This process continue untill SRD reach D
Finally SRD arrives at D
Verify SRD with VKj & VKa
Confirms SRD's authentication
Extracts EKa
Z create SRR & unicast it back to reverse path
H forword SRR to Predecessor
Each node check the information of the previous hop
A receives the SRR
Verify Z certificates
Confirms Z authenticity
Extracts the session key Kaz
A finally encrypt the packet using Kaz

Fig. 9. Basic activity diagram of Secure Inter-zone routing

5.5. Analysis of Proposed Secure Routing Protocol

In this section, the authors analyze the security aspects of the proposed Routing Protocol by evaluating its robustness in the presence of various security attacks. The proposed Protocol can prevent all types of attacks that include information disclosure, impersonation, modification, fabrication and replay of packets caused by both an external advisory and an internal compromised node.

- Prevention from Information Disclosure: No hop count information is present in the SRD or SRR packets. This prevents an external advisory or an internal compromised node from getting any kind of information about the network topology. Topology information is restricted to nodes within a zone (Tahboush, M., & Agoyi, M., 2021). This is harmless as nodes accept packets only after verifying the sender’s signature. Further, all the data packets and the control packets that contain the session key are encrypted which ensures confidentiality.

- Attacks involving impersonation: Proposed Protocol participants, accept only those packets that have been signed with a certified key issued by a CA (Fotohi, R., & Jamali, S., 2014). In intra-zone routing, since the SKREQs and SKREPs can only be signed by an authenticated source with its own private signature key, nodes can't impersonate (spoof) other nodes (Meddeb, R., Triki, B., Jemili, F., & Korbaa, O., 2017). Inter-zone routing follows hop-by-hop authentication during route discovery and end-to-end authentication during the route reply phase. So it is impossible for an external node or an internal compromised node to impersonate an intermediate node during inter-zone routing (Bhattacharyya, A., Banerjee, A., Bose, D., Saha, H. N., & Bhattacharya, D., 2011). Further, since the SRD packet is signed by the source node using its private key, it guarantees that only the source can initiate a route discovery process (Goyal, P., Batra, S., & Singh, A., 2010). Similarly, the SRR packets include the destination's certificate and signature, ensuring that only the destination can respond to the route discovery. This prevents attacks where the source, the destination or any intermediate nodes are spoofed e.g. man-in-the-middle attacks and Sybil attacks (Hamdi, M. M., Audah, L., Abood, M. S., Rashid, S. A., Mustafa, A. S., Mahdi, H., & Al-Hiti, A. S., 2021).
- Routing message Modification: Proposed Protocol specifies that all fields of LSPs, SRD and SRR packets remain unchanged between the source and the destination (Lilhore, U. K., Khalaf, O. I., Simaiya, S., Tavera Romero, C. A., Abdulsahib, G. M., & Kumar, D., 2022). Since all packets are signed by the initiating node, any alterations in transit would be immediately detected by intermediate nodes along the path, and the altered packets would be subsequently discarded (Xue, X., Shanmugam, R., Palanisamy, S., Khalaf, O. I., Selvaraj, D., & Abdulsahib, G. M., 2023). Repeated instances of altering packets could cause other nodes to exclude the errant node from routing. Thus, modification attacks like redirection of routing messages and DoS attacks are prevented.
- Fabrication of messages: Messages can be fabricated only by the internally compromised nodes with certificates (Liu, Y., Wu, H., Rezaee, K., Khosravi, M. R., Khalaf, O. I., Khan, A. A., ... & Qi, L., 2022). In that case, the Proposed Protocol does not prevent the fabrication of routing messages, but it does offer a deterrent by ensuring non-repudiation. A node that continues to inject false messages into the network may be excluded from future route computation.
- Replay Attacks: Replay attacks like tunnelling and wormhole (Hassan, H. J., Abdulsaheb, G. M., & Khalaf, O. I., 2022) attacks are prevented by including a nonce and a timestamp with routing messages.

6. SIMULATION FOR SECURE ROUTING PROTOCOL

6.1. Simulation Setup

The simulation of Secure Zone Routing Protocol (SZRP) was conducted in NS-allinone-2.1b6a, on an Intel Core(TM) i-3- 8100 CPU processor (3.60 GHz) and 4GB of RAM running Ubuntu 12.2. To make the results as general as possible, the authors have simulated SZRP to support nodes with moderate resources. The proposed protocol has been implemented over the ZRP protocol specification document for NS-2 with required modifications to support the adopted security mechanisms. In order to evaluate the performance of Secure Zone Routing Protocol (SZRP), both ZRP and SZRP were run and compared under identical mobility patterns and traffic scenarios. A basic version of ZRP was used, which did not include optimizations. This enables consistent comparison of results. Two classes of metrics were used to compare the performance of ZRP and SZRP. The first class of metrics evaluates both protocols under a non-adversarial network setting, assuming all the nodes in the network to be well-behaved and benign. The second class of metrics was used to compare their performances under a hostile environment where malicious nodes are present in the network.

