Design Secure AODV Routing Protocol for MANETs using Group Signature and Onion Routing Cryptographic Algorithms

Selamawit Eshetu Mecha

A Thesis Submitted to the Department of Computer Science and Engineering

School of Electrical Engineering and Computing

Presented in Partial Fulfillment of the Requirement for the Degree of Master's in Computer Science and Engineering

Office of Graduate Studies

Adama Science and Technology University

September 2023

Adama, Ethiopia

Design Secure AODV Routing Protocol for MANETs using Group Signature and Onion Routing Cryptographic Algorithms

Selamawit Eshetu Mecha

Major advisor: Dr. Ketema Adere

A Thesis Submitted to the Department of Computer Science and Engineering
School of Electrical Engineering and Computing
Presented in Partial Fulfillment of the Requirement for the Degree of Master's in Computer Science and Engineering

Office of Graduate Studies
Adama Science and Technology University

September 2023
Adama, Ethiopia

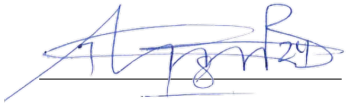
APPROVAL PAGE OF M.SC THESIS

We, the advisors of the thesis entitled *"Design Secure AODV Routing Protocol for MANETs using Group Signature and Onion Routing Cryptographic Algorithms"* and developed by Selamawit Eshetu Mecha, hereby certify that the recommendation and suggestions made by the board of examiners are appropriately incorporated into the final version of the thesis.

Major Advisor	Signature	Date
Co-advisor	Signature	Date

APPROVAL OF BOARD OF EXAMINERS

We, the undersigned, members of the Board of Examiner of the thesis by Selamawit Eshetu Mecha have read and evaluated the thesis entitled *"Design Secure AODV Routing Protocol for MANETs using Group Signature and Onion Routing Cryptographic Algorithms"* and examined the candidate during open defense. That is, therefore, to certify that the thesis is accepted for partial fulfillment of the requirement of the degree of Master of Science in Computer Science and Engineering.

Chairperson	Signature	Date
Internal Examiner	Signature	Date
Asrat Mulatu (Ph.D.)		27/10/2023
External Examiner	Signature	Date

Finally approval and acceptance of the thesis is contingent upon submission of its final copy to the Office of Postgraduate Studies (OPGS) through the Department Graduate Council (DGC) and School Graduate Committee (SGC).

Department Head	Signature	Date
School Dean	Signature	Date
Office of Postgraduate Studies, Dean	Signature	Date

DECLARATION

I hereby declare that this Master Thesis entitled *"Design Secure AODV Routing Protocol for MANETs using Group Signature and Onion Routing Cryptographic Algorithms"* is my original work. That is, it is not been submitted for the award of any academic degree, diploma or certificate in any other university. All sources of materials that are used for this thesis have been duly acknowledged through citation.

Name of Student	Signature	Date

RECOMMENDATION

We, the advisors of this, hereby certify that we have read the revised version of the thesis entitled *"Design Secure AODV Routing Protocol for MANETs using Group Signature and Onion Routing Cryptographic Algorithms"* prepared under our guidance by Selamawit Eshetu Mecha submitted in partial fulfillment of the requirement for the degree of Master's of Science in Computer Science and Engineering. Therefore, we recommend the submission of revised version of the thesis is to the department following the applicable procedures.

Major Advisor	Signature	Date
Co-advisor	Signature	Date

ACKNOWLEDGEMENT

First of all, I would like to thank the Almighty God and the Holy Virgin Mary those helped me in every situation .

Secondly, I would like to express my sincere gratitude to my advisor, Dr Ketema Adere for their important guidance and support during my thesis work. Their capability and encouragement helped me to complete this research.

I would like to thank you sincerely, My grandma. She helped me by praying, loving, financially, and advice to be successful.

I would like to thank My Mom for her kindness, love, and prayer.

I would also like to thank my friends especially Mr. Tinsae and Mrs. Merima for their advice and support.

Finally, I would like to thank all of the participants in my study for their time and willingness to share their experiences. This work would not have been possible without their contribution.

Table of Content

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

AODV	Ad-hoc on Demand Distance Vector
ACK	Acknowledge
CCA	Clear Channel Assessment
CGSR	Cluster-Based Routing Protocol
D	Destination
DLL	Data Link Layer
DO	Direct Observation
DR	Delivery Ratio
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing Protocol
EE	Energy-Efficient
FTP	File Transfer Protocol
IMANET	Internet-Based Mobile Ad-hoc Network
IOS	International Organization for Standardization
LAR	Location Aided Routing
LLC	Logical Link Layer
MAC	Medium Access Control
MANET	Mobile Ad-hoc Network
NAM	Network Animation
NRL	Normalized Routing Load
NS2	Network Simulator 2
NS3	Network Simulator 3
MATLAB	Mathematical laboratory
PDF	Packet Delivery Ratio
PLCP	Physical Layer Convergence Protocol

PMD	Physical Medium Dependent
PHY	Physical
PPM	Packet Purse Model
PTM	Packet Trade Model
OLSR	Optimized Link State Routing Protocol
OMNET++	Optical Micro-Networks Plus Plus
OR	Overhead Ratio
OSI	Open System Interconnected
OTCL	Object Oriented Tool Command Language
QoS	Quality of Service
PDR	Packet Delivery Ratio
S	Source
SN	Selfish Node
TCL	Tool Command Language
TTL	Time to Live
TORA	Temporally Ordered Routing Algorithm
Wifi	Wireless Fidelity
WSN	Wireless Sensor Network
VANET	Vehicular Ad-hoc Network
ZHLS	Zone-based Hierarchical Link State
ZRP	Zone Routing Protocol

ABSTRACT

A mobile Ad hoc network is infrastructure-less network where the nodes are mobile and can move at high speeds. This mobility allows nodes to easily join or leave the network. MANETs have a dynamic topology, making them susceptible to various types of security threats. The inherent randomness of these networks poses a significant challenge for ensuring their security. Attacks on MANETs can be categorized into two main types: active attacks, which involve modifying and disrupting network operations, and passive attacks, which do not disrupt network operations but focus on unauthorized data access or monitoring. Traffic analysis stands as a particularly covert and unresolved form of passive security threat in the context of MANETs. This type of attack involves eavesdropping on network traffic to deduce valuable information about the applications in use and the entities involved in the communication. Such gleaned information may encompass details like node identities, geographical locations, and the relationships between the communicating nodes. To protect an AODV route discovery, from traffic analysis different security mechanisms existed for secured communication for MANET, however, most of the study intensive on prevents Vulnerability of routing packet but not routing traffic. In this study to satisfy the requirements and to defend against the attacks a new routing protocol SAODV has been proposed to give confidentiality protecting traffic analysis and RREQ modification. This protocol uses a key-encrypted onion to record a discovered route and design an encrypted secret message and a Group signature is used to authenticate the RREQ packet one hop, to prevent the intermediate node from altering the directing packet. Extensive simulations are done to provide maximum throughput and minimized packet loss ratio. We use NS2 for our simulation experiments we use NS2 for our simulation experiments traffic network area is 1501m $\times$ 600m using 30 nodes. Finally, the route request packets are authenticated by group signatures, which can defend the potential active anonymous attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message is designed to not only record the anonymous routes but also prevent the intermediate nodes from inferring the real destination.

Keywords: Group signature, Onion routing, Encrypted,Throughput,Delay

CHAPTER ONE
1. INTRODUCTION

1.1 Background of the Study

Wireless networks have gained immense popularity due to their ability to support mobility, wireless connections, and widespread accessibility. They can be broadly classified into two primary types: Infrastructure networks and infrastructure-less, also known as ad hoc networks. Infrastructure networks rely on stationary base stations to furnish wireless connectivity to end-user devices. An illustrative example is cellular networks, where base stations establish wireless links with mobile users, providing them access to the underlying wired network infrastructure. On the other hand, infrastructure-less or ad hoc networks consist of individual systems known as nodes, which autonomously configure themselves to communicate with one another without depending on any fixed infrastructure. These nodes are mobile and can freely change their positions while collaborating to relay packets, facilitating multi-hop wireless communication among them. (Gupta, Verma, & Sambyal, 2018; R. Singh, 2018).

A Mobile Ad-hoc Network (MANET) is a type of ad hoc network that facilitates the transmission of data packets between two nodes without relying on any existing infrastructure. MANET possesses the unique ability to self-configure, self-organize, and reduce deployment expenses across a wide range of application domains. It adopts an approach to access various computing resources. One of the defining features of MANET is its dynamic topology, which encourages mobility. Nodes within a MANET have the freedom to move randomly within the network, leading to a constantly changing network structure that typically involves multi-hop communication. Moreover, nodes exhibit diverse movement patterns, varying in terms of speed and direction, and these movements occur at unpredictable intervals.In the MANET architecture, every node serves a dual role: it acts both as a router, responsible for routing packets on behalf of other nodes, and as a host, engaging in its communication activities. (Chitkara & Ahmad, 2014).

Figure 1.1: Mobil Ad hoc Network (Kaur et al., 2013).

High-speed node movement and the potential depletion of node batteries can lead to nodes either joining the network or some existing nodes leaving it. If a node that serves as a router departs, it can disrupt the route between the source and destination, necessitating the initiation of the route discovery process anew. Consequently, the primary goal of MANET routing protocols is to effectively manage multi-hop communication and swiftly identify the most suitable path. Routing protocols in MANETs are primarily designed to calculate the optimal routes from the source to the destination, primarily due to the high mobility of nodes. Therefore, there's a pressing need for protocols that can adapt to the frequent changes in network topology and the dynamic nature of wireless links in infrastructure-less networks. (Arnous, El-kenawy, & Saber, 2019)

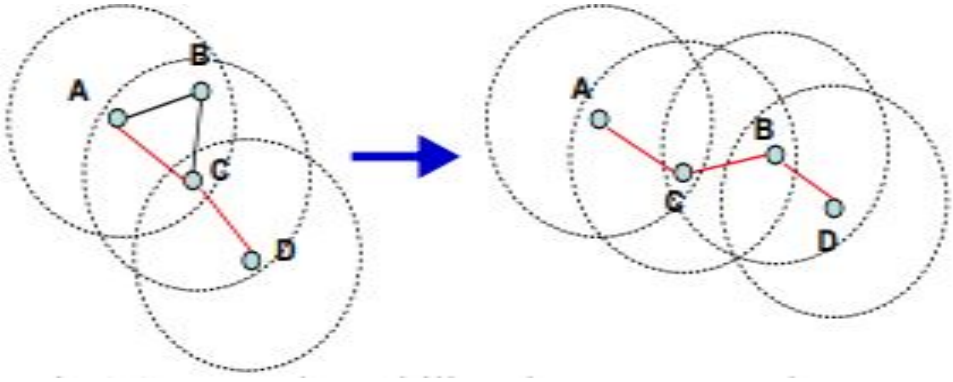


Figure 1.2: node mobility change (Aggarwal, 2013)

Therefore There's a necessity for protocols that can adjust to the frequent alterations in network topology and the dynamic nature of wireless link conditions in infrastructure-less networks. Ad hoc network routing protocols are broadly categorized into three main types: proactive (table-driven), reactive (on-demand), and hybrid (combining elements of both proactive and reactive protocols). In proactive protocols, nodes maintain a routing information table where routes are pre-established before they are needed. This approach enables quicker route discovery compared to reactive protocols, where routes are only created when they are specifically required. In contrast, hybrid protocols incorporate a blend of both reactive and proactive techniques, allowing for a more flexible approach to route management.(Chitkara & Ahmad, 2014)

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is a reactive approach specifically crafted for mobile ad hoc networks. In contrast to proactive protocols, AODV doesn't continuously maintain routing details for all nodes. Instead, it establishes routes only when they're required. AODV employs distance-vector algorithms, where nodes retain data solely about their immediate neighboring nodes as next hops and the associated costs for reaching known destinations. In situations where a node within AODV needs to transmit data to another node but lacks an existing route, it triggers a route discovery process to find a new path. This is achieved by transmitting Route Request (RREQ) messages across the network

until they reach a node that has a recent route to the destination or the destination node itself. The destination node or an intermediary node with an up-to-date route then replies with a Route Reply (RREP) message back to the source node. As the RREP travels in reverse, it establishes the forwarding path between the source and destination at each intermediate hop along the way. AODV also provides route maintenance functionality through Route Error (RERR) messages. These RERR messages are utilized by nodes to invalidate routes in cases where the links along those routes become disrupted. Such disruptions can occur due to factors like node mobility, elevated error rates, and so on. When a node experiences a loss of connection with a neighboring node, it transmits a RERR message to inform other nodes using routes that pass through the disconnected neighbor, indicating the unavailability of that route. The RERR message contains a list of destinations that can no longer be reached via the broken link. It's important to note that AODV was initially designed without security considerations and did not include mechanisms to detect malicious attacks (Maurya et al., 2012).

Our research primarily concentrates on devising a secure AODV routing protocol to prevent the tampering of routing messages as they are transmitted between nodes. This secure communication design serves the purpose of preventing the need for re-establishing the communication path, thereby conserving energy and reducing delays associated with rediscovering the transmission route.

1.2 MANET Vulnerabilities

Mobile ad hoc networks (MANETs) encounter heightened security threats in comparison to conventional wired networks. Their decentralized structure renders them more susceptible to malevolent activities. Due to the absence of centralized surveillance, identifying attacks and maintaining trust among nodes becomes a challenging endeavor. Additionally, the dynamic topology of MANETs, characterized by ever-shifting connections, presents its own set of difficulties. Security measures must exhibit scalability to accommodate networks of varying sizes, seamlessly adapting as nodes enter and exit the network's range. Moreover, MANET routing protocols operate under the assumption of node cooperation, leaving the network vulnerable to disruptions in cases where malicious nodes deviate from expected behaviors. Scarce resources such as battery power can tempt nodes to decline routing responsibilities, resulting in interruptions to network operations. Consequently, MANETs necessitate heightened scrutiny of security concerns and the implementation of self-organizing, adaptable security mechanisms to ensure robust protection in the face of the uncertainties inherent to a decentralized and mobile environment (U. K. Singh et al., 2011). These mechanisms are typically enumerated as follows..

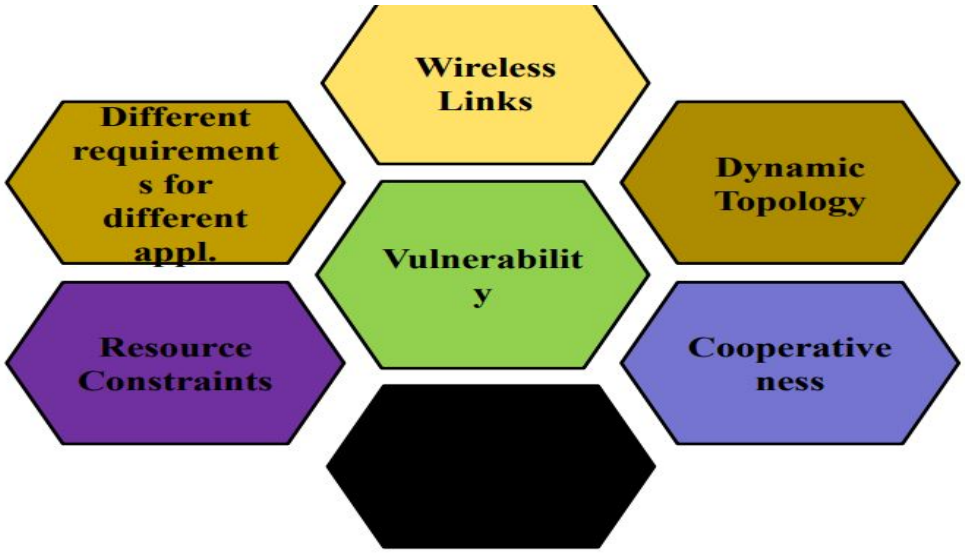


Figure 1.3: Vulnerability of MANET

Lack of centralized management: *In a MANET, the absence of a centralized monitoring server poses challenges in detecting attacks, mainly due to the complexity of monitoring traffic within a dynamic and expansive ad-hoc network. The absence of centralized management also hinders the establishment of trust among nodes.*

Resource availability: *A significant challenge in MANETs lies in ensuring secure communication within a constantly evolving environment, which necessitates the creation of diverse security strategies and structures to safeguard against specific threats and attacks. Furthermore, collaborative ad-hoc settings enable the deployment of self-organizing security mechanisms.*

Scalability:- *Because nodes in ad-hoc networks frequently move, the network's size is in constant flux, making scalability a significant security concern. Security measures must possess the capability to address both large and small networks effectively*

Cooperativeness:- *Typically, the routing algorithms used in MANETs operate under the assumption of node cooperation and non-malicious behavior. Consequently, a malicious attacker can exploit this assumption by posing as a critical routing agent, thereby disrupting network operations through protocol violations.*

Dynamic topology:- *The dynamic topology and the constantly shifting composition of nodes can disrupt the trust dynamics among nodes, especially when nodes are identified as compromised. To better safeguard against this dynamic behavior, distributed and adaptive security mechanisms are more suitable for maintaining trust and security within the network.*

Limited Resource:- *Certain nodes within MANETs choose not to relay received packets to conserve battery power and extend their longevity within the network.*

1.3 Motivation of the study

The Ad-hoc On-demand Distance Vector (AODV) routing protocol is designed for mobile ad hoc networks, encompassing a wide range of tens to thousands of mobile devices. AODV demonstrates effectiveness in scenarios with low, moderate, and high node mobility, accommodating varying data traffic volumes. However, it relies on the assumption that nodes trust each other and that the network is devoid of malicious intruders. AODV's design focuses on reducing control traffic overhead and eliminating data packet overhead to enhance scalability and efficiency. Although AODV incorporates mechanisms to prevent routing loops, its decentralized nature permits any node to engage in routing, potentially allowing malicious nodes to disrupt the network. (Molva & Michiardi, 2003).

Nevertheless, MANETs find applications in various domains such as disaster recovery, emergencies, and military battlegrounds, underscoring the critical importance of secure communication in MANETs, particularly in military contexts. Securing MANETs has been a significant challenge, given the numerous constraints imposed on the nodes within the network. The primary objective of this research is to examine and assess the repercussions of misbehaving nodes on the integrity, availability, and security of a network, particularly in the context of attacks involving the interception of routing traffic and the modification of packets during route discovery, notably through the alteration of RREQ messages. To enhance network security and performance, this study proposes the incorporation of both a group signature scheme and cryptographic key onion routing algorithms.

This study specifically investigates the influence of packet modification and the interception of routing traffic within the route discovery process of the AODV protocol. The simulations conducted as part of this thesis work aim to gauge the impact of misbehaving nodes on AODV protocol performance by utilizing network performance metrics like packet loss and throughput as evaluative measures

1.4 Statement of the problem

MANETs are more vulnerable to attacks than wired networks because of their weak physical security, node mobility, and lack of centralized administration. Furthermore, MANET protocols are usually not developed with security in mind and instead concentrate on lowering the routing-related overhead on nodes, allowing every node to participate in the routing process. This is obvious from the fact that MANET routing algorithms often presume that nodes are cooperative and are not malicious. As a result, a malicious attacker can quickly become an essential routing agent and disrupt network operations, by violating protocol standards. One potential security issue that can happen in the AODV protocol is that nodes may manipulate the RREQ messages forwarded by other nodes to disrupt the route discovery process.

Such packet alterations can be used to deceive the nodes involved in the routing process. (U. K. Singh et al., 2011)

Several researchers have examined the various preventative and detective security techniques that may be deployed to solve the problem of packet alterations and traffic analysis in MANET. However, these security techniques didn't fully satisfied the issue of route packet interruption and traffic interception. To address this issue, we present a method for developing a secure AODV routing protocol in a MANET with reduced routing overhead and transmission delay. We suggest combining Onion routing and the Group signature cryptographic technique to improve the security of transmitted packets and routing messages across the network.

1.5 Research Question

Based on the above problems this study aims to answer the following questions.

1. *How can we prevent routing packet from being modified and routing traffic analysis by using onion routing and Group signature algorithm ?*
2. *How the performance of the new AODV protocol can be evaluated based on the previous AODV protocol ?*

1.6 Objectives of the Study

1.6.1 General Objective

The general objective of this study is to design secure AODV protocol to enhance security in MANET routing.protocol

1.6.2 Specific Objectives

Specific objectives of the study are:

1. *To study the problem of routing traffic analysis and packet modification on the performance of AODV protocol*
2. *To investigate the group signature and onion routing cryptographic algorithms for authenticating the RREQ packet at every hop in order to prevent intermediary nodes from altering the routing packet and traffic.*
3. *To compare and evaluate the proposed algorithm with the existing.*

1.7 Methodology of the Study

To achieve the goals of this research, various approaches will be employed. Below is an overview of the planned methods.

Step 1. Identify the research area:- *Conduct a literature review to identify research areas and issues with AODV routing in MANETs.*

Step 2.Identify the research problem:- *Formulate a specific research problem based on the limitations of existing solutions..*

Step 3. Design Proposed Solution:- *Design a proposed solution by modifying AODV using onion routing and group signature algorithms. Describe the overall process and scenarios.*

Step 4. Simulating the proposed system using NS2:- *Simulate the proposed SAODV solution in NS2 to demonstrate improvements over standard AODV. Use C++ and TCL to modify AODV files. the performance of AODV. Then, C++ and OTCL programming languages modify the existing file for the proposed solution.*

Step 5.Reporting, evaluating, and discussing the result:- *Evaluate the performance of SAODV vs AODV using metrics like packet delivery ratio, throughput, end-to-end delay, and packet loss ratio. Discuss research outcomes based on simulation results.*

The proposed method's performance is evaluated using the following:

1. *Packet Delivery Ratio(PDR) Ratio of packets received to packets sent. Measure's reliability.*
   PDR=Packet received/packet sent
2. *Throughput Rate of successful packets delivered per unit time. Measures effectiveness.*
3. *Packet Loss Ratio Ratio of packets lost to total packets sent. Measure's reliability.*

To simulate different hardware and software tools are used Software

1. *Operating system: Ubuntu*
2. *Simulation tools: NS2.*
3. *Programming language: C++ and OTCL*
4. *TEXstudio*

Hardware

1. *RAM: 8GB*
2. *OS: 64-bit*
3. *Storage: Hard Drive (HDD) The key performance metrics are PDR, throughput, and packet loss ratio. The simulation will be done in NS2 on an Ubuntu system using C++ and OTCL. Hardware includes sufficient RAM, 64-bit OS, and HDD storage.*

1.7.1 Result Assessment

The simulation results were obtained and reached the objective of the study and answer the research question based on the following procedure and techniques were followed.

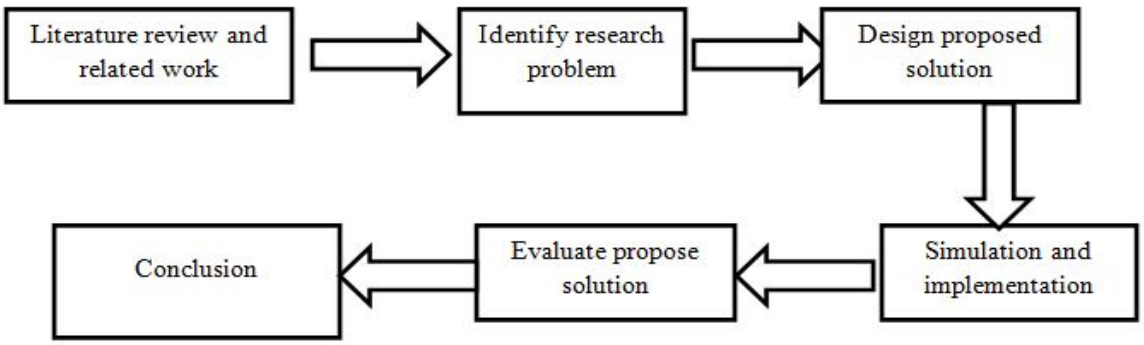


Figure 1.4: Research Methodology

1.8 Delimitation Scope

1.8.1 Scope of the Study

TThis thesis focuses on improving the security of the route discovery process in the AODV routing protocol for mobile ad hoc networks (MANETs). Specifically, it aims to prevent and detect alteration of RREQ packets and interception of routing traffic by malicious nodes. The proposed solution seeks to conceal the real destination during route discovery. It utilizes two key algorithms - encrypted onion routing and group signatures. Encrypted onion routing is used to record discovered routes and create encrypted messages to verify linkage between RREQ and RREP packets, preventing intermediate nodes from knowing the real destination since not all nodes are trustworthy. Group signatures are used to authenticate RREQ packets at each hop, preventing modification of routing packets by intermediates. The newly proposed SAODV mechanism enhances standard AODV by protecting against potential active and passive attacks without revealing node identities. It provides higher throughput, lower packet loss, and better resilience against adversarial attacks in mobile scenarios. Overall, the thesis focuses on improving secure communications through enhanced route discovery in AODV for MANETs.

1.8.2 Limitation

MANET is a broad research topic, due to resource and time constraints this study focuses only secure route discovery process on forwarding RREQ the study did not include another type of message in AODV, and again Other types of protocol were not considered in this thesis, and it did not address various MANET issues and energy efficiency. As was already established, only the RREQ and routing traffic interception were overcome by this investigation. It intends to improve AODV performance through the use of secure communication. and also The simulation isn't deployed in real-world scenarios.

1.9 Results of the Study

This study aimed to increase the AODV protocol's effectiveness and security in MANET. Reducing packet loss, and raising packet delivery ratio were used to address other performance issues to apply security methods to current routing performance. The current version of AODV lacks any security controls that prevent network communication from selfish and malicious nodes. The recommended course of action was to protect each neighboring node's traffic routing security. The method can apply Integrity and confidentiality utilizing an onion encryption method in addition to performing authentication using a group signature.

The result of this study is listed below

1. *To develop security and anonymity AODV in MANET*
2. *To protect the privacy of routing traffic*
3. *The best Performance of the AODV protocol was attained*

1.10 Thesis organization

The thesis is organized into five chapters progressing from introduction to proposed solution to experimentation to conclusions.

Chapter 1:- *Introduces the research, including the problem statement, motivation, objectives, methodology, scope, and limitations.*

Chapter 2:- *Reviews relevant literature and related work to provide background on the research area and problem being addressed.*

Chapter 3:- *Explains the proposed SAODV mechanism in detail, covering its working principles and architecture.*

Chapter 4:-*Presents the simulation analysis and results evaluation.*

Chapter 5:-*Concludes the thesis, summarizing key points and providing recommendations for future work in this research area*

CHAPTER TWO
2. LITERATURE REVIEW AND RELATED WORK

2.1 OSI Model and AD HOC Wireless Networks

In the early 1980s, the International Organization for Standardization (ISO) introduced the Open Systems Interconnection (OSI) reference model to enable communication between multi-vendor computer systems. The OSI model provides a modular framework for networking by dividing functions into hierarchical layers containing sub-functions. OSI consists of seven layers ranging from the physical layer to the application layer.Li, Li, Cui, ZhangLi et al..

The OSI model separates network functions into two categories:

1. *End-to-end data transmission.*
2. *Hierarchical layers with sub-functions*

Though developed decades ago, OSI remains a reference model used to define and relate different levels of networking protocols.

In mobile ad hoc networks (MANETs), communication mechanisms involve protocols operating in the lower three layers of the OSI model (layers 1-3). The upper layers are only active on the source and destination nodes. The OSI model provides a basis for designing and standardizing protocols for MANETs(Briscoe, 2000).

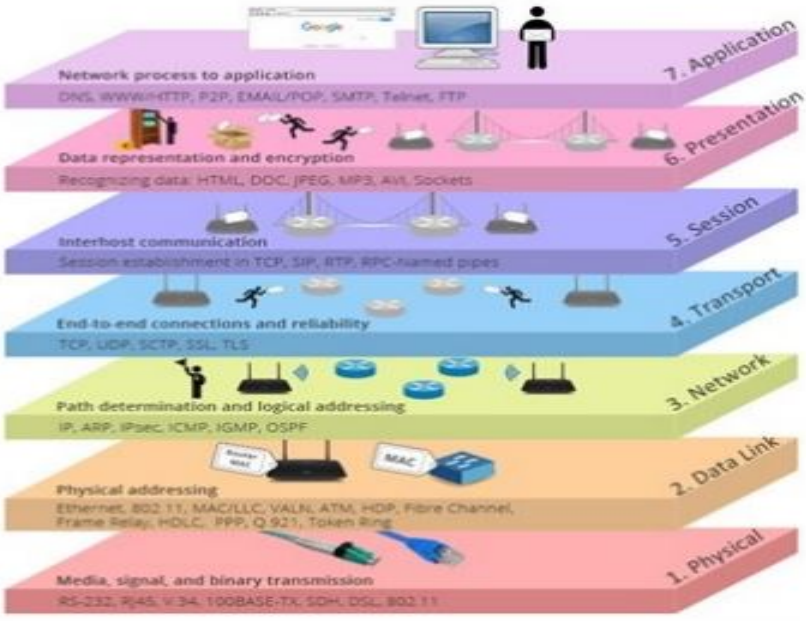


Figure 2.1: OSI seven-layer model (Mahmood et al., 2020)

2.1.1 The Physical Layer Structure

The physical (PHY) layer acts as an interface between the medium access control (MAC) sublayer and the wireless medium, enabling transmission and reception of frames. The PHY layer provides channel sensing mechanisms called clear channel assessment (CCA) to indicate to the MAC sublayer when a signal is detected or the channel is free. As shown in Figure 2.2, the PHY layer contains two sublayers: Physical Layer Convergence Protocol (PLCP) sublayer - Responsible for reporting channel status from the PHY to the MAC sublayer. Physical Medium Dependent (PMD) sublayer - Handles signal encoding, decoding, and modulation procedures (Briscoe, 2000).

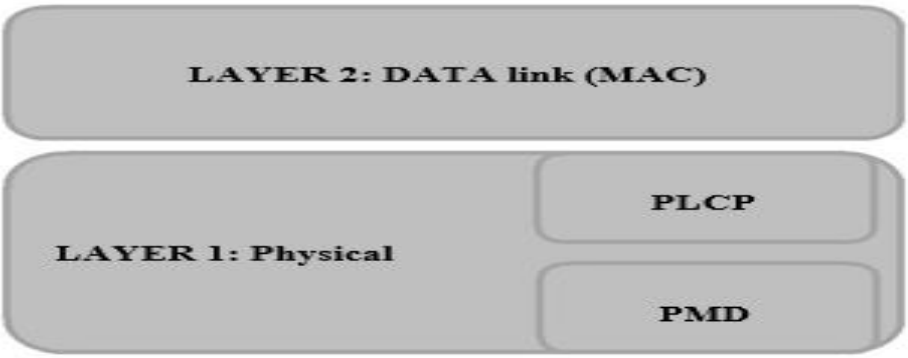


Figure 2.2: Physical Layer Structure (Briscoe, 2000)

2.1.2 The Data Link Layer

The data link layer (DLL) executes multiple important operations such as flow control, error control, addressing, and communication with medium access control. The DLL has two sub-layers(Mahmood et al., 2020).

1. *The medium access control sub-layer is responsible for addressing, framing, and medium access control.*
2. *The logical link control sub-layer (LLC), takes care of error control and flow control.*

The data link layer (DLL) performs crucial functions like flow control, error control, addressing, and interfacing with the medium access control. The DLL contains two sublayers: The medium access control (MAC) sublayer handles addressing, framing, and medium access control. The logical link control (LLC) sublayer manages error control and flow control. In MANETs, nodes share a common channel so collisions can occur when multiple nodes transmit simultaneously. The MAC sublayer controls access to the shared channel among MANET nodes. A key challenge is the hidden node problem: When a hidden node transmits while a visible node is also transmitting to the same receiver, collision occurs at the receiver. For example, in Figure 2.3, when A transmits to B, hidden nodes C and D are unaware of this transmission. If C and D also transmit to B, collision occurs at B. The MAC sublayer must manage this hidden node issue in the shared MANET channel (Jayasuriya, Perreau, Dadej,

Gordon, et al., 2004).

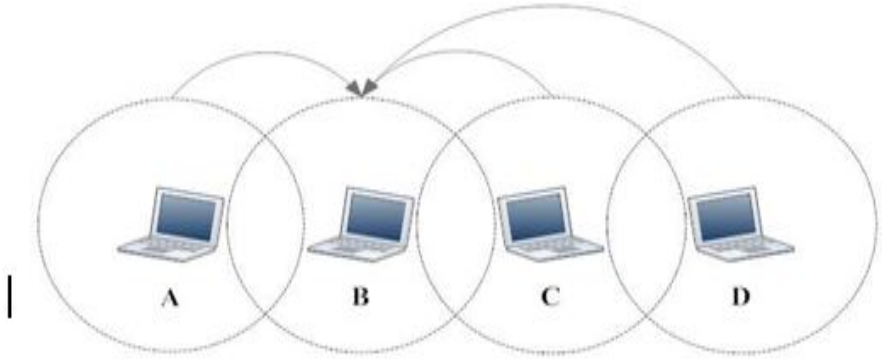


Figure 2.3: A hidden terminal problem in a MANET(Jayasuriya et al., 2004)

Many MAC protocols have been proposed to minimize the hidden terminal problem through collision avoidance. Many employs sender-initiated channel reservation using control frames before data transmission. This informs nearby nodes that the channel will be occupied for a duration. For example, if node A wants to transmit to B, it first broadcasts a request-to-send (RTS) frame with the data length and B's address. Node B responds with a clear-to-send (CTS) frame containing the data length for A. Nodes overhearing either frame remain silent during the transmission period, called virtual carrier sense. However, overheard RTS/CTS frames can prevent other non-interfering transmissions, called the exposed terminal problem, reducing channel efficiency. For instance, in Figure 2.4, communication between A and B inhibits D from transmitting to C (Wang, Wu, & Hamdi, 2012).

One solution is using directional smart antennas, where RTS, CTS, and data frames are transmitted only toward intended recipients. Smart antennas employ beamforming to dynamically adjust direction and bandwidth - listening with large bandwidth and transmitting narrowly focused. This alleviates the exposed terminal problem and improves spatial reuse (Figure 2.3). Some devices employ smart antennas which allow them to use beamforming techniques to change the bandwidth and direction of transmission or reception. This allows the device to use large bandwidth to listen and, small bandwidth to transmit.

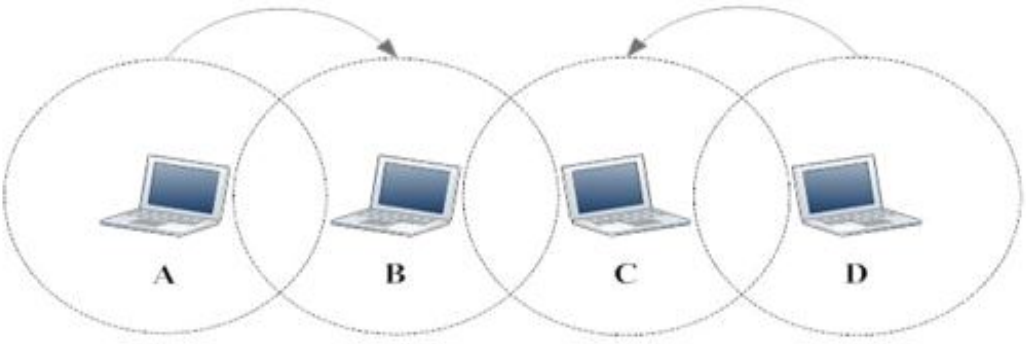


Figure 2.4: An exposed terminal problem in a MANET (Jayasuriya et al., 2004)

2.1.3 The Network Layer

The network layer provides end-to-end transmission services including routing information exchange, path discovery, link repair, and efficient bandwidth utilization. However, mobility in MANETs can cause issues like route breaks, packet collisions, routing loops, stale routes, and difficulty with resource reservation. Using routing protocols with low overhead can mitigate these issues given MANET constraints on battery lifetime and bandwidth. Overhead should be minimized by reducing routing control packets for route discovery and maintenance. Control packet overhead is problematic because of the low bandwidth, potentially causing data packet collisions. Therefore, developing routing protocols that use a small number of control packets is desirable for MANETs. The network layer and routing protocols need to be efficient to provide reliable end-to-end transmission despite mobility, while operating within the limited bandwidth and power of MANET nodes

The above problems may be reduced with the use of a suitable routing protocol with a low communication overhead. In MANETs because of the limitation of available battery lifetime and bandwidth, the use of a routing protocol with a low communication overhead is important. To reduce overhead, the routing control packets for discovering a new route or maintaining existing routes should be reduced. The control packets, due to the use of low bandwidth, cause data packet collision. Consequently, it is desirable to develop a routing protocol that uses only a small number of routing control packets (Sullivan, Brighente, Kumar, & Conti, 2021).

2.1.4 The Transport Layer

The objectives of the transport layer protocols are:

1. *Establishing and maintaining end-to-end connections;*
2. *Reliable end-to-end data delivery;*
3. *Flow control;*
4. *Congestion control*

The two main transport layer protocols are:

Transmission Control Protocol (TCP) - Provides reliable data transmission/reception. Suitable for applications like file transfer and email that need guaranteed delivery rather than speed. TCP can cause delays due to waiting for lost packets or retransmissions.

User Datagram Protocol (UDP) - Enables nodes to transmit/receive short messages called datagrams. Does not ensure reliable delivery like TCP. Packets may arrive out-of-order, duplicated, or lost without notification. Avoids overhead of TCP, making UDP faster for applications like broadcasting and video streaming that do not require guaranteed delivery.

2.2 Network Overview

A network refers to any collection of interconnected devices/computers using communication channels to share resources and information. There are two main network types (Ochola & Eloff, 2011).

Wired Network: : *Devices are connected via cables. The wires act as communication medium to transfer information across different points in the network.*

Wireless Network: : *Devices connect to the network wirelessly without cables. Wireless networks have two categories*

- *Infrastructure Network: Wireless devices connect to wired network infrastructure via access points*
- *Infrastructure-less Network: Wireless devices communicate directly without wired infrastructure. Also called ad-hoc network.*

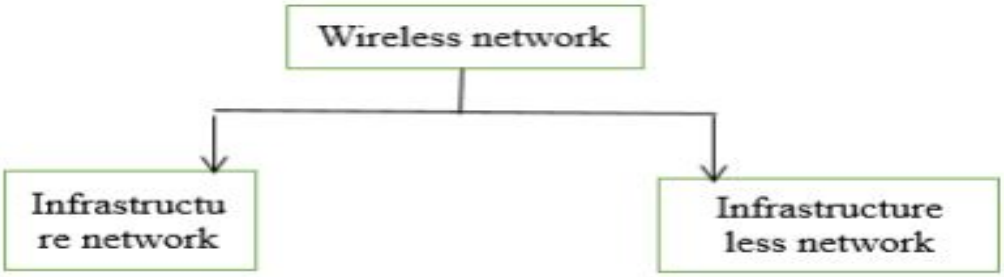


Figure 2.5: Wireless Networks Categories

Infrastructure network

These networks typically feature an access point or a centralized base station, which falls within the category of infrastructure networks. In such networks, each node is connected to a central base station, and these base stations are stationary. Communication among nodes relies on the presence of these base stations within their respective coverage areas. When a node moves beyond the range of one base station, another base station takes over the responsibility of providing communication services to the mobile nodes. (Fazeldehkordi, Amiri, & Akanbi, 2015).

Figure 2.6: Infrastructure Network (Gupta et al., 2018)

Infrastructure-less (Ad hoc Network)

Ad hoc networks are infrastructure-less networks that have no fixed base stations. Nodes are mobile and can move while communicating. All nodes participate in routing by forwarding data dynamically based on network connectivity (Kale, Gupta, & Prmit, 2013).