6.2. Simulation Issues

- Average packet delivery fraction: This is the fraction of the data packets generated by the sources that are delivered to the destination.
- Average route acquisition latency: This is the average delay between the sending of a secure route discovery packet by a source for discovering a route to a destination and the receipt of the first corresponding route reply.
- Percentage of Packets Dropped that passed through Malicious Nodes: This metric indicates the percentage of total packets dropped that traverse malicious nodes when using each routing protocol. Assuming that all the packets that pass through a malicious or compromised node were altered, this metric can be calculated as follows:

$$\begin{array}{l}\textit{\% of Packets}\\ \textit{Dropped that}\\ \\ \textit{passed through}\\ \textit{Malicious Nodes}\end{array} = \left(\frac{\begin{array}{c}\textit{No. of packets dropped by the benign nodes}\\ \textit{that are previously generated by or passed}\\ \textit{through any malicious node in the network}\end{array}}{\textit{Total number of packets communicated}} \right) \text{X } 100$$

6.3. Simulation Result

- Average Packet Delivery Fraction: Figure 10 shows the observed results for the average packet delivery fraction for both the 10 and 20-node networks. As shown in Figure 10, the packet delivery fraction obtained using the proposed algorithm is above 96% in all scenarios and almost identical to that obtained using ZRP. This suggests that the proposed algorithm is highly effective in discovering and maintaining routes for the delivery of data packets, even with relatively high node mobility.

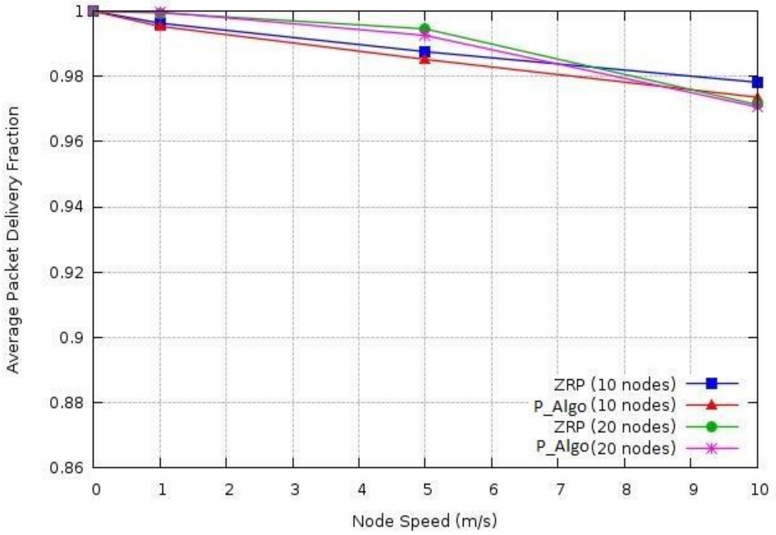


Fig. 10. Simulation Results – Average Packet Delivery Fraction

- Average Route Acquisition Latency: Figure 11 shows that the average route acquisition latency for the Proposed Protocol is approximately 2 times that of ZRP. For example, for 10 nodes moving at 5 m/s, it is 60ms as compared to 100ms for ZRP, while for 20 nodes moving at 10 m/s, it is nearly 135ms as compared to 75ms as in the case of ZRP. While processing proposed algorithm control packets, each node has to verify the digital signature of the previous node, and then replace this with its own digital signature, in addition to the normal processing of the packet as done by ZRP. This signature generation and verification causes additional delays at each hop, and so the route acquisition latency increases.