Key features of ad-hoc networks

- *Form temporary, decentralized networks*
- *No central infrastructure like base stations or access points*
- *Nodes are portable*
- *All nodes play equal roles*
- *No pre-defined routers or gateways*
- *Nodes act as both hosts and routers*
- *Routing is performed dynamically based on current topology*

Figure 2.7: Infrastructural-less network(Gupta et al., 2018)

Advantages of Ad hoc Network

- *They offer access to information and services irrespective of physical location.*
- *Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.*
- *Can be implemented with minimal costs and in a short time*

- *The network can be expanded to locations where wiring is not achievable*

2.3 Types of Ad hoc Networks

Vehicular Ad hoc Network (VANET)

Vehicular Ad hoc Networks (VANETs) are a subset of ad-hoc networks where vehicles are treated as individual nodes. VANETs equip these vehicular nodes with wireless communication devices and integrate them into an Intelligent Transportation System (ITS). VANETs have emerged as a valuable technology with significant contributions to road safety, enabling intelligent traffic management systems, facilitating high-speed data exchange among vehicles, and offering entertainment services. However, VANETs possess distinctive traits such as rapid topology changes and unpredictable variations in traffic node density, which can disrupt data transmission and pose challenges. The primary objective of VANETs is to empower vehicles to establish and sustain a communication network among themselves without the need for a central base station or access point (Raya & Hubaux, 2007).

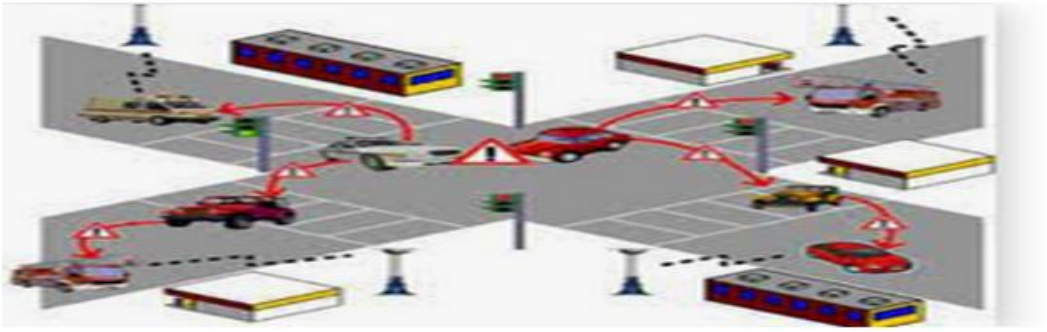


Figure 2.8: Network Architecture in VANET (Raya & Hubaux, 2007)

Wireless Sensor Network (WSN)

Wireless Sensor is comprised of a group of sensor nodes that are densely positioned within or in close proximity to the area of interest. These sensor nodes collaborate to observe and transmit data to a central base station, typically situated at a considerable distance from the monitored area. Sensor networks find diverse applications in fields like military, industry, and healthcare.

2.4 Mobile Ad Hoc Networks (MANETs)

MANETs were first proposed in 1970 it is a type of Ad hoc Network Mobile Ad Hoc Networks (MANETs) were initially introduced in 1970 and are a subset of Ad hoc Networks(Srivastava, Mishra, Upadhyay, & kumar Yadav, 2014).MANETs are comprised of "mobile nodes" that have the freedom to move freely and unpredictably within the network. These nodes are interconnected through Wireless LAN technology, and each node functions as both a router

and a host. It's important to note that MANET nodes rely on battery power. MANETs are characterized by their self-configuring and self-managing nature, forming a network system that does not rely on a fixed infrastructure or centralized administration.Due to the mobility of wireless hosts, each host in a MANET must possess the capability to act autonomously, including performing routing functions, without the need for a pre-established infrastructure or central control. Mobile hosts can move without constraints and can power on or off without prior notification to other hosts. This mobility and autonomy introduce dynamic network topologies, not only because end hosts are transient but also because intermediate hosts along a communication path are transient as well. The transmission range of nodes in a MANET is limited, which means that direct communication between a source and destination is not always possible when they are beyond each other's transmission zones. In such cases, intermediate nodes play a crucial role in facilitating communication. Therefore, communication in a MANET is categorized into two types: "Single Hop Communication," where nodes within each other's radio range communicate directly, and "Multiple Hop Communication," where intermediate nodes assist in relaying messages to their destinations when the destination node is outside the radio range of the source node.

2.4.1 Mobile Ad hoc Network Characteristics

Mobile Ad Hoc Network (MANET) is a network that configures itself, consisting of mobile routers connected by wireless links without the presence of access points. In MANETs, each node serves the dual role of being a router and a host. When communication is required between a source node and a destination node that are out of each other's direct transmission range, other nodes in the network collaborate to facilitate this communication (Kumar & Mishra, 2012).

Distributed operation: *Unlike networks with a centralized administrator, MANETs rely on decentralized control. Network management and control are distributed across the participating nodes. These nodes collaborate and communicate with each other, with each node taking on the role of a relay when necessary to fulfill specific network functions.*

Multi-hop routing: *In scenarios where data packets need to travel from a source to a destination that is beyond their direct wireless transmission range, the packets are relayed through one or more intermediate nodes. This multi-hop routing allows data to traverse the network through a series of interconnected nodes until it reaches its intended destination..*

Dynamic topologies: *In MANETs nodes can move randomly, and the network topology can change frequently and unpredictably.*

Mobility: *Nodes in MANET move freely while carrying information.*

Energy Constrained Operation: *all All the nodes in MANETS depend on battery power. They have less memory, power, and lightweight features. Hence it can move everywhere.*

Limited Security: *The Absence of any central administration mechanism and shared wireless medium make MANET more vulnerable.*

2.4.2 Application of MANET

Mobile Ad hoc Networks (MANETs) are a type of network that operates without a fixed infrastructure. They hold significant value, especially in situations where establishing conventional wired networks is cost-prohibitive or impractical, such as in battlefield scenarios, disaster recovery operations, and emergency services. The versatility of MANETs makes them suitable for use in various environments and at any time, enabling users to access and share information regardless of their geographical location. In MANETs, all nodes are mobile, and their connections are fluid, with no need for centralized administration. This inherent decentralization grants the network significant flexibility, enhancing its adaptability and flexibility. (Ahmed & Khalifa, 2017).

Military Sector: *MANETs offer the military the opportunity to utilize readily available network technology for establishing an information network that connects soldiers with military headquarters. The foundational principles of ad hoc networks were initially derived from this field.*

Commercial Sector : *In disaster relief scenarios, such as during fires, floods, or earthquakes, MANETs find valuable applications. They enable communication between different emergency response teams, facilitating coordination and information exchange.*

Smart Agriculture : *Enables the sharing of crucial information like water data, topography, aspect, and climate change details with remote users.*

Figure 2.9: MANET Application (Ahmed & Khalifa, 2017)

2.4.3 Routing

Routing involves transferring data from a source to a destination. When the destination is within the transmission range, direct communication occurs between nodes. However, if the destination is beyond this range, various metrics are employed as standard measurements to determine the optimal routing path for the packets to reach their intended destination. Routing aims to determine the best path to reach a destination (Yadav & Uparosiya, 2014).In the

context of ad hoc networks, several strategies have been proposed for efficient routing. However, due to the dynamic and ever-changing network topology, a straightforward approach might involve the sender specifying the exact route for a message from sender to recipient. Yet, this assumes that the sender possesses knowledge of the entire network topology, which is often an impractical assumption. An alternative approach is to transmit the message to a nearby neighbor in proximity to the intended recipient. This neighbor can then similarly make routing decisions(Chang, Gaydadjiev, & Vassiliadis, 2005).

2.4.4 Desirable properties of an efficient routing protocol

Numerous routing protocols have been suggested for ad hoc networks, each offering its unique advantages compared to earlier methods. However, there are several shared and desirable characteristics that any routing protocol designed for an ad hoc network should ideally exhibit, as outlined in the study by (Habib, Saleem, & Saqib, 2013). These are:

Loop free: *For a routing protocol, preventing the presence of loops in the path from the source to the destination is of utmost importance. Loops can result in inefficient routing, causing packets to circulate endlessly in the network without ever reaching their intended destination.*

Distributed control *Centralized routing schemes, where a single node holds all topological data and makes all routing decisions, lack robustness and scalability. They can be susceptible to single points of failure and might lead to network congestion around the central router due to routing queries and responses.*

Fast routing:- *Appropriate routing decisions play a vital role in accelerating the packet's journey to its destinations. Swift decisions enhance the chances that packets will traverse the selected route before it's affected by the mobility of nodes.*

Localized reaction to topological changes:- *Routing protocols should exhibit minimal responsiveness to topological changes occurring in one network section. This ensures that routing updates do not generate excessive overhead and maintains the scalability of the algorithm.*

A multiplicity of routes *In cases where node mobility disrupts certain routes, it is essential to have alternative paths available for packet delivery to sustain network connectivity.*

Power efficient *Efficient distribution of network load by routing protocols is crucial to prevent partitioned topologies caused by inactive nodes. Such partitioning can result in inaccessible routes, making load distribution a key factor.*

Secure *A routing protocol should emphasize security by offering authentication for communicating nodes, non-repudiation, and encryption. These measures help prevent routing deception and ensure the privacy of the network*

QoS aware *Being aware of Quality of Service (QoS) is vital, as the routing protocol should*

possess information about factors such as delay and throughput specific to source-destination pairs. Additionally, it should be able to validate its reliability, enabling real-time applications to depend on it for communication.

2.4.5 Quantitative Performance Metrics of MANET Routing Protocols

Performance metrics for Mobile Ad Hoc Network (MANET) routing protocols are quantitatively assessed, as outlined in the study by Ochola and Eloff (2011). These metrics include (Ochola & Eloff, 2011).

1 Packet Delivery Ratio(PDR)

It is calculated as the total number of packets successfully received at their intended destination divided by the total number of packets generated and sent in the network

PDR = (Packets Received) / (Packets Sent)

2 Normalized Routing Load (NRL)

NRL represents the ratio of control packets propagated by each node in the network to the number of data packets received by the destination nodes.

3 End –to-End Delay

This metric measures the average delay time experienced by all successfully delivered packets as they traverse the network.

4 Throughput

Throughput quantifies the total number of data packets that have successfully reached their intended destination. It is typically expressed in terms of bytes, and it is determined by multiplying the total number of packets by the maximum packet size to calculate the total number of data bits that have reached the destination.

2.4.6 Routing Protocols in MANET

A Mobile Ad Hoc Network (MANET) is characterized as a self-configuring network of mobile routers linked through wireless connections, without the presence of access points. The nodes within the network have the capability to move arbitrarily, leading to a dynamic and unpredictable network topology that poses challenges for efficient packet routing. The routing protocol plays a crucial role in managing data flow within the network and determining the most efficient path to reach the destination. Routing protocols in MANETs are typically categorized into three main types: proactive, reactive, and hybrid(Yadav & Uparosiya, 2014).

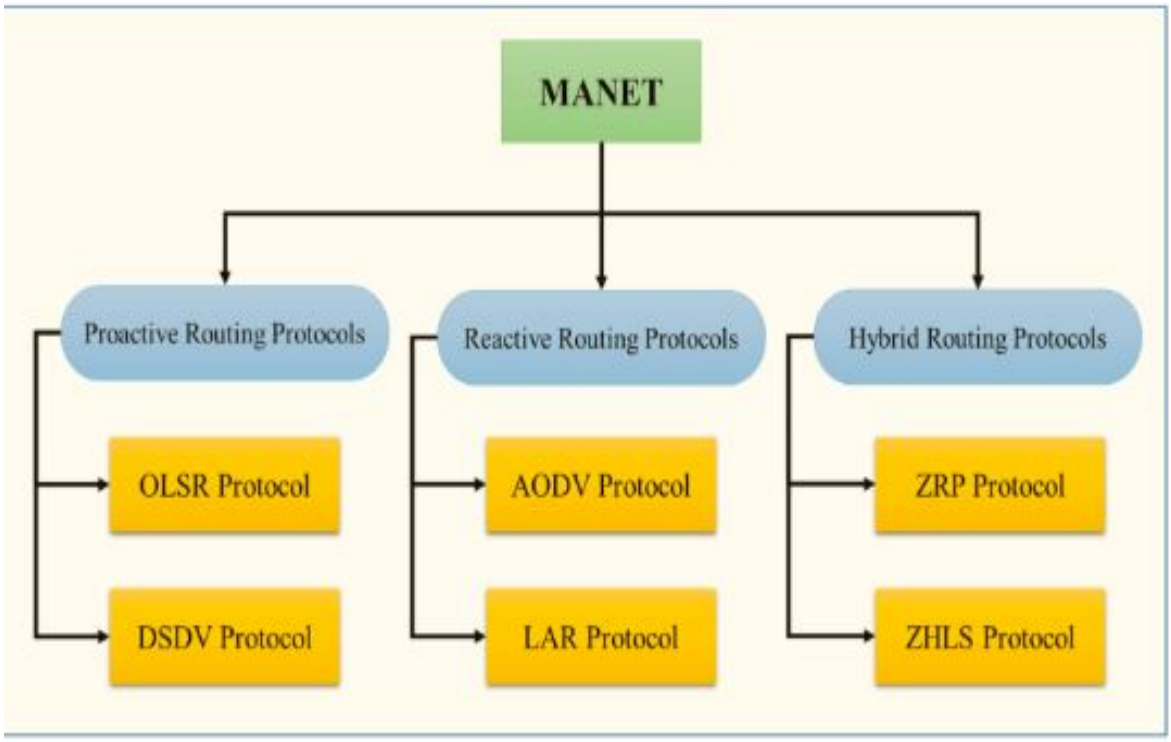


Figure 2.10: MANET Routing Protocol

Proactive protocols (Table-driven) *also known as table-driven routing protocols, operate by equipping each node within the network with a routing table that facilitates connections to other nodes. In this type of network, every node maintains information in the form of tables, and any changes in the network's topology necessitate updates to these routing tables. The information in these tables is continually updated proactively, ensuring that each node in the network possesses an up-to-date view of the network's current structure. Proactive protocols are well-suited for networks with a relatively small number of nodes as they require constant updates to node entries within the routing tables. However, this frequent updating results in increased routing overhead, leading to higher bandwidth and energy consumption within the routing table. On the positive side, proactive routing protocols provide immediate availability of the path to the destination without any delay in route discovery. Examples of proactive routing protocols include DSDV and OLSR. (Venkatesan, Rajakumar, & Pitchaikkannu, 2014).*

Reactive protocols(On-demand) *Reactive protocols, also known as on-demand routing protocols, function by establishing routes from a source node to a destination node only when there is a need for communication between two nodes. These protocols are initiated when a source node intends to send data packets to a specific destination node. One of the primary advantages of employing reactive routing protocols is their efficiency in terms of routing overhead, which is comparatively low. Examples of reactive routing protocols include DSR and AODV.*

2.4.7 AODV Protocol

AODV, which stands for Ad Hoc On-Demand Distance Vector, is a routing algorithm developed by Charles E. Perkins and Elizabeth M. Royer(Azza & Hacene, 2017).It falls into the category of reactive or on-demand routing protocols. Unlike protocols that maintain all network routes, AODV focuses on efficiently establishing or discovering routes when needed, minimizing control overhead in node communication. Routes are maintained only as long as they are required for communication between nodes. The route is maintained between two nodes as long as it is needed. AODV ensures loop-free routing by employing destination sequence numbers, generated by the destination node itself. It utilizes routing tables to store crucial routing information, including destination IP addresses, next-hop IP addresses, destination sequence numbers, active neighbors for the route, and the route's expiration time. AODV supports both unicast and multicast packet transmissions.The route discovery process in AODV is initiated through Route Request (RREQ) and Route Reply (RREP) messages. When a route needs to be established, the network is flooded with RREQ packets. As RREQ propagates through the network, nodes store routing information about the source, destination, and the previous and next hops through which they received the RREQ. This information is later used to create the reverse path back to the source node. Once an intermediate node is reached by RREQ and has information about the destination or the route itself, it responds to the source with a data packet (RREP). This data packet is routed back via the reverse path established by RREQ, effectively setting up the route from source to destination (Maurya et al., 2012).

Route Discovery

When a node within the network intends to send data packets to another node, it first checks its routing table for an existing path to the destination. If such a path exists, the data packet is transmitted to the destination through this established route, with each hop handled by the appropriate intermediate node. However, if no route exists between the source and destination, the route discovery procedure is initiated, starting with the generation of Route Request (RREQ) and Route Reply (RREP) messages)(RREP) (Patel, Patel, Kothadiya, Jethwa, & Jhaveri, 2014).

***Route Request Message (RREQ):** The RREQ packet includes essential information such as the source node's address, source sequence number, destination node's address, destination sequence number, and a broadcast ID. When a node receives the RREQ packet, it establishes a reverse path in its routing table, pointing back to the node from which it received the RREQ packet.*

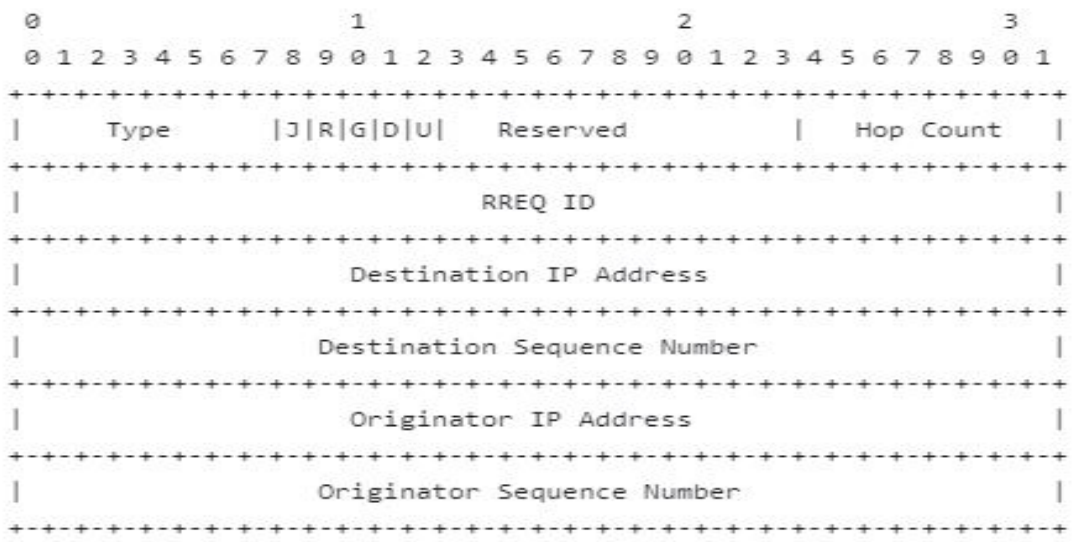


Figure 2.11: RREQ Message Format

The reverse route consists of essential components, which encompass the source's IP address, the source node's sequence number, the hop count to the source, the IP address of the node that received the Route Request (RREQ), and a lifetime field. Maintaining this reverse route primarily serves the purpose of enabling the transmission of a Route Reply (RREP) packet back to the source nodeOnce the Route Request (RREQ) packet reaches the destination node and its IP address aligns with the destination's IP address, the destination node reacts by transmitting a Route Reply (RREP) packet to the source node. This RREP packet is relayed through the reverse path, employing unicast transmission (Patel et al., 2014).

Route Reply Message (RREP): *The Route Reply (RREP) packet responds to the Route Request packet sent from the source end.*

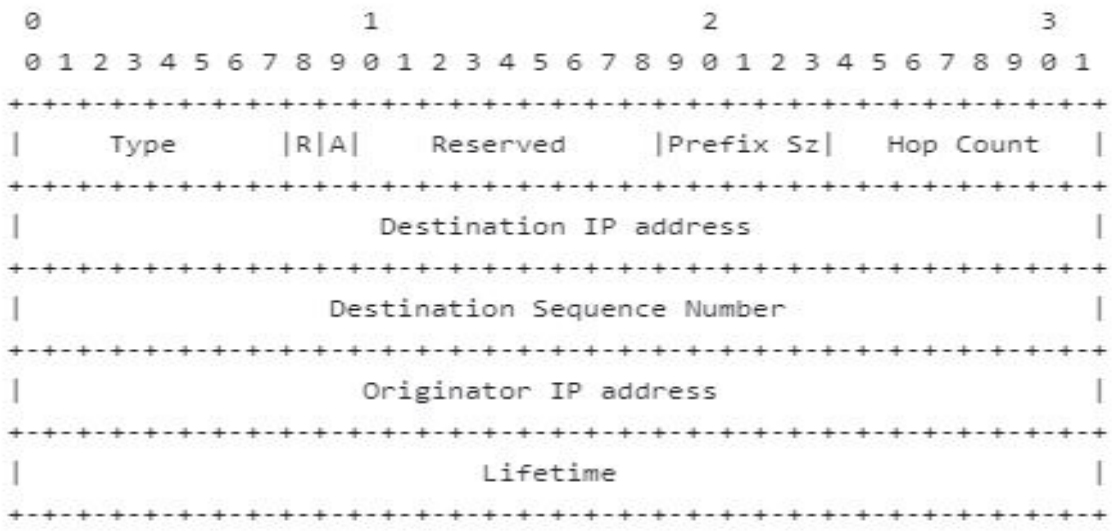


Figure 2.12: RREP Message Format

When a node possesses an exact route to the specified destination, it responds to the Route Request packet (RREQ) by transmitting the Route Reply packet (RREP). This is carried out

to ensure that the source node is aware of the route for sending its packets to the destination; thereby avoiding unnecessary time spent searching for alternative routes. This packet will include fields such as the source address, destination address, destination sequence number, hop count, and lifetime.

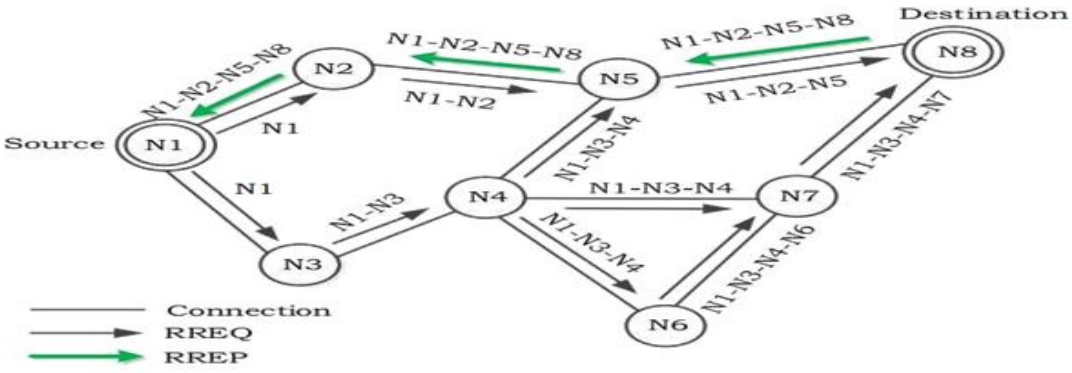


Figure 2.13: Route Discovery Mechanism (Srivastava et al., 2014)

Route Maintenance

Throughout the packet transmission process, all nodes remain active and continuously monitor their neighboring nodes. This monitoring is essential to determine the status of nearby nodes and ensure their activity. However, it's important to note that not all nodes in the network may perform optimally, and there can be instances where a node fails to function correctly. In the case of AODV, if any node within an active route experience a failure, the protocol generates a Route Error Message (RERR). The RERR message serves a crucial role in identifying nodes that are not actively participating in the routing process. Its primary purpose is to notify neighboring nodes about the occurrence of a link failure(Rukhande & Shete, 2015).

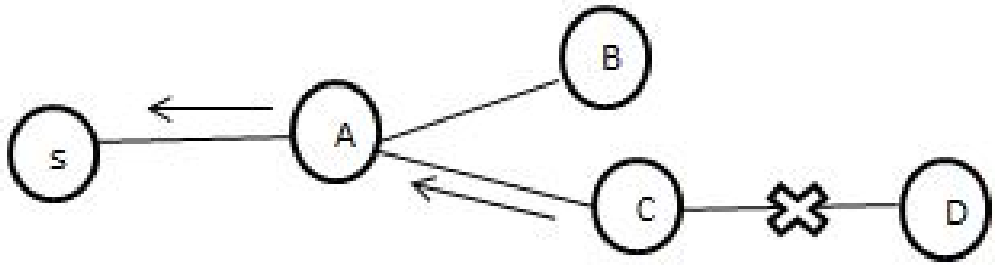


Figure 2.14: Route Error (RERR)

2.4.8 Hybrid Routing Protocols

Hybrid routing protocols are a fusion of both reactive and proactive routing protocols. The primary objective of these protocols is to mitigate the control overhead associated with proactive routing approaches while simultaneously reducing the latency introduced by route

discovery in reactive routing protocols. Hybrid routing protocols harness the benefits of both proactive and reactive strategies. One instance of a hybrid routing protocol is the Zone Routing Protocol (ZRP)(Shivahare, Wahi, & Shivhare, 2012).

2.4.9 Security Attacks in Ad-Hoc Network

Security is a major concern in Mobile Ad-Hoc Networks (MANETs) due to the absence of a central governing body to oversee the numerous nodes operating within the network. The network can be vulnerable to attacks initiated by nodes that are not legitimate members of the network and are attempting to gain unauthorized access. These nodes are commonly referred to as "outsiders." To safeguard the network against such malicious outsiders, cryptographic techniques are commonly employed. These techniques enable nodes to securely validate the identity of other nodes, thereby mitigating potential harm caused by unauthorized intruders.Additionally, the network must also consider threats from nodes that are legitimately authorized to be part of the network, often referred to as "insiders." Insider nodes may pose security risks if they have been compromised by an unauthorized user, such as a hacker who gained access remotely, or if they have been physically compromised or captured(Meddeb, Triki, Jemili, & Korbaa, 2017).

2.4.10 Classification of Security Attack in MANET

Figure 2.15: Classification of Attack in MANET

External Attack : *The individual attempting to get access to the network from outside the network uses these attacks. And if they gain access to the network, they abuse it by sending forged packets, which brings the entire system to a halt. This attack can also occur in networks that are wired.*

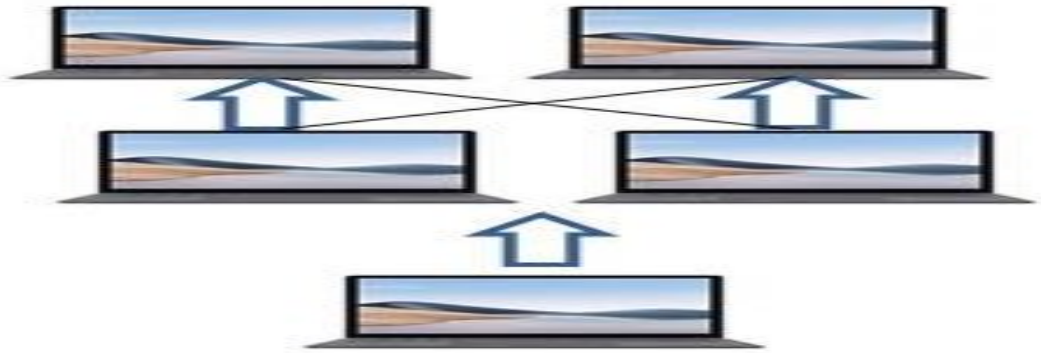


Figure 2.16: External Attack

In a network consisting of four computers or nodes are connected all of which are interconnected within the same network, an external computer, attempts to gain unauthorized access to the network to disrupt its normal operation.

Internal Attack : *Typically, this attack takes place within the network. Normally, the attacker can participate in the conversation. A newly added node to the network can take the place of an intruder who has obtained access to the network. Either through a contract with the current node or through impersonation, it has obtained access to the network. Compared to external attacks, internal attacks are much harder to foresee.*

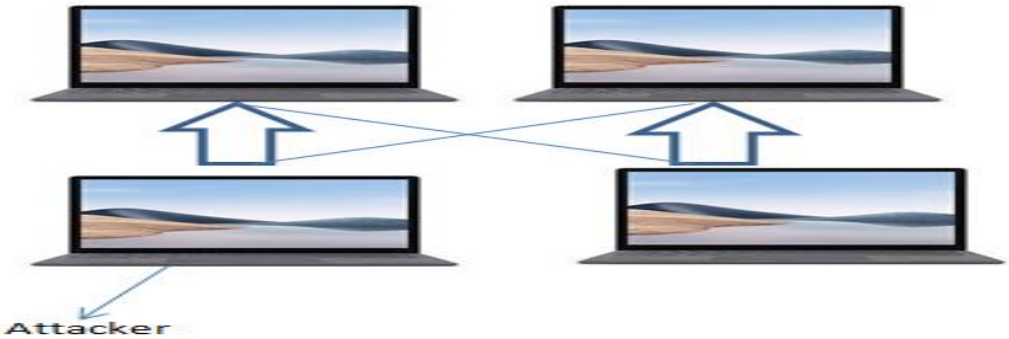


Figure 2.17: Inside Attack

Initially, a network consists of three nodes all interconnected within the same network. However, a new node is introduced into the network and becomes an active participant in communication. Regrettably, a new node is malicious and poses a threat to communication integrity. It can disrupt communication either by transmitting counterfeit packets to other nodes or by intentionally discarding all incoming packets.

Passive attacks: *are arranged by adversaries with the sole intention of clandestinely monitoring data exchange within the network. These attackers engage in eavesdropping on network traffic, enabling them to perform traffic analysis and potentially compile a user profile. The confidentiality of transmitted data is compromised if an attacker can decipher the information obtained through such covert surveillance. While these attacks may appear innocuous on the surface, they can become more insidious when combined with active attacks.*

Passive attacks do not overtly disrupt the overall network functionality, rendering their detection and identification quite challenging. The impact of such attacks can be significantly mitigated by implementing robust encryption techniques. Passive attacks encompass activities such as snooping, eavesdropping, traffic analysis, and monitoring.

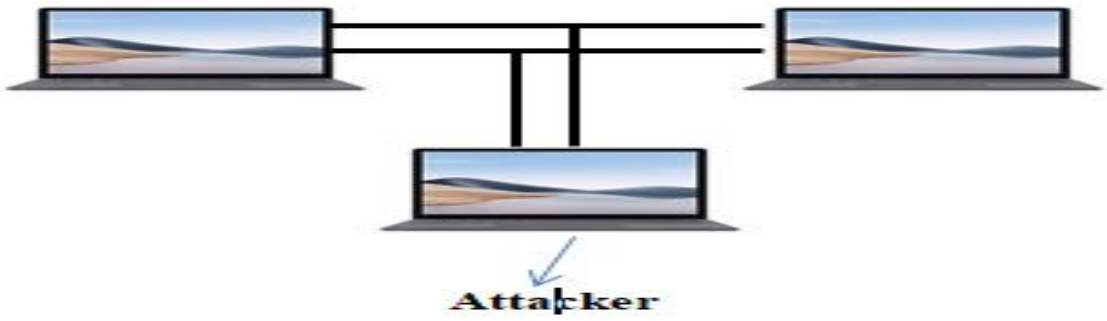


Figure 2.18: passive attack

1.Two computers, engage in communication where they exchange confidential information. During this exchange, a third computer enters the scenario and assumes the role of a sniffer. Its purpose is to intercept and monitor all communication transpiring between two computers. This type of attack involves the attacker solely observing and recording the exchanged information, intending to potentially reveal it to others.

1. *Eavesdropping: In this scenario, the attacker surreptitiously captures all transmitted data between the two parties with the aim of uncovering valuable information such as passwords, secret codes, or other confidential data.*
2. *Traffic analysis and monitoring: In this form of attack, the malicious actor closely observes the traffic patterns within the network. By doing so, they can discern the whereabouts of hosts, determine messaging patterns, assess message frequency, and analyze message lengths.*

Active attacks: *are deliberate attempts to alter, manipulate, or disrupt the information being transmitted within a network, leading to a disturbance in its regular operations. These attacks can take various forms, such as modifying packets, manipulating routing information, replaying old packets, assuming different identities, or causing service denials through actions like extensive network flooding and physical communication channel jamming. Attacks can further be categorized into two types: Insider attacks and Outsider attacks. Insider attacks originate from compromised nodes within the network. These compromised nodes seek to gather sensitive information and may exploit their access to the network's protocol privileges. Detecting Insider attacks is challenging because these compromised nodes were once legitimate and authorized, making their activities harder to identify. Outsider attacks, on the other hand, are orchestrated by adversaries who are not part of the network. These attacks can be thwarted through the use of robust encryption techniques and firewalls(Meddeb et al.,*

2017).

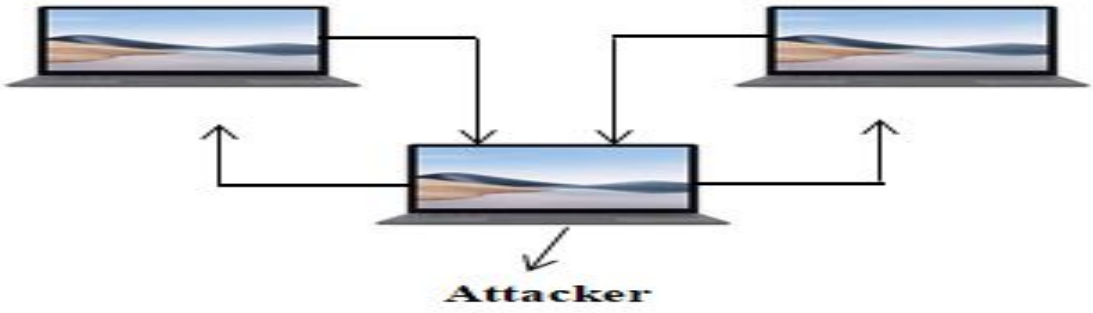


Figure 2.19: Active Attack

TTwo computers communicate with each other and one of the computers acts as an attacker who will modify or change all the data coming from the computer and then send the modified data to the next computer.

2.4.11 Routing Attacks in MANET

Routing protocols, especially those used in Mobile Ad Hoc Networks (MANETs), are susceptible to attacks by malicious nodes. Typically, these protocols are not initially created with security as a primary focus, making them vulnerable to misbehaving nodes. This vulnerability is amplified in MANET routing protocols, which aim to minimize overhead and enable every node to partake in routing. The pursuit of efficiency often heightens the security risks and permits a single node to have a substantial influence on the protocol's functioning due to the absence of redundancy mechanisms in the protocol design (U. K. Singh et al., 2011).

Black Hole Attack:- *In this particular attack, a malicious node exploits the routing protocol by falsely claiming that it offers the shortest route to the target node whose data it intends to intercept. Consequently, the attacker ends up receiving the traffic intended for other nodes and gains the option to either discard the packets to execute a denial-of-service attack or leverage its position in the route to initiate a man-in-the-middle attack. In this man-in-the-middle scenario, the attacker reroutes the packets to nodes posing as the intended destination, thereby potentially intercepting and manipulating the transmitted data.*

Spoofing:-*Involves an attempt to usurp the identity of another node, enabling the attacker to intercept all packets meant for the genuine node. This deceptive node may also propagate false routing information, among other malicious activities. To thwart this attack, a straight forward preventive measure involves mandating that every node signs each routing message, provided there is a key management system in place. However, it's important to note that this countermeasure, while effective, may lead to higher bandwidth consumption and increased CPU usage on each node due to the process of message signing.*

Modifying Routing Packets:- *One potential threat involves a node tampering with routing messages originally sent by another node. Such alterations are typically made with the inten-*

tion of deceiving other nodes within the network. For instance, routing protocols like AODV rely on sequence numbers to indicate the freshness of routes, making them vulnerable to attacks where sequence numbers are manipulated to disregard recent route advertisements. Detecting the node responsible for modifying routing messages while in transit can be quite challenging. However, implementing a security measure where each node is required to sign every routing message can prevent such attacks. In this scenario, if a node does attempt to modify routing packets, it may go unnoticed, but it won't succeed in misleading other nodes because the routing messages will lack the correct signature. The cryptographic safeguards in place allow other nodes to identify unauthorized alterations in the packet content.

Packet Dropping *In a specific type of attack, a node might announce routes through itself to multiple other nodes and then intentionally choose to discard the packets it receives, rather than forwarding them as per the advertised routes. Another variant of this attack involves a node dropping packets that contain routing messages. These attacks can be categorized as a specialized form of the broader class of packet dropping attacks.*

Selfish Nodes *The functioning of routing in MANET relies on the willingness of each node to engage in the routing process. However, in specific scenarios, nodes may opt out of participating in routing, such as to conserve their battery power. If multiple nodes choose this path, it can result in the breakdown of the MANET and render the network nonfunctional. Various protocols have been suggested to incentivize nodes to actively partake in the routing process.*

Wormhole Attack *In this type of attack, malicious entities can collaborate to transport routing and other packets using channels outside the designated communication band. This interference disrupts the normal operation of routing protocols.*

Rushing Attack *In this scenario, an attacker can expedite the transmission of certain routing packets towards the destination, which can result in routing issues.*

2.4.12 Security Goals

Securing a mobile ad hoc network is a challenging endeavor that requires substantial financial investments. In MANETs, nodes autonomously handle all networking functions, including packet forwarding and routing, further complicating the task of ensuring network security. To assess the security of a mobile ad hoc network, the following objectives are employed(Kargl, Geis, Schlott, & Weber, 2005).

1 Availability

This attribute aims to guarantee the availability of network services whenever they are required by the different network entities. Its primary focus is on countering attacks, such as denial-of-service attacks, that aim to obstruct authorized users from accessing critical services.

2 Confidentiality

ensures that the content of information is never disclosed to organizations who are not authorized to receive it. A system that possesses this property assures that the information conveyed can only be understood by the intended recipients. Other phrases that are often used interchangeably with confidentiality are secrecy and privacy. Confidentiality has become essential in the context of ad hoc networks for preserving the transmission of sensitive data. Given that wireless links are easily vulnerable to eavesdropping, this is extremely important. In some circumstances, such as the conditions of a battlefield, a leak of data traffic or control traffic information, such as routing, could have disastrous results.

3 Integrity

The verification process ensures that data remains unaltered during transmission, safeguarding it from unauthorized modifications. Such alterations can occur due to malicious actions, such as the presence of adversaries, or unintentional factors like unstable wireless connections. Attackers can tamper with the data by adding, removing, or substituting information. While many protocols, including TCP and IP, incorporate techniques like check sums to enhance resilience against benign faults, these measures often prove insufficient in guarding against deliberate manipulation of data by hostile adversaries.

4 Authentication

Authentication ensures that a node can trust that the other parties it's communicating with are indeed who they claim to be. There are two types of authentication: entity authentication, which focuses on verifying the identity of the other party, and data authentication. In systems lacking entity authentication procedures, adversaries can potentially pose as insiders, gaining access to network resources. This can impact the operation of other nodes within the network as well. Entity authentication requires active communication to verify the identity of the requester and often relies on the requester's assertion alone. Conversely, data authentication is focused on validating the integrity of the data itself. It's important to note that data authentication happens automatically.

5 Non-repudiation

ensures that neither a party nor any entity can falsely claim that another party has committed an action they haven't. For example, in the context of data transmission, the sender of a message cannot deny having sent it if they indeed did, and the receiver cannot falsely allege receiving a message from an entity that never sent it.

6 Anonymity

Involves concealing the identity of an entity participating in a process, while authorization entails granting official permission to another entity for specific actions. Time stamping refers to recording the time of an event, access control involves limiting access to authorized

entities, revocation pertains to the ability to withdraw authorization, and so forth.

2.4.13 Schemes for Solving Security Attacks

The scheme for solving security Attacks used to enhance trust in data security is interpreted as the degree of belief that a node performs as expected Based on this interpretation, a trust management scheme is developed to enhance the security of MANET.

2.4.14 Anonymous Communication and Security

Anonymity refers to the state of not being distinguishable within a set of topics. In the context of MANETs, anonymous communication is typically achieved through a combination of unlinkability and un-identifiability, which aim to keep the identities of the sender and/or receiver hidden from external observers. Adversaries cannot connect intercepted data to real network traffic patterns, ensuring that information remains unlinkable. The shared wireless infrastructure in MANETs presents opportunities for passive eavesdropping on data communications. Adversaries can eavesdrop on all messages being transmitted through the airwaves without the need for physical collaboration with a node. The crucial step in establishing secure communication within MANETs is the creation of effective anonymous and secure routing protocols, coupled with end-to-end data traffic encryption. In pursuit of this goal, we introduce several common mechanisms frequently employed in anonymous and secure routing (Lo, Chiang, & Hsu, 2015).