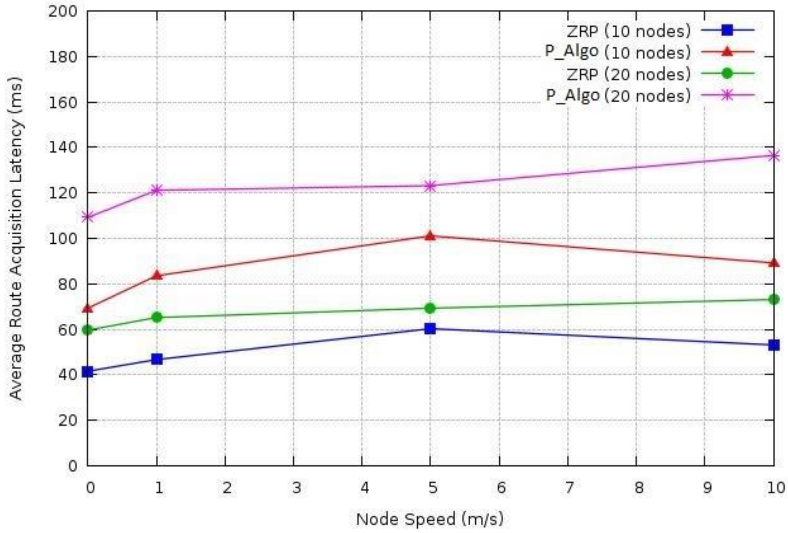


Fig. 11. Simulation Results – Average Route Acquisition Latency

- Percentage of Packets Dropped: As shown in Figure 12, when using the proposed algorithm, a much larger fraction of packets that passed through malicious nodes were dropped, as compared to that of ZRP. These results show that about 50% of packets that were possibly altered by malicious nodes in the network remained undetected and could potentially make their way through authentic nodes when using ZRP, as compared to the proposed protocol. This is a significant increase in the degree of security level.

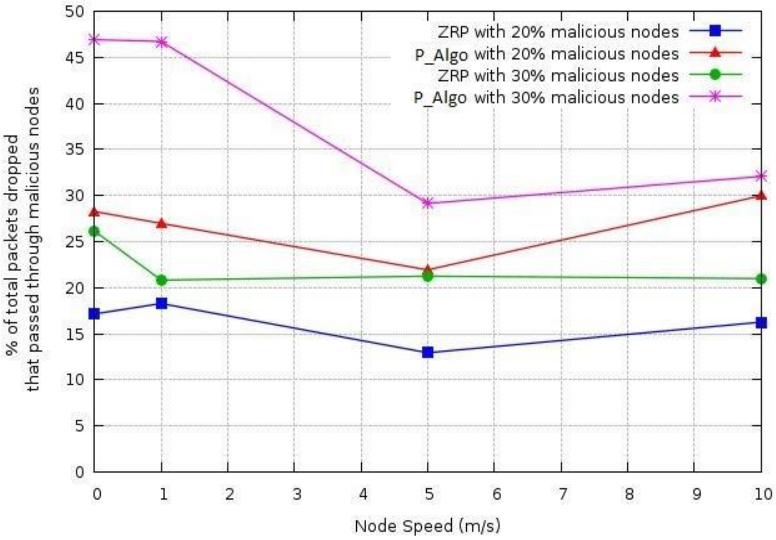


Fig. 12. Simulation Results – Percentage of Packets Dropped

7. CONCLUSION

Indeed, enhancing the performance of Mobile Ad Hoc Networks (MANETs) can make them the best choice for certain scenarios at the moment. Mobile Ad Hoc Networks offer several advantages that make them attractive in various applications, especially in situations where traditional fixed infrastructure networks are impractical or unavailable. By focusing on performance improvements, MANETs can become even more versatile and beneficial in many ways like, Flexibility and Mobility, Decentralized and Self-Organizing, Scalability, Internet of Things (IoT) Integration, Real-Time Applications and Resilience in Challenging Environments. However, it is essential to acknowledge that MANETs also have some inherent challenges, such as limited bandwidth, energy constraints, and potential security vulnerabilities. Addressing these challenges through performance improvements, efficient protocols, and security mechanisms is critical to realizing the full potential of MANETs. In conclusion, an adaptive, secure, and efficient routing protocol is essential to enhance the performance of Mobile Ad Hoc Networks (MANETs). The proposed protocol should be able to adapt to the network's dynamic topology and changing traffic patterns while maintaining the security and confidentiality of communication between nodes. To ensure secure routing, the protocol should incorporate various security mechanisms such as authentication, encryption, key management, and intrusion detection to guarantee the authenticity, confidentiality, and integrity of the routing messages. Additionally, the protocol should be able to detect and mitigate security attacks, such as Sybil attacks, flooding attacks, and sinkhole attacks, to ensure network availability. To optimize network performance, the routing protocol should consider factors such as energy consumption, network load, and Quality of Service (QoS) requirements of the applications. The protocol should be able to balance routing efficiency and security requirements to achieve optimal network performance. Overall, an adaptive, secure, and efficient routing protocol which is based on Zone Routing Protocol can significantly enhance the performance and security of Mobile Ad Hoc Networks (MANETs) and enable the deployment of various applications, including military, emergency response, and disaster management.

REFERENCES

Aroulanandam, V. V., Latchoumi, T. P., Balamurugan, K., & Yookesh, T. L. (2020). Improving the energy efficiency in mobile Ad-Hoc network using learning-based routing. *Revue d'Intelligence Artificielle*, *34*(3), 337-343. https://doi.org/10.18280/ria.340312

Ramphull, D., Mungur, A., Armoogum, S., & Pudaruth, S. (2021, May). A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. *2021 5th international conference on intelligent computing and control systems (ICICCS)* (pp. 204-211). IEEE. https://doi.org/10.1109/ICICCS51141.2021.9432258

Sirajuddin, M., Rupa, C., Iwendi, C., & Biamba, C. (2021). TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network. *Security and Communication Networks*, *2021*, 5521713. https://doi.org/10.1155/2021/5521713

Saminathan, K., & Thangavel, R. (2022). Energy efficient and delay aware clustering in mobile adhoc network: A hybrid fruit fly optimization algorithm and whale optimization algorithm approach. *Concurrency and Computation: Practice and Experience*, *34*(11), e6867. https://doi.org/10.1002/cpe.6867

Vinoth Kumar, V., Deepa, R., Ranjith, D., Balamurugan, M., & Balajee, J. M. (2022, February). Selection of routing protocol-based QoS improvement for mobile ad Hoc network. *International Conference on Computing, Communication, Electrical and Biomedical Systems* (pp. 317-330). Springer. https://doi.org/10.1007/978-3-030-86165-0_26

Sk, B., Reddy-B, V., Vellela, S. S., D, R., Yakubreddy, K., & Rao, M. V. (2023). Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation. *merging Technologies and Innovative Research*, *10*(3). https://ssrn.com/abstract=4429086

Agrawal, R., Faujdar, N., Romero, C. A. T., Sharma, O., Abdulsahib, G. M., Khalaf, O. I., Mansoor, R. F., & Ghoneim, O. A. (2022). Classification and comparison of ad hoc networks: A review. *Egyptian Informatics Journal*. *24*(1), 1-25. https://doi.org/10.1016/j.eij.2022.10.004

Xu, K., Hong, X., & Gerla, M. (2002, April). An ad hoc network with mobile backbones. *2002 IEEE international conference on communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333)* (Vol. *5*, pp. 3138-3143). IEEE. https://doi.org/10.1109/ICC.2002.997415

Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. *IEEE Access*, *10*, 14260-14269. 10.1109/ACCESS.2022.3144679

Shajin, F. H., & Rajesh, P. (2022). Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol. *International Journal* *of Pervasive Computing and Communications*, *18*(5), 603-621. https://doi.org/10.1108/IJPCC-09-2020-0136

Shantaf, A. M., Kurnaz, S., & Mohammed, A. H. (2020, June). Performance evaluation of three mobile ad-hoc network routing protocols in different environments. *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-6). IEEE. 10.1109/HORA49412.2020.9152845

Quy, V. K., Nam, V. H., Linh, D. M., & Ngoc, L. A. (2022). Routing algorithms for MANET-IoT networks: a comprehensive survey. *Wireless Personal Communications*, *125*(4), 3501-3525. https://doi.org/10.1007/s11277-022-09722-x

Soomro, A. M., Fudzee, M. F. B. M., Hussain, M., Saim, H. M., Zaman, G., Atta-ur-Rahman, H. A., & Nabil, M. (2022). Comparative review of routing protocols in manet for future research in disaster management. *Journal of Communications*, *17*(9). 734-744.

Pamarthi, S., & Narmadha, R. (2022). Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms. *International Journal of Intelligent Unmanned Systems*, *10*(4), 482-506. https://doi.org/10.1108/IJIUS-05-2021-0028

Kariyannavar, S. S., Thakur, S., & Maheshwari, A. (2021, January). Security in mobile ADHOC networks: Survey. *2021 6th International Conference on Inventive Computation Technologies (ICICT)* (pp. 135-143). IEEE. https://doi.org/10.1109/ICICT50816.2021.9358611

Navaneethan, T., & Lalli, M. (2014). Security attacks in Mobile Ad hoc Networks–A Literature Survey. *International Jouranl of Computer Science and Mobile Applications*, *2*(4), 1-7.

Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894. https://doi.org/10.1016/j.adhoc.2022.102894

Pamarthi, S., & Narmadha, R. (2022). Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms. *International Journal of Intelligent Unmanned Systems*, *10*(4), 482-506. https://doi.org/10.1108/IJIUS-05-2021-0028

Shekhar, S., Mahajan, M., & Kaur, S. (2022). A Comprehensive Review of Various Attacks in Mobile Ad Hoc Networks. *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 638-643). IEEE. https://doi.org/10.1109/ICOEI53556.2022.9777180

Nagpal, S., Aggarwal, A., & Gaba, S. (2022, January). Privacy and security issues in vehicular Ad Hoc networks with preventive mechanisms. In *Proceedings of International Conference on Intelligent Cyber-Physical Systems: ICPS 2021* (pp. 317-329). Springer Nature Singapore.

Schaumann, J. (2002). Analysis of the zone routing protocol.

Tripathy, B. K., Jena, S. K., Bera, P., & Das, S. (2020). An adaptive secure and efficient routing protocol for mobile ad hoc networks. *Wireless Personal Communications*, *114*, 1339-1370. https://doi.org/10.1007/s11277-020-07423-x

Hinds, A., Ngulube, M., Zhu, S., & Al-Aqrabi, H. (2013). A review of routing protocols for mobile ad-hoc networks (manet). *International journal of information and education technology*, *3*(1), 1-5.

Bagwari, A., Jee, R., Joshi, P., & Bisht, S. (2012, May). Performance of AODV routing protocol with increasing the MANET nodes and its effects on QoS of mobile ad hoc networks. *2012 International Conference on Communication Systems and Network Technologies* (pp. 320-324). IEEE. https://doi.org/10.1109/CSNT.2012.76

Sirmollo, C. Z., & Bitew, M. A. (2021). Mobility-aware routing algorithm for mobile ad hoc networks. *Wireless Communications and Mobile Computing*, *2021*, 1-12. https://doi.org/10.1155/2021/6672297

Tahboush, M., & Agoyi, M. (2021). A hybrid wormhole attack detection in mobile ad-hoc network (MANET). *IEEE Access*, *9*, 11872-11883. https://doi.org/10.1109/ACCESS.2021.3051491

Fotohi, R., & Jamali, S. (2014). A comprehensive study on defence against wormhole attack methods in mobile Ad hoc networks. *International journal of Computer Science & Network Solutions*, *2*(5), 37-56.

Meddeb, R., Triki, B., Jemili, F., & Korbaa, O. (2017, May). A survey of attacks in mobile ad hoc networks.

In *2017 international conference on engineering & MIS (ICEMIS)* (pp. 1-7). IEEE. 10.1109/ICEMIS.2017.8273007

Bhattacharyya, A., Banerjee, A., Bose, D., Saha, H. N., & Bhattacharya, D. (2011). Different types of attacks in Mobile ADHOC Network. *arXiv.* https://doi.org/10.48550/arXiv.1111.4090

Goyal, P., Batra, S., & Singh, A. (2010). A literature review of security attack in mobile ad-hoc networks. *International Journal of Computer Applications*, *9*(12), 11-15.

Hamdi, M. M., Audah, L., Abood, M. S., Rashid, S. A., Mustafa, A. S., Mahdi, H., & Al-Hiti, A. S. (2021). A review on various security attacks in vehicular ad hoc networks. *Bulletin of Electrical Engineering and Informatics*, *10*(5), 2627-2635. https://doi.org/10.11591/eei.v10i5.3127

Lilhore, U. K., Khalaf, O. I., Simaiya, S., Tavera Romero, C. A., Abdulsahib, G. M., & Kumar, D. (2022). A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks. *International Journal of Distributed Sensor Networks*, *18*(9), https://doi.org/10.1177/15501329221117118

Xue, X., Shanmugam, R., Palanisamy, S., Khalaf, O. I., Selvaraj, D., & Abdulsahib, G. M. (2023). A hybrid cross layer with harris-hawk-optimization-based efficient routing for wireless sensor networks. *Symmetry*, *15*(2), 438. https://doi.org/10.3390/sym15020438

Liu, Y., Wu, H., Rezaee, K., Khosravi, M. R., Khalaf, O. I., Khan, A. A., ... & Qi, L. (2022). Interaction-enhanced and time-aware graph convolutional network for successive point-of-interest recommendation in traveling enterprises. *IEEE Transactions on Industrial Informatics*, *19*(1), 635-643. https://doi.org/10.1109/TII.2022.3200067

Hassan, H. J., Abdulsaheb, G. M., & Khalaf, O. I. (2022). Design of QoS on data collection in wireless sensor network for automation process. *International Journal of Computer Applications in Technology, 68*(3), 298-304. . https://doi.org/10.1504/IJCAT.2022.10049756