2.4.15 Trapdoor

In the realm of cryptographic functions, the concept of a "trapdoor" is a well-known idea that establishes a one-way function between two sets (Raghu & Menakadevi, 2016). A "global trapdoor" refers to a method of gathering information in which intermediate nodes can provide pieces of information, like node IDs, to this trapdoor. However, only specific nodes, typically the source and destination nodes, can unlock and retrieve these elements using predetermined secret keys. Utilizing a trapdoor requires the establishment of an anonymous end-to-end key agreement mechanism between the source and destination.

2.4.16 Onion Routing

Rather than directly connecting to a responsive system, initiating programs utilize a series of intermediary machines known as onion routers. To ensure anonymity, the onion technique employs multiple layers of encryption for message packets as they traverse relay servers. Message protocols utilize efficient symmetric encryption to secure data transmitted across the network, while public-key encryption is employed to establish secure and authorized connections between devices in the network chain. The onion routing network ensures that the link between the initiator and responder remains anonymous.

External eavesdroppers and compromised onion routers are unable to discern who is con-

nected to whom and for what purpose due to the use of anonymous connections. If the initiator also desires anonymity to the responder, all identifying information must be removed from the data stream before transmission via the anonymous connection. Onion routers within the network are connected through persistent socket connections. Anonymous connections through the network are multiplexed over these enduring connections (Raghu & Menakadevi, 2016)

The sequence of onion routers in a route for any anonymous connection is established during connection setup. However, each onion router can only identify the previous and next hops along the path. Data transmitted through the anonymous connection appears differently at each onion router, preventing monitoring during transit, and compromised onion routers cannot collaborate by correlating the data they observe. Replay attacks or data cannot be used in this context.

Data transferred via the anonymous connection appears differently at each onion router, thus data cannot be monitored en route, and hacked onion routers cannot cooperate by correlating the data stream each sees. We'll also see that they can't use replayed onions or data.

Access to the onion routing network is facilitated through various proxies. An initiating application establishes a socket connection with an application proxy, which converts the connection message format (and later data) into a generic format suitable for transmission through the onion routing network. It then links to an onion proxy, responsible for creating a layered data structure called an onion that outlines a route through the onion routing network. The onion is directed to the entry funnel, which occupies one of the enduring connections to an onion router and multiplexes connections into the onion routing network at that router. The onion router corresponds to the outermost layer of the onion. Each layer of the onion specifies the next hop along the path (Aggarwal, 2013).

When an onion router receives an onion, it removes one layer, determines the next destination, and forwards the remaining onion to that next router in line. The final onion router then transfers the data to an exit funnel, which is responsible for managing the data exchange between the onion routing network and the recipient. Each layer of the onion, besides indicating the next hop, also contains key seed material that is used to generate encryption keys for securing data sent both forward (the direction the onion is traveling) and backward (the opposite direction).

. Once the anonymous connection is established, it can transmit data. Before transmitting data through an anonymous connection, the onion proxy adds an encryption layer for each onion router in the route. As data traverses the anonymous connection, each onion router removes one encryption layer, eventually delivering plaintext data to the recipient.

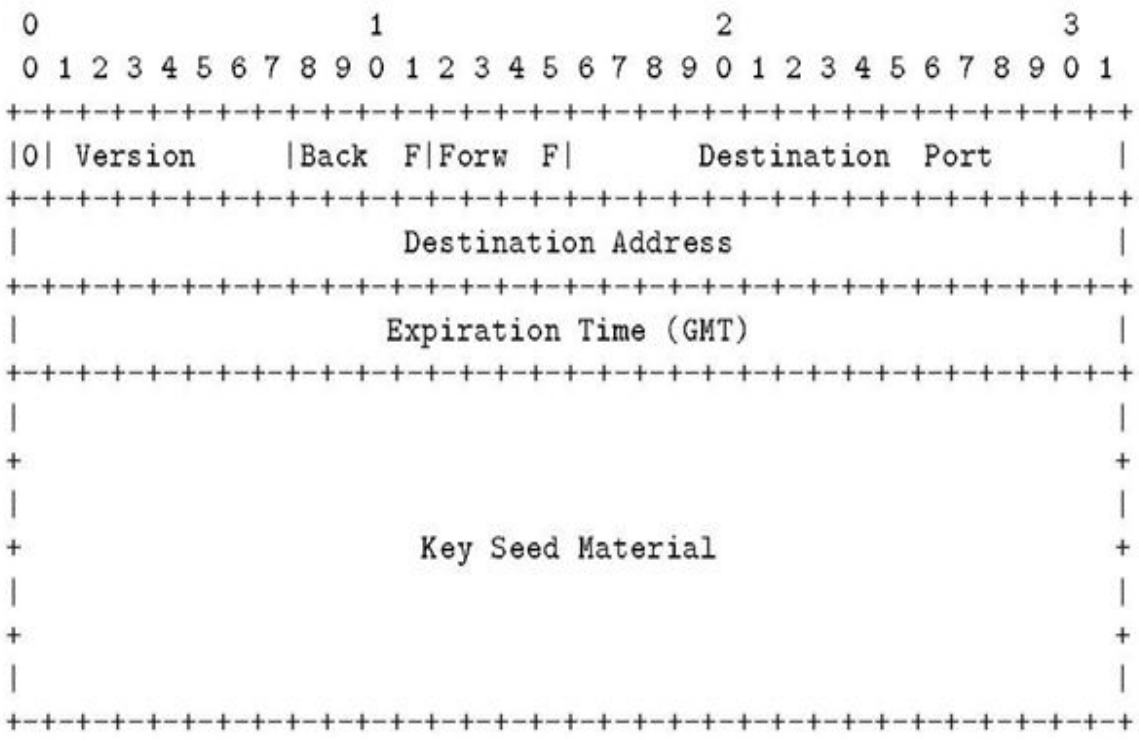


Figure 2.20: Single Onion Layer(Aggarwal, 2013)

This process is reversed for data traveling back to the initiator. This layered encryption approach offers an advantage over link encryption because each onion router sees the data differently as it travels through the network. Therefore, the privacy of an anonymous connection is as strong as its weakest link, and even one honest node in the chain can ensure the route's confidentiality. In contrast, in link-encrypted systems, compromised nodes can easily collaborate to expose routing information.Onion routers keep track of received onions until they expire. Since replayed or expired onions are not transmitted, they cannot be used by outsiders or compromised onion routers to discover routing information. It's worth noting that any discrepancies in the clocks of onion routers might cause an onion router to reject a fresh onion or retain processed onions for longer than necessary. Additionally, because data is encrypted using stream ciphers, replayed data appears different each time it passes through a properly functioning onion router (Goldschlag, Reed, & Syverson, 1999). While we refer to this system as onion routing, the routing process here occurs at the application layer of the protocol stack, not at the IP layer. Specifically, we rely on IP routing to transport data over persistent socket connections. An anonymous connection comprises fragments from multiple interconnected long-standing multiplexed socket connections. Consequently, while the sequence of onion routers in an anonymous connection remains fixed during that connection's duration, the actual route data takes between individual onion routers is determined by the underlying IP network. Therefore, onion routing can be contrasted with loose source routing. Onion routing depends on connection-based services that deliver data reliably and in the correct order, simplifying the system's specification. These guarantees are provided by

TCP socket connections, built on top of a connectionless service like IP.

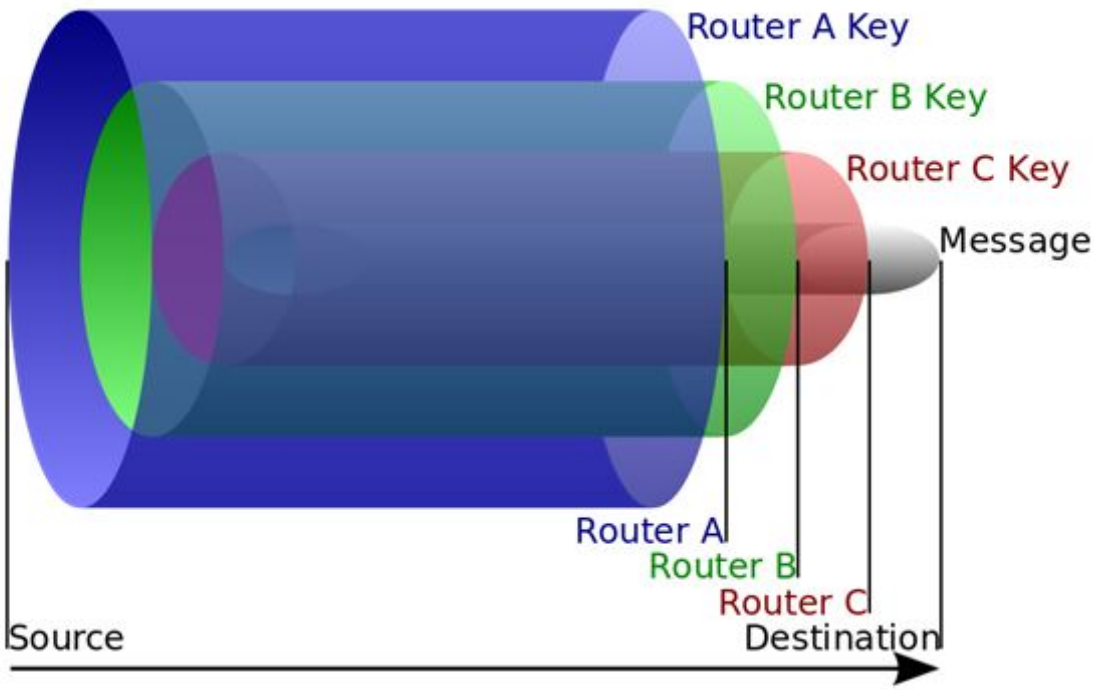


Figure 2.21: Messages are encapsulated in layers of encryption

Referring to Figure 2.21, in the encrypted process, the initial node establishes a connection. The sender can then route a message through this first node to a second node within the chain, using encryption, to the second node via the established encrypted link with the entry node. Upon receiving the message, the second node connects to the first node. While this action extends the encrypted link from the sender, the second node has no way of verifying whether the first node is the original sender. Consequently, onion routing stands in contrast to loose source routing. The sender can further transmit a message, encoded in such a way that only the third node can decipher it, through the first and second nodes to reach the third node. Like the second node, the third node establishes a connection with the sender, but only with the second node. This process can be repeated to create longer circuits, although it is typically limited to maintain network performance. Once the chain is complete, the sender can unknowingly transmit data over the Internet.

2.4.17 Secure Packet Forwarding

Securing the exchange of routing messages is just one aspect of the broader network layer security strategy for MANETs. It's important to address the possibility of a malicious node that correctly participates in the route discovery phase but fails to forward data packets accurately. To mitigate this risk, the security solution must ensure that every node forward packets in alignment with its routing table. Typically, this is achieved through a reactive approach because it's challenging to prevent attacks on packet forwarding entirely. An attacker might

choose to drop all packets passing through it, even if those packets are meticulously signed. Reactive solutions at their core incorporate a detection method and a response mechanism, which are elaborated upon as follows (Gonzalez, Ansa, Howarth, & Pavlou, 2008).

2.4.18 Detection

In a wireless network, each node has the capability to perform localized detection by monitoring ongoing broadcasts and observing its neighbors' behavior when the wireless channel is open. However, the accuracy of this localized detection is limited by various factors like errors in the channel, interference, and node mobility. Additionally, there's a risk that a rogue node could manipulate the security solution by falsely accusing legitimate nodes. To address these challenges, the detection findings at individual nodes can be aggregated and refined in a distributed manner to achieve a consensus among a group of nodes. An alternative detection method relies on explicit acknowledgments from the destination and/or intermediary nodes back to the source. This allows the source to pinpoint where the packet was dropped.

Localized Detection

In protocols like DSR (Dynamic Source Routing), a watchdog mechanism is employed on top of source routing to monitor the forwarding of packets. This watchdog mechanism assumes symmetric bidirectional connectivity, meaning if Node A can hear Node B, then Node B can also hear Node A. Since the entire path is known, when Node A passes a packet to the next hop, Node B, it is aware of B's subsequent hop, Node C. Node A then listens to the channel for any messages from B to C. If it doesn't detect any signals after a certain timeout, a failure count associated with Node B is incremented. If this count surpasses a predefined threshold, Node A sends a report packet to the source, notifying it of Node B's improper behavior. Similar concepts apply to distance vector protocols like AODV (Ad Hoc On-Demand Distance Vector), where the next-hop information is included in AODV packets, ensuring that a node is informed about the correct next hop of its neighboring nodes. These protocols also address various other types of attacks such as packet tampering, duplication, and denial-of-service attacks through packet jamming. Each individual detection result is signed and disseminated throughout the network. Multiple such results from different nodes can collectively revoke the certificate of a malicious node, effectively excluding it from the network.

Ack-Based Detection

Explicit acknowledgments (Ack) serve as the foundation for detecting defects in the communication process. When a packet is received successfully, the destination sends an Acknowl-

edgment (ACK) back to the source. If a particular path experiences an excessive number of packet drops within a short time, the source can initiate a fault detection process this process, a binary search is executed between the source and the target. Data packets are transmitted along with a list of intermediary nodes, often referred to as probes, which are anticipated to respond with acknowledgments. Each probe shares a common key with the source, and the probe list is encrypted in layers, akin to an onion. Once a probe receives the packet, it sends back an acknowledgment (ACK) that is encrypted using the key provided by the source. Subsequently, the source verifies the encrypted ACKs and attributes any errors to the node closest to it in the sequence.

2.4.19 Related Work

In MANET security is one of the most important concerns because a Manet is much more vulnerable to attacks than infrastructure-based wireless network.

Dan Boneh et.al (Boneh, Boyen, & Shacham, 2004) introduced a concise method for group signatures. Notably, this scheme achieves signature sizes similar to those of typical RSA signatures while maintaining an equivalent level of security. The security of the group signature system is built upon the Strong Diffie-Hellman assumption and the recently introduced Decision Linear assumption within bilinear groups. Additionally, the system's security is demonstrated using the random oracle model, which employs an adapted version of the security definition for group signatures.

Jiejun Kong et.al (Kong & Hong, 2003) show that the attacker can undertake traffic analysis against interceptable routing information that is encoded in routing messages and data packets in hostile settings. Covert operations may be seriously affected if enemies are able to track network routes and determine the motion patterns of the nodes at the end of those routes. We put forth ANODR, an anonymous on-demand routing system, for use in hostile contexts when mobile ad hoc networks are installed. ANODR ensures location privacy by preventing opponents from learning the true identities of local transmitters and route anonymity by preventing powerful adversaries from tracking a packet flow back to its source or destination. The "broadcast with trapdoor information" concept, a novel network security concept that combines elements of two existing networks and security procedures, provides the foundation for the creation of ANODR, namely "broadcast" and "trapdoor information".

K.K. Lakshmi Narayanan, A.Fidal Castro et.al A.Fidal Castro et.al demonstrated that within Mobile Ad Hoc Networks (MANETs), Multimodal Biometric technology plays a crucial role in enhancing security for user-to-device authentications. This research focuses on the integration of Intrusion Detection and authentication through data fusion in MANETs. To address the limitations found in unimodal biometric systems, Multimodal biometrics are em-

ployed in conjunction with Intrusion Detection Systems (IDS). Since each device comes with its own set of constraints and measurements, multiple devices are chosen, and the Dempster-Shafer theory for data fusion is utilized to enhance observation accuracy. Depending on the security posture, the system determines which biosensor (IDS) to utilize and whether user authentication (or input from IDS) is necessary. Decisions are made in a fully distributed manner for each authentication device and Intrusion Detection System (IDS).

Song. R. et.al (Song, Korba, & Yee, 2005) We commence by uncovering and evaluating the limitations of various established routing methods for mobile ad hoc networks, taking into consideration security and anonymity requirements. Building upon these insights, we introduce a fresh and innovative system known as Anonymous Dynamic Source Routing (AnonDSR), designed with three tiers of security. We compare scalability against security constraints and subject the new protocol to scrutiny, demonstrating its capability to deliver robust security, anonymity, and commendable scalability.

(Wan, Ren, & Gu, 2012)It has been recognized that certain ad hoc networks necessitate enhanced privacy safeguards, making privacy-preserving routing a vital consideration. Several privacy protection methods have been devised for ad hoc networks, but none of these systems achieve complete unlinkability or unobservability, as data and control packets remain linkable and distinguishable. In this paper, we establish more stringent privacy criteria for privacy-preserving routing in mobile ad hoc networks. Subsequently, we introduce USOR, a secure routing approach that ensures complete unlinkability and content unobservability for all types of packets. In its route discovery process, USOR utilizes a novel blend of group signature and ID-based encryption techniques. A security analysis demonstrates that USOR effectively protects user privacy against threats from both internal and external attackers.

Zhang, Liu, Lou, FangZhang et al.proposed that the inherent characteristics of mobile ad hoc networks (MANETs), such as their dynamic topology and open wireless medium, make them vulnerable to various security threats, including passive eavesdropping that can lead to devastating attacks. To counteract these risks, they introduced a novel anonymous on-demand routing protocol called MASK. MASK is designed to provide both MAC-layer and network-layer communications without revealing the real identities of participating nodes, even under the presence of strong adversaries. It offers sender, receiver, and sender-receiver relationship anonymity while maintaining high routing untraceability. Additionally, MASK exhibits resilience against a wide range of attacks and demonstrates efficiency compared to previous proposals. Simulation studies have confirmed MASK's effectiveness and efficiency.

(Wei, Tang, Yu, Wang, & Mason, 2014) highlighted the distinct characteristics of MANETs, emphasizing their dynamic topology and open wireless medium, which make them susceptible to security vulnerabilities. They proposed a trust management scheme that comprises two components: trust derived from direct observation and trust obtained from indirect ob-

servation. The trust value based on direct observation utilizes Bayesian inference, a form of uncertain reasoning, when a complete probability model can be defined. Indirect observation, gathered from neighboring nodes, contributes to trust values using the Dempster-Shafer theory, another uncertain reasoning approach applicable when deriving the proposition of interest indirectly. By combining these two components, their scheme yields more accurate trust values for nodes within MANETs. Extensive simulations demonstrate the scheme's effectiveness, showcasing improvements in throughput and packet delivery ratio with only slight increases in average end-to-end delay and message overhead.

2.4.20 Related Work Summary

Given the susceptibility of MANETs to security attacks, extensive research is underway to assess how these attacks affect the performance of MANET routing protocols, with each study focusing on specific aspects of interest. However, in this paper, our primary focus is on enhancing data security within the context of anonymous routing. As such, our literature review will concentrate on related works that delve into data security within anonymous routing.

No	Title and Year	Problem Addressed	Objective	Method used	Gap
1	Secure Routing Protocol against Internal and External Attack in MANET[2022]	Avoid the involvement of malicious node in routing	Privacy protection and optimizing packet delivery ratio	Establishing a session key with its neighboring node	High-end to end delay
2	Design and development of anonymous location based routing for mobile ad-hoc network[2022]	Improve the performance of node and routing security	Improve the performance of parameter by Minimizing delay and energy consumption.	Optimal tug of war and partition algorithm and optimal decided trust inference	No corrective scheme for active attack
3	Anonymous Safe Routing Scheme for Compromised Network Environment[2018]	proposes a protocol that stops strong adversaries from tracing a packet flow from source to destination and compare it to other existing anonymous routing protocol	providing anonymity with low computation cost overhead	asymmetric cryptography and certificates	No security measure for packet authentication.
4	Active Attack Detection and Unavailability over ALERT Protocol in MANET[2017]	Provide protection of source, destination, and location identity	Improving th packet delivery ratio	ALERT-APD algorithm	Increase the cost of Latency.
5	A Secure AODV Routing Protocol with Node Authentication [2017]	only authenticated node participate in route establishment	Improving the packet delivery ratio	Digital certificate cryptography	slightly increase end-to-end delay.
6	An Improved and efficient multi-path Anonymous routing in MANET[2017]	a void intermediate node from interfering area destination	Improving the throughput	public key cryptography	it is not scalable for a large number of node.

Table 2.1: Related work summary

CHAPTER THREE
3. PROPOSED SOLUTION

3.0.1 Proposed Solution

In the AODV protocol, when one node wishes to transmit data to another node, direct communication is possible if the target node is within the transmission range. However, when a node is out of the transmission range, intermediate nodes are required to relay data from the source to the destination node. In AODV, it's important to note that not all participating nodes can be assumed as completely trusted; some nodes may be compromised and either modify or drop messages, or eavesdrop on routing traffic. These challenges have been tackled by the proposed Secure AODV (SAODV) protocol. In the AODV protocol, when one node wishes to transmit data to another node, direct communication is possible if the target node is within the transmission range. However, when a node is out of the transmission range, intermediate nodes are required to relay data from the source to the destination node. In AODV, it's important to note that not all participating nodes can be assumed as completely trusted; some nodes may be compromised and either modifies or drop messages, or eavesdrop on routing traffic. These challenges have been tackled by the proposed Secure AODV (SAODV) protocol. This form of communication relies on the active involvement of intermediate nodes in forwarding messages, and it is during this phase that malicious nodes can disrupt communication. To address this issue, the proposed solution involved implementing relay-based transmission as part of SAODV, which was a direct response to this challenge.

The generalized pseudo-code of the proposed transmission flow of SAODV is described below

Step 1: Node S is the source want to send to node D
Step 2: If(node D is the destination) then
Step 3: Node S forwards Data to Node D
Step 4: Else if(node S apply route discovery process)
Step 5: Then
Step 6: Then SAODV applied in route discovery
Step 7: Node S will forward via a relay node to node D
Step 8: End

3.0.2 Proposed Scheme for Protocol Design

The SAODV protocol's design is presented in this section. The source node transmits an RREQ packet to every node in the network during the route discovery phase. If the destination node receives the RREQ, it will respond to an RREP packet sent back along the RREQ's arriving path. To ensure security when transferring route information, we updated the RREQ

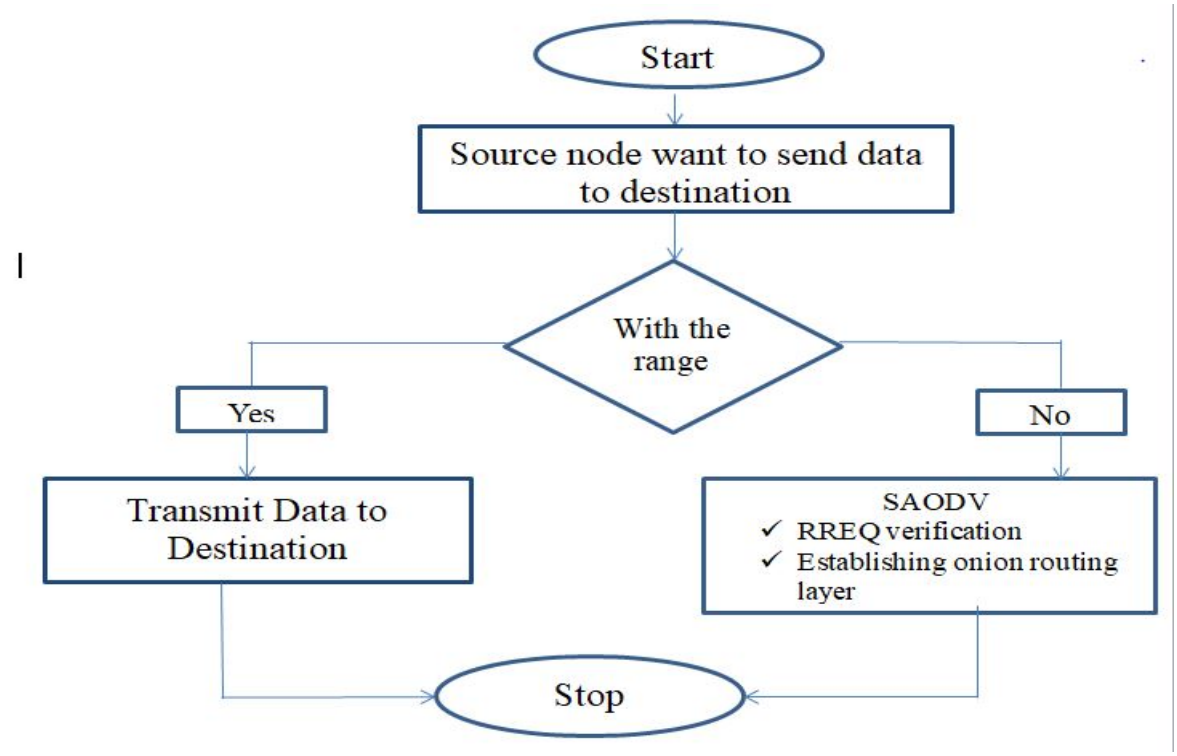


Figure 3.1: proposed Overall Data transmission

and RREP formats and adjusted the associated processes. To demonstrate the secure routing operations, we utilize a five-node network as an example. The network is shown in Fig 3.2, where the source node S discovers a path to the destination node D.

Route Discovery

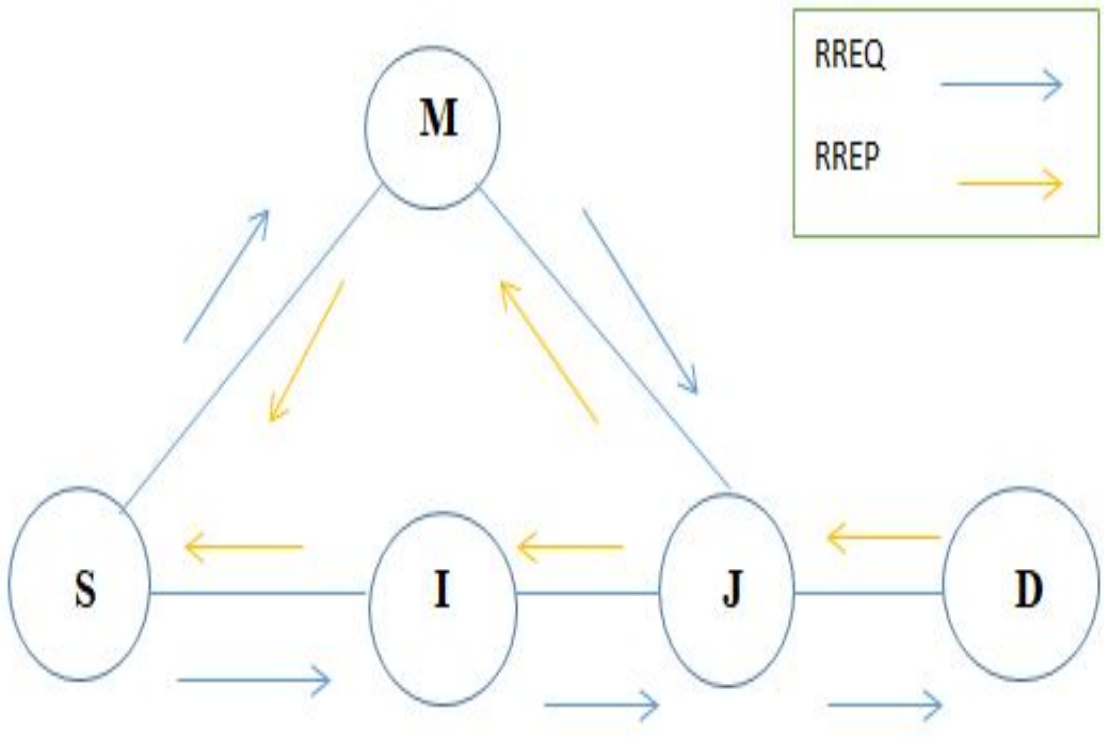


Figure 3.2: Route discovery

Secure Route Request

Source Node: For preventing route traffic analysis S will generate a new session key KSD for the association between S and D. The following entry will be updated in S's destination table.

Dest.Nym	Dest Str	Dest Pub _Key	Session key
ND	dest	K_D	K_{SD}

Table 3.1: Route Request

S will assemble and broadcast an RREQ packet in the format of (1).

$$S = [RREQ; N_{Sq};\ V_D;\ V_{SD};\ Onion(S)]\ GS \quad (3.1)$$

N_{Sq} is a sequence number randomly generated by S for this route request;

V_D is an encrypted message for the request validation at the destination node;

V_{SD} is an encrypted message for the request validation at the intermediate nodes;

Onion(S) refers to an encryption technique where S generates a crucially encrypted layer. Within this process, S generates two parameters, Nv and Kv, which are then passed on to D for future route confirmation purposes. Nv serves as a one-time nonce for route exploration, while Kv functions as a symmetric key. The VD secret message can be described as follows:

VSD=(Nv)(Kv)

$$VD = (Nv, Kv, dest)KSD, (K, D)KD..... \quad (3.2)$$

If D is the intended recipient of the message, it can decrypt the second portion of VD using its private key KD. Afterward, it can decrypt the first portion using the derived KSD. If D is not the intended destination, it becomes evident. If S and D have previously established the KSD during a prior communication, the session key encryption in the second part of VD can be omitted, simplifying the definition of VD.

S signs the entire RREQ packet using its group private key GS. Each intermediate node then examines the Nsq and timestamp to assess if the packet has been previously processed. Subsequently, the intermediate node attempts to decrypt a section of VD with its private key. If decryption fails, the intermediate node recognizes that it isn't the intended RREQ destination, prompting it to construct and broadcast another RREQ packet. When the destination successfully decrypts the VD section, it realizes that it is indeed the intended recipient of the

RREQ.

The destination can acquire the session key and validate all data, leading to the creation of an Encrypted Onion Layer at the Intermediate node. As for the RREQ packet sent by S and flooded to intermediate nodes, let's concentrate on an intermediate node called I, as illustrated in Figure 3.2. We assume that I has previously established neighbor relationships with both S and J, and it can identify the source of the incoming RREQ packet. At this point, I has stored the following entries: [include the specific entries as needed].

create Encrypted Onion Layer at Intermediate node

The RREQ packet from S is flooded into to intermediate Node. Now we focus on an intermediate node I, as shown in Fig. 3.2 We assume that I has already established the neighbor relationship with S and J. I know where the RREQ packet comes from. The following entries are stored

Neigh. Nym	**Session_Key**
NS	KSI
NJ	KIJ

Table 3.2: Intermediate Node I

Once I receive the RREQ packet, it will verify the packet with its group public key GT +. As long as the packet is signed by a valid node, I can obtain the packet information. Otherwise, such an RREQ packet will be marked as malicious and dropped.

I check the Nsq and the timestamp to determine whether the packet has been processed before or not. If the Nsq is not known in the routing table, it is a new RREQ request; if the Nsq exists in the table but with an old timestamp, it has been processed before and will be ignored; if the Nsq exists with a fresh timestamp, then the RREQ is a repeated request and will be recognized.

Then I try to decrypt the part of VD with its private key. In case of a decryption failure, I understand that it is not the destination of the RREQ. I will assemble and broadcast another RREQ packet in the following format.

I = (RREQ, Nsq, VD,VSD,Onion(I))GI-..... We assume that J has already established a neighbor relationship with I, D, and M. The following entries are already in J's neighborhood table:

Neigh. Nym	Session_Key
ND	KJD
NI	KIJ
NM	KMJ

Table 3.3: Intermediate Node J

Upon receiving the RREQ packet from I and M, J proceeds to validate the packet using its group public key GT+. If the packet bears a valid signature from an authenticated node, J can access its contents and information. However, if the RREQ packet lacks a valid signature, suggesting potential malice, it will be labeled as malicious and discarded. J then appends an additional encrypted Onion layer and forwards the packet to the next node in the route.

Destination node

The arrival of the RREQ packet at D, D follows a similar validation process to that of intermediate nodes like I or J. However, as D can decrypt the VD portion successfully, it becomes aware that it is indeed the intended destination of the RREQ. Consequently, D can access and retrieve the session key KSD, the validation nonce Nv, and the validation key Kv. With this information at hand, D is well-prepared to construct an RREP packet as a response to S's route request. Anonymous Route Reply.

Anonymous Route Reply

Destination Node: When D receives the RREQ from its neighbor J, it will assemble an RREP packet and send it back to J.

$$D = (RREP; Nrt; Kv; Onion(J)KJD) \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.3)$$

Intermediate Node:*let's suppose that J has already formed neighbor relationships with I, D, and M.*

When J receives the RREP from D, it will search its neighborhood table for shared keys and attempt to use them to decrypt Kv and Onion(J) with KJD. If this decryption process is successful, J can confirm the validity of the RREP, identify it as coming from ND, and acquire the validation key Kv. Following this, J proceeds to decrypt the onion part and learns that the next hop for the RREP is NI.

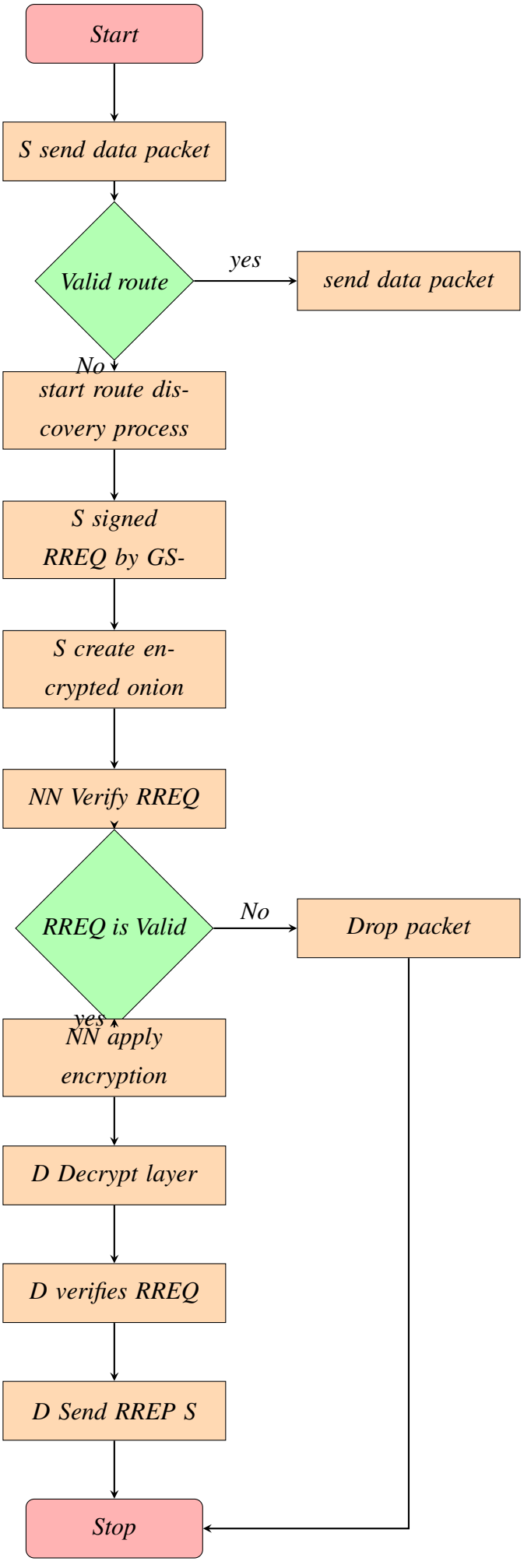
Subsequently, J will validate the connection between the received RREP and its stored RREQ. It attempts to employ the obtained Kv to decrypt the verification message VSD, which is stored in its routing table. Given that Nv in VSD does not originate from J, indicating that J is not the source of the RREQ, it becomes necessary for J to assemble another RREP and

forward it along the route.

Since Nv in VSD is not issued by J, J is not the source of the RREQ, then it has to assemble another RREP and forward it.

$$J = (RREP; Nrt; Kv; Onion(I) KIJ) \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.4)$$

Where Nrt and Kv are obtained from the received RREP; Onion(I) is obtained from the decrypted onion(J) the shared key KIJ is obtained from the decrypted Onion(J); the shared key KIJ is obtained from J's neighborhood table. The intended receiver of the RREP is I.


Start
S send data packet
Valid route
yes
send data packet
No
start route dis-
covery process
S signed
RREQ by GS-
S create en-
crypted onion
NN Verify RREQ
RREQ is Valid
No
Drop packet
yes
NN apply
encryption
D Decrypt layer
D verifies RREQ
D Send RREP S
Stop

1. *Start the program*
2. *a source node broadcasts an Encrypted RREQ packet.*
3. *Intermediate nodes verify request message and add encrypted onion layer.*
4. *The destination node decrypts the request message to route the reply to the source.*
5. *Intermediate node forward the reply message to the source*
6. *The source node receives the reply message*
7. *Stop the program.*

Destination Node: *In the context of the protocol, as the RREP packet retraces its path through the layers of the onion, it begins its journey at the destination node and moves backward toward the previous node in the route. During each step of this journey, the intermediate nodes can associate a value with the wireless link that the RREP packet is traversing. This process continues until the RREP packet reaches the source node. In this protocol, each node keeps a record of the one-time link pseudonyms that its neighboring node has disclosed. Consequently, after the RREP packet has completed its journey, the intermediate nodes can establish their forwarding tables based on the information collected during the RREP's .*

D = [RREP; Nrt;(KV;onion(J),KJ)] GS . . . . . .

Route Reply: *As the RREP packet responds along the route, it starts its journey at the destination node and retraces its path back towards the previous node in the route. At each step of this process, the intermediate node can link a value with the wireless link over which the RREP packet is traveling, until it ultimately returns to the source node.*

Secure AODV routing for MANET is suggested here as a solution to the issues previously discussed. A route is recorded using a key-encrypted onion, and a secret message is created using encryption to confirm the RREQ-RREP connection. To stop intermediary nodes from altering the routing packet, the RREQ packet per hop is authenticated using a group signature. To improve routing and data security in MANETs, an integrated trust management system has been also proposed.

where RREP is the packet type identification, Nrt is the route pseudonym provided by D, and Kv and Onion(J) are acquired from the original RREQ and encrypted using the shared key KJD. J. is the intended recipient of the RREP:

3.0.3 Summary

The newly developed algorithm, New AODV, is designed to thwart intermediate nodes from disrupting the route discovery process and intercepting routing traffic. SAODV (Secure AODV) has been employed to mitigate the interference of misbehaving nodes during route

discovery. To incorporate this new algorithm, modifications were made to the existing AODV protocol.

CHAPTER FOUR
4. SIMULATION AND PERFORMANCE EVALUATION

This section outlines the performance comparison between the proposed solution and the simulation results, using performance metrics for evaluation.

4.0.1 Introduction to Network Simulator

The Network Simulator is a simulation tool designed for research in both wired and wireless networking, including local and satellite networks. NS is a highly promising tool and is widely adopted by universities and researchers for their work (using Xgraph/GNUplot).

Optical Micro-Networks Plus Plus $(OMNET++)$

OMNeT++ boasts a versatile and adaptable architecture that allows it to excel in various domains, including network connectivity, hardware architectures, and business operations. Its components also referred to as modules, are written in C++, and they can be seamlessly combined into more extensive components and models using a high-level language. OMNeT++ offers GUI (Graphical User Interface) support, and its modular architecture enables the simulation kernel to be integrated into a diverse array of user applications (Pan & Jain, 2008).

Mathematical laboratory $(MATLAB)$

MATLAB was established in 1984 by Math Works. It offers an interactive software environment for Pan Jain's programming needs and is written in C, making it compatible with multiple platforms. MATLAB provides a range of features, including command-line functionalities and tools for data measurement, analysis, and visualization. It covers tasks like digital filtering, signal processing, and signal modulation. Additionally, it's employed for generating waveforms and creating test systems. MATLAB caters to various technical computing applications and is utilized by scientists, engineers, researchers, and educators alike.

Network Simulator version3 $(NS3)$

The ns-3 simulator is a discrete-event network simulator for Internet systems, targeted primarily for research and educational use Pan JainPan Jain. The ns-3 project, which began in 2006, is an open-source initiative dedicated to the development of ns-3. Ns-3 is free software distributed under the GNU GPLv2 license. It will rely on continual community contributions to construct new models, debug or maintain old ones, and discuss results.

4.0.2 Network Simulator version2 $(NS2)$

NS2 provides users with the executable command ns, which accepts an input argument, the name of a Tcl simulation scripting file. Users supply the name of a Tcl simulation script (which starts a simulation) as an input argument to the NS2 executable command ns. In most cases, a simulation trace file is created and utilized to plot graphs and/or create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (Otcl). While C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up the simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles (Pan & Jain, 2008)

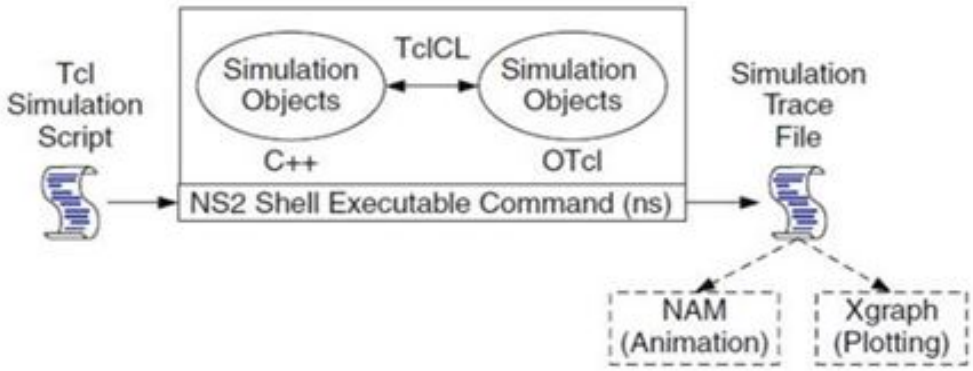


Figure 4.1: Basic Architecture of Ns2 (Mandhata et al., 2012)

4.0.3 Structure of NS-2

- ✓ *Create the event scheduler*
- ✓ *Turn on tracing*
- ✓ *Create network*
- ✓ *Setup routing*
- ✓ *Insert errors*
- ✓ *Create transport connection*

- ✓ *Create traffic*
- ✓ *Transmit application-level*

Network components

The hierarchy in NS2 begins with the TclObject, serving as the superclass for all OTcl library objects. This includes schedulers, network components, timers, and various objects, including those related to NAM. The NsObject class, being an ancestor of TclObject, serves as the superclass for fundamental network component objects responsible for packet handling. These objects can make up more complex network entities like nodes and links. The basic network components are further categorized into two subclasses: Connector and Classifier, based on the number of potential output data paths they offer. The fundamental network objects that can have multiple output data paths fall under the Classifier class. (Siraj, Gupta, & Badgujar, 2012)

.

Packet

In NS, a packet consists of a stack of headers and an optional data section. The format of a packet header is established when a simulator object is instantiated. This format includes a stack of all registered headers, such as the common header, which is commonly used by various objects as needed, along with headers like IP, TCP, RTP (used by UDP), and trace header. The stack also records the offset of each header within it. This means that when a packet is processed, whether or not a specific header is used, a stack containing all registered headers is created based on the corresponding offset value.

Link

Another significant component in NS is the link. When a user creates a link using the duplex link function of a simulator object, two simplex links are established to facilitate communication in both directions. It's important to note that an output queue of a node is implemented as a component of the simplex link object. Packets dequeued from a queue are then sent to a Delay object, which simulates the link delay. Any packets dropped at a queue are directed to a NULL Agent and subsequently released. Additionally, a Time to Live (TTL) object calculates TTL parameters for each received packet and updates the TTL field of the packet accordingly.

Network Animation(NAM)

NAM provides a visual interpretation of the network topology created. Displays the NAM application and its components. Provides the visual interpretation of the network created. Can be executed directly from Tool Command Language (TCL) script. Controls include play, stop, ff, rw, pause, a display speed controller, and a packet monitor facility.

4.0.4 Overview of AODV implementation in NS2

AODV (Ad Hoc On-Demand Distance Vector) is a routing protocol in NS2 that utilizes routing agents to create, transmit, receive, and manage routing packets. In NS2, there is a C++ class named AODV, which inherits from the class Agent and inherits three key attributes and behaviors:

. (1) *a pointer " target_" which points to a link layer object.*

(2) *a function allocpkt() which can be used to create packets.*

(3) *a packet reception function recv(p,h). Among these attributes and behaviors, only the packet reception function is customized within the AODV class.*

Main C++ files for AODV are stored in the directory of ≈/aodv/ and include the following

- ✓ *Aodv.cc and aodv.h These files contain the primary definitions of AODV routing agents.*
- ✓ *Aodv_packet.h This file defines the packet header for the AODV protocol, encompassing messages like RREQ (Route Request), RREP (Route Reply), and RERR (Route Error).*
- ✓ *Aodv_rtable.cc and aodv_rtbale.h These files manage the routing entries and tables for the AODV routing protocol.*
- ✓ *Aodv_rqueue.cc and aodv_rqueue.h They define the buffer responsible for storing data packets during a routing discovery process*

OAdditionally, there are other AODV-related classes, including Agents, Timers, and routing information. The Agent class is responsible for the creation, transmission, reception, processing, and destruction of routing packets, and AODV utilizes the AODV class for these tasks. Timers manage time-driven actions and include classes such as BroadcastTimer, HelloTimer, NeighbourTimer, and RoutecacheTimer. Routing information is handled using two classes: aodv_rt_entry and aodv_rt_table classes.

For route discovery, AODV uses Send Request $(nsaddr\_tdst)$*, Send Reply* $(nsaddr, ipds)$ *, receive Request* $(Packet * p)$ *and receive Reply* $(Packet * p)$ *In the case of the send functions, RREQ or RREP messages are first constructed, and the appropriate fields are populated with the correct values before being sent to neighboring nodes..*

4.1 Simulation Parameters

Table 4.1: Simulation Parameters

General Parameters	
Operating system and simulations	Ubuntu, NS2 $(Ubuntu, NS2)$ $(version 2.35)$
Simulation area	1501x 600
Radio propagation	Two ray ground
Channel type	Wireless channel
Traffic model	CBR
Routingprotocol	AODV
Mobility model	Random waypoint
Number of nod	30
Simulation time	0.5ms
MAC type	IEEE 802.11n
Packet size	LL
Antenna	Omni-directional

4.1.1 Simulation for Existing AODV protocol

The protocol used before was visible in the simulator tool but didn't effectively prevent misbehavior. It's an ongoing protocol that hasn't resolved the issue caused by a disruptive node interfering with packets and communication channels. In this simulation, the goal was to assess the performance of the current protocol before considering any modifications. Additionally, it presents the outcome by contrasting the current AODV with the suggested SAODV.

The nodes will be configured using Tcl code. The default setup in ns-2.35 employs the existing protocol as is, without incorporating any new algorithms or alterations. The protocol is executed straightforwardly by executing the Tcl code. The simulation generates two files: one is the "nam" file, which depicts node broadcast packet animations, and the other is the "trace" file used for analyzing performance parameters.

The objective of this simulation was to observe the results of the existing AODV protocol without any measures to mitigate standard node misbehavior. The diagram below depicts an AODV configuration lacking any mechanism to prevent misbehavior. In this setup, there are 30 nodes freely moving within a defined range. These nodes move without any measures to prevent packet interruptions, and the analysis of traffic routing is performed in the absence of any misbehavior prevention mechanisms within the AODV protocol.

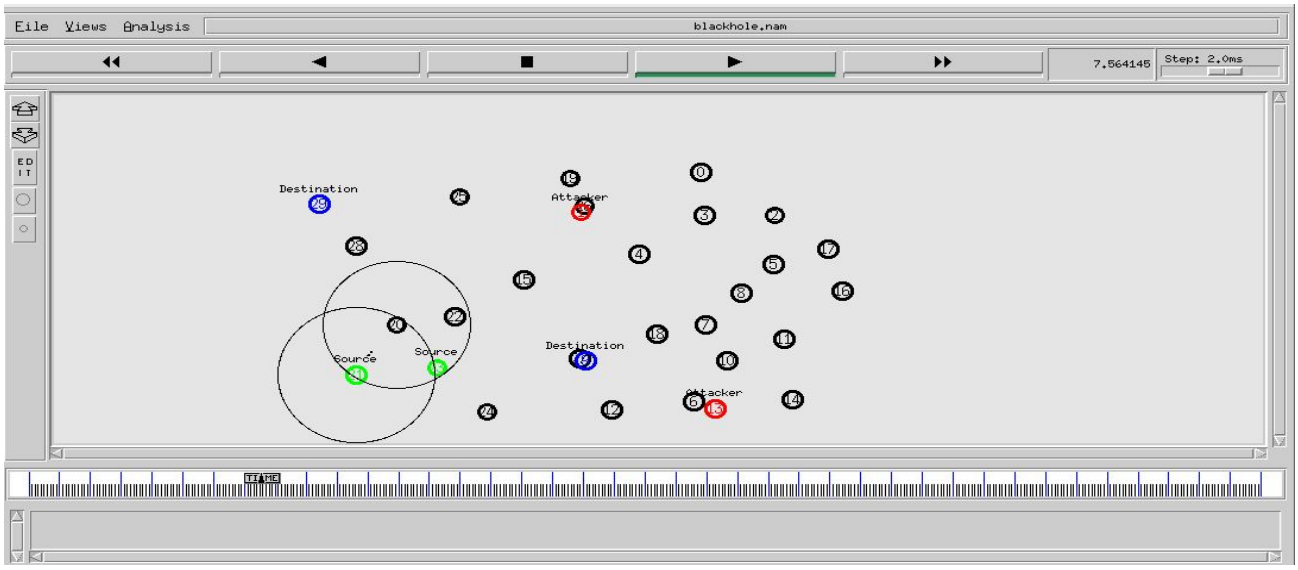


Figure 4.2: Existing AODV Simulation

4.1.2 Simulation of New AODV

To introduce RREQ authentication and incorporate an additional layer of onion encryption, the algorithm was integrated into the existing AODV routing protocol through modifications to the C++ source code in ns2.35. Specifically, the changes were made in the files AOD-Vagent.cc and AODVagent.h

Onion Layer of encryption

```
encryption(hdr->data);
send(pkt, 0);
 return (TCL_OK);
  }
else if (strcmp(argv[1], "start-WL-brdcast") == 0)
 {
Packet* pkt = allocpkt();
hdr_ip* iph = HDR_IP(pkt);
hdr_security_packet* ph = hdr_security_packet::access(pkt);
strcpy(ph->data, "test");
iph->daddr() = IP_BROADCAST;
iph->dport() = iph->sport(); ph->ret = 0; send(pkt, (Handler*) 0);
return (TCL_OK);
}
else if (strcmp(argv[1], "oneway") == 0) {
oneway=1;
return (TCL_OK);
```

```
}
(Agent::command(argc, argv));
}
Encryption Function voidSecurity_packetAgent::encryption(char out[])
{
int key =3; inti=0; for (i=0;I; <strlen(out);i++)
}
}
```

In this section, we conduct simulations to assess node mobility, with AODV routing serving as the foundation for our protocol. This encompasses the various phases such as route discovery, data transmission, and route maintenance. Our proposed approach leverages the AODV module to facilitate cryptographic operations. Each node possesses its transmission range, and we simulate a group signature scheme. The routing is determined using a trust-based routing scheme, achieved by generating the required number of nodes. Consequently, in this section, we demonstrate the simulation of secure AODV routing, as depicted in the following figure.

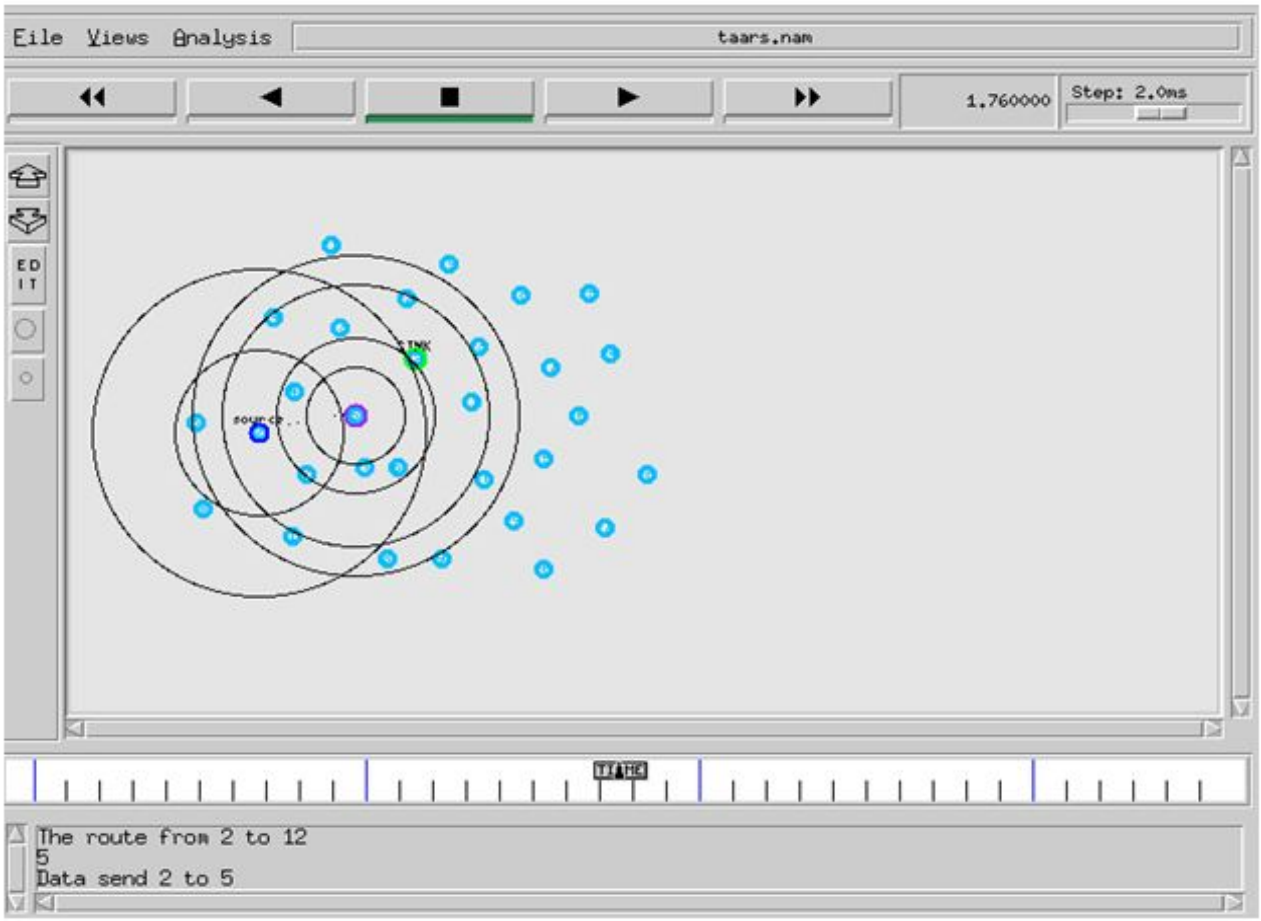


Figure 4.3: Trust-based authentication routing simulation

4.1.3 Route Request

In Chapter 3, we covered onion routing, where during the route request phase, each forwarding node adds an encrypted layer to the route request message. Importantly, the source and destination nodes may not possess information about the identity of the forwarding nodes involved. When the destination node receives the onion, it forwards it along the route back to the source. Intermediate nodes have the ability to confirm their role by decrypting and removing the outer layer of the onion. Ultimately, this process leads to the establishment of an anonymous route.

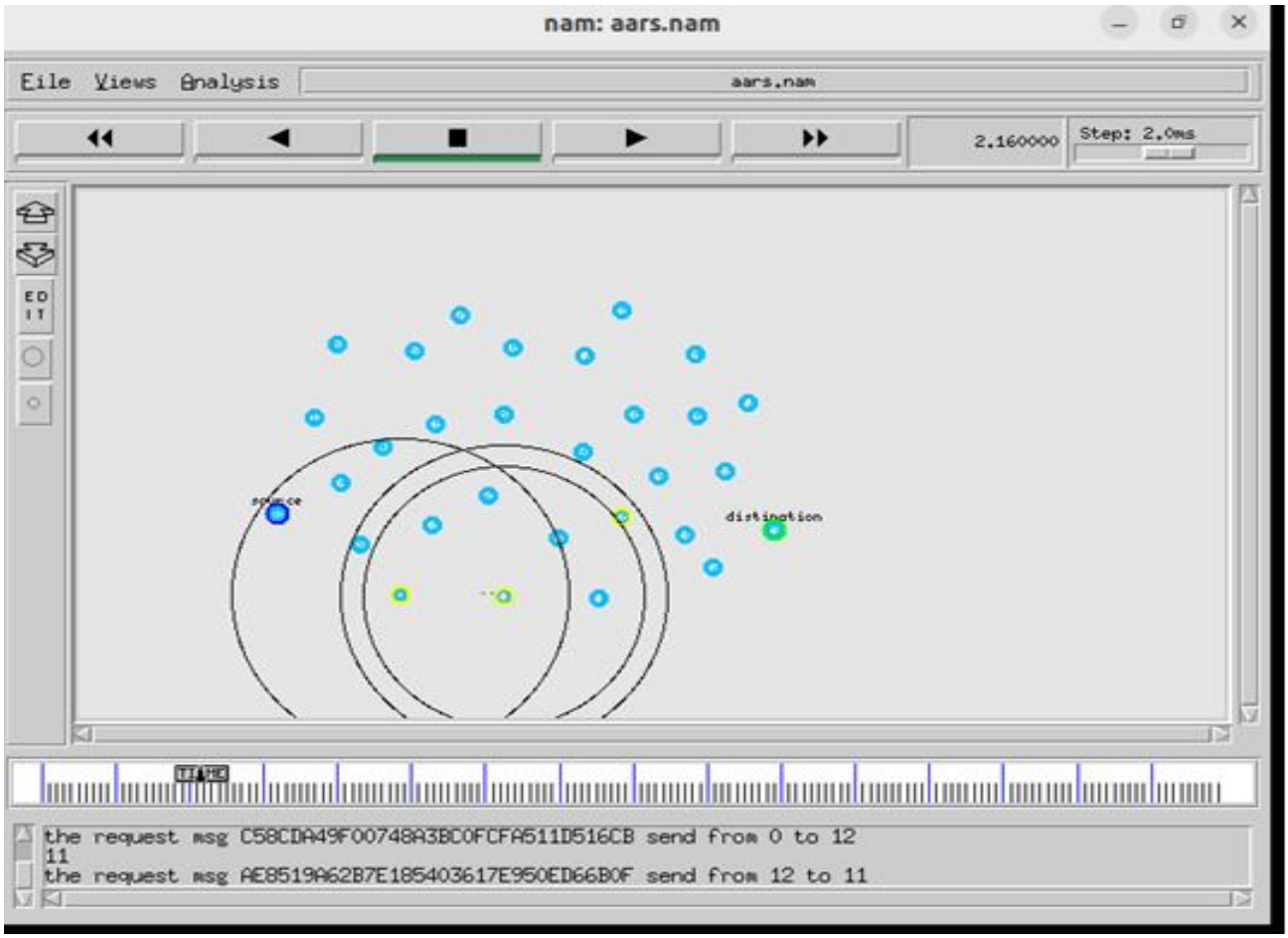


Figure 4.4: Route Request

Route Reply

The route discovery phase involves the transmission of a Route Request message (RREQ) from the source node to the destination node and the subsequent reception of a Route Reply message (RREP) from the destination node back to the source node through neighboring and intermediate nodes, as illustrated in Figure 4.5

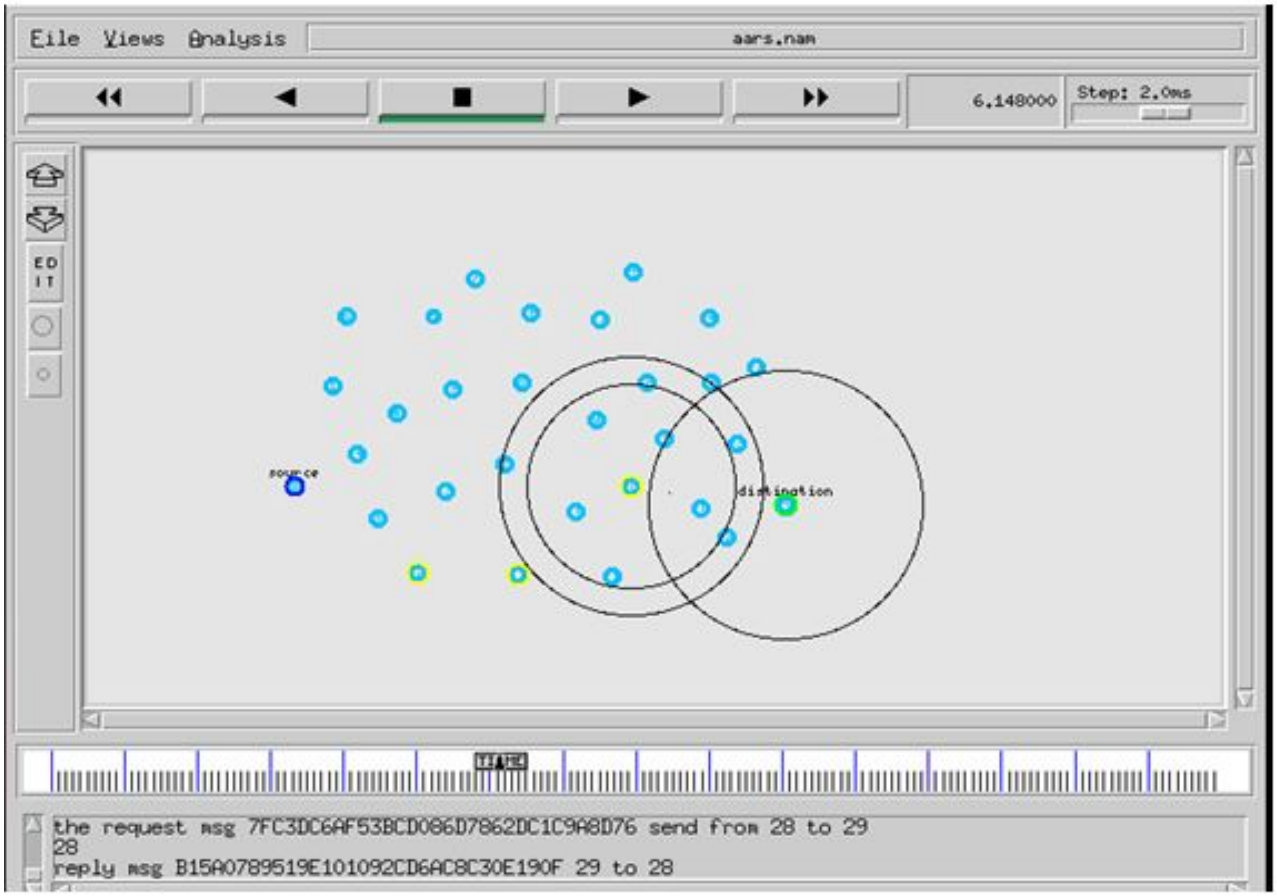


Figure 4.5: Route Reply

4.1.4 Trust Get Phase And Data Transmission

After establishing a secure route, the source node encrypts the data and sends it through the established path, taking into account the trust values computed for each intermediate node. The data is decrypted at the destination node. Figure 4.5 illustrates the encryption process at the source node, Figure 4.6 shows the encryption at the source node; Figure 4.7 shows the encryption and forwarding of data by intermediate node and the Figure 4.8 shows the decryption at a destination node.

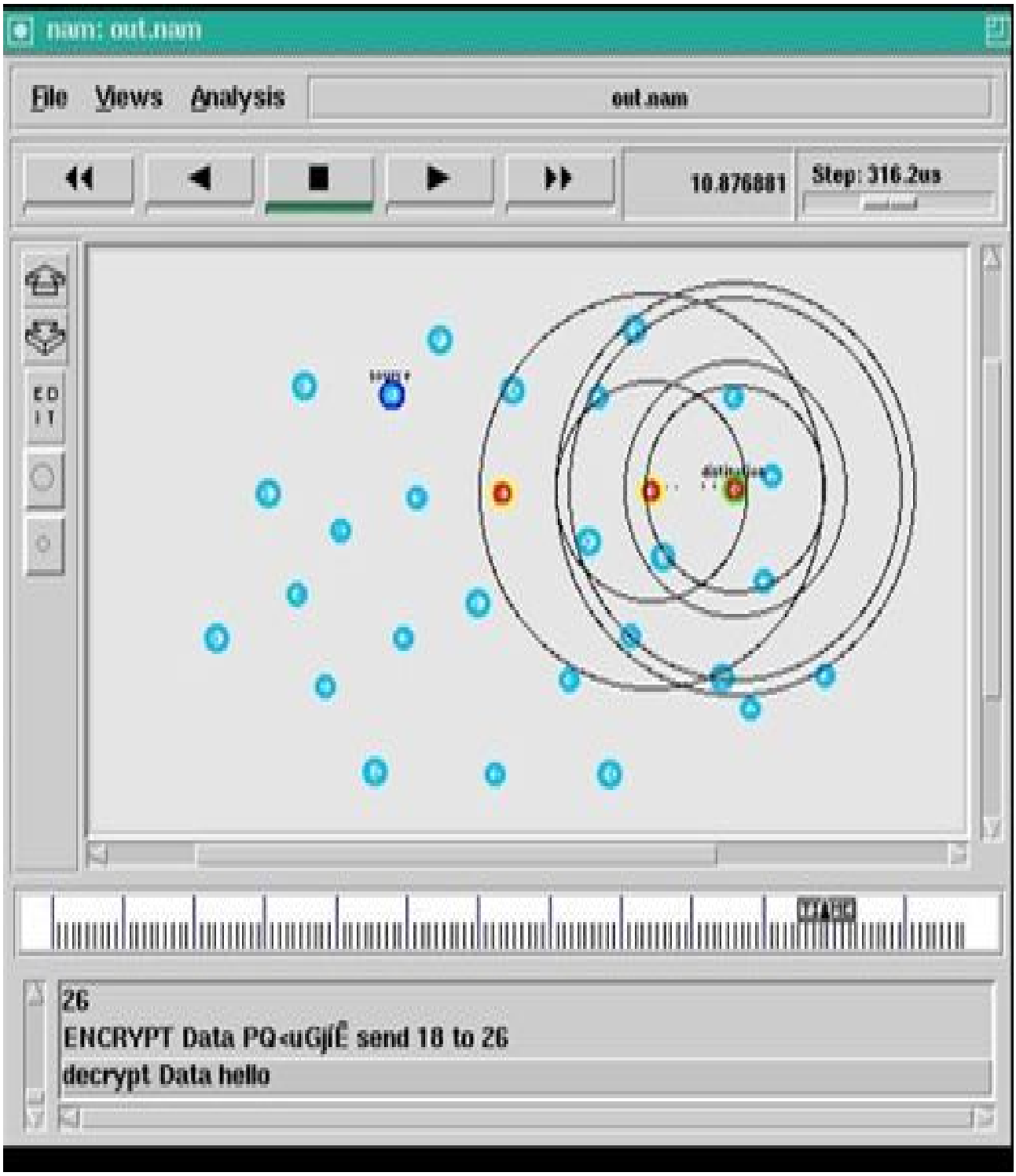


Figure 4.6: Encryption at Source node

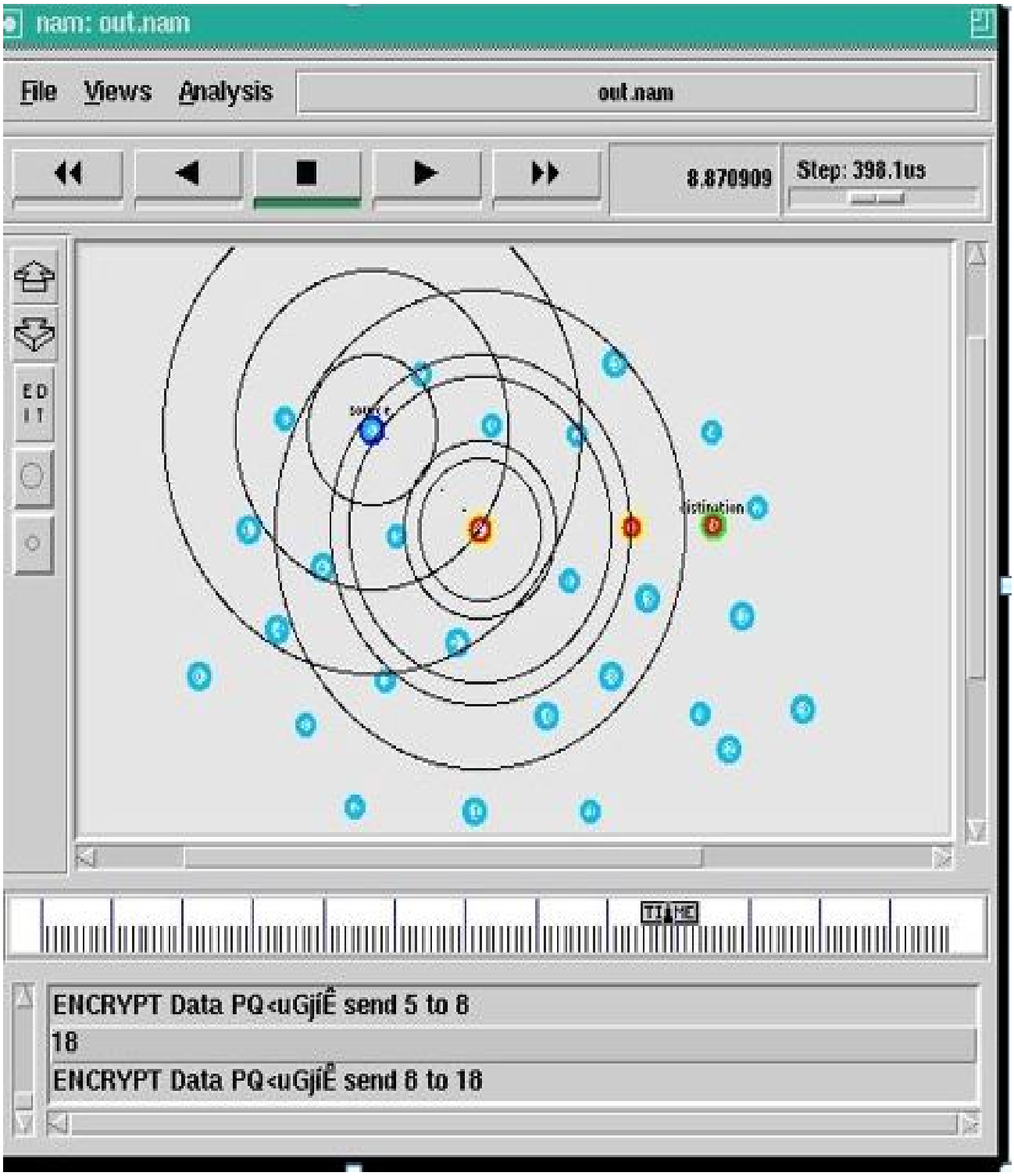


Figure 4.7: Encryption at forwarding node

Once the secure route is identified the intermediate node encrypts the message and transmits it via the established route based to destination node

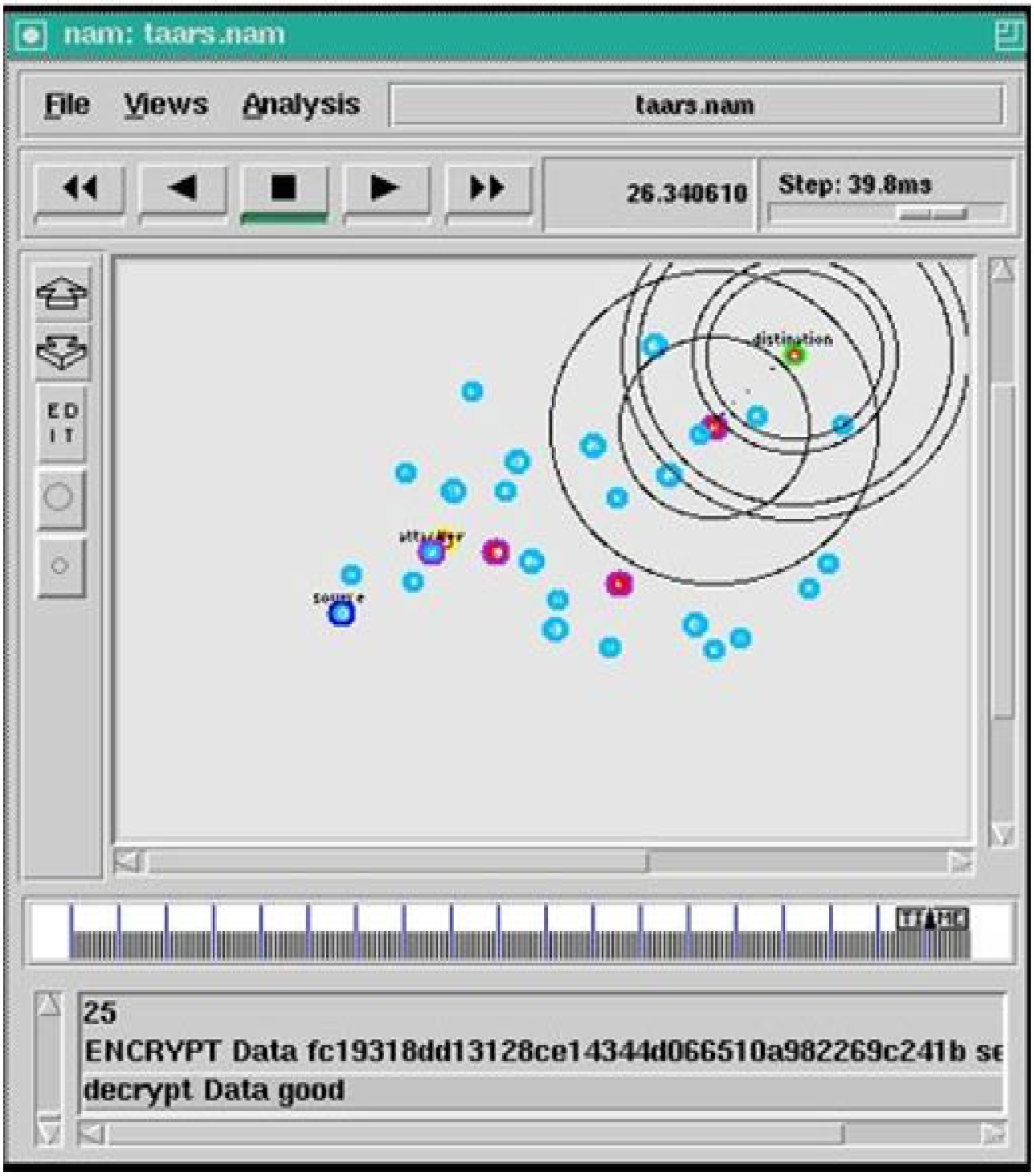


Figure 4.8: Decryption at the Destination node

4.1.5 Simulation Result and Result Comparison

The proposed protocol is evaluated and compared with the previous work based on the factors such as topology and traffic, attack models and the End results.

- ✓ *Topology and Traffic –The network area is 1501m × 600m with 30 nodes initially and uniformly distributed. The radio uses the two-ray ground reflection propagation model.*

- ✓ *When the number of misbehavior nodes increases, can affect average throughput of protocols and Packet delivery ratio.*

4.1.6 Result of the SAODV

The simulation performance was evaluated using various metrics, including throughput, average end-to-end delay, and packet delivery ratio for the existing DSR (Dyn amic Source Routing) protocol. Figure 4.9 below illustrates the throughput, which represents the number of packets delivered per unit of simulation time, both at the point of sending and receiving the packet.

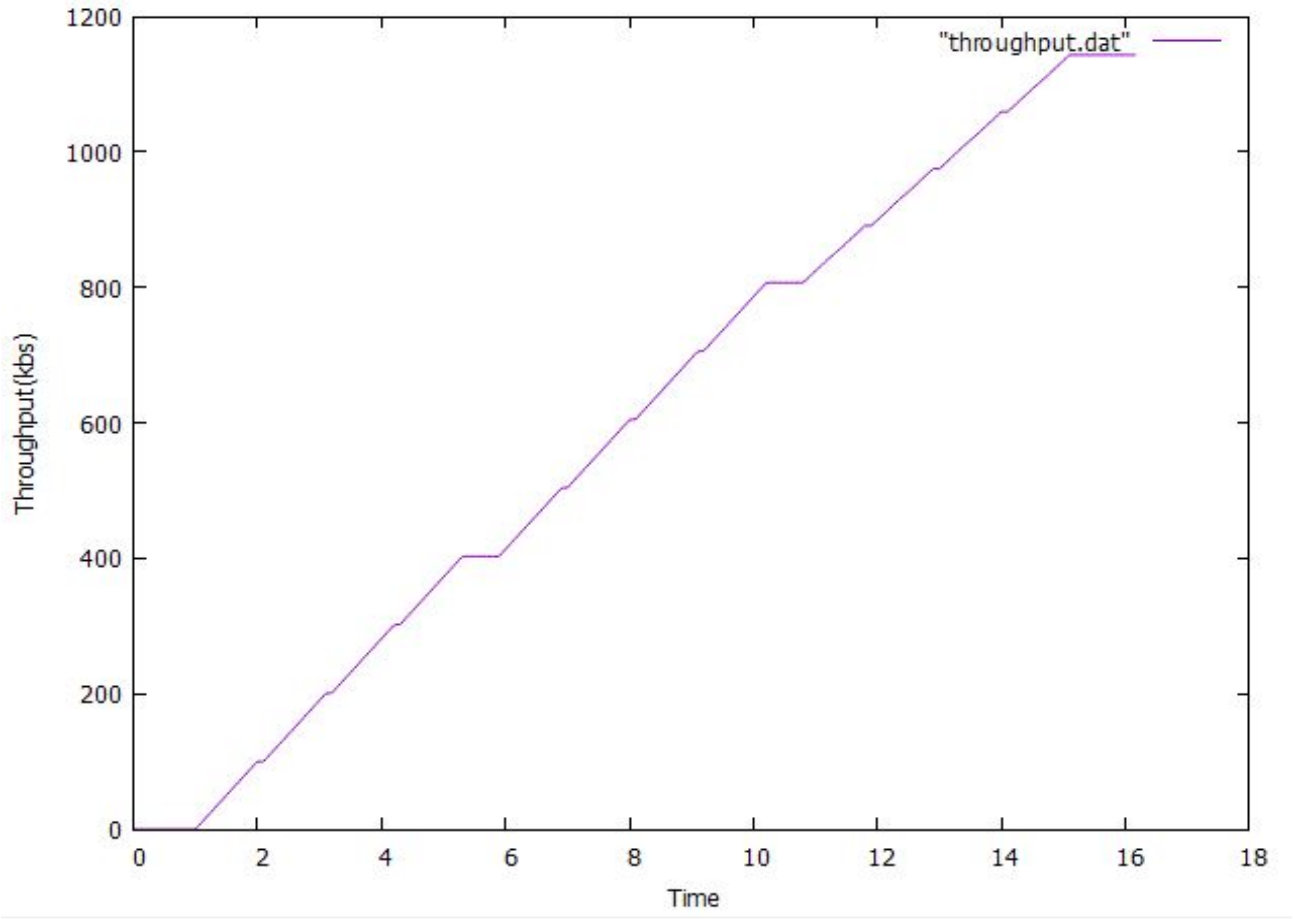


Figure 4.9: Throughput vs time

The outcome presented in Figure 4.9 represents the packet delivery ratio, which signifies the proportion of received data packets in comparison to the total sent data packets. A higher value for the packet delivery ratio indicates superior protocol performance.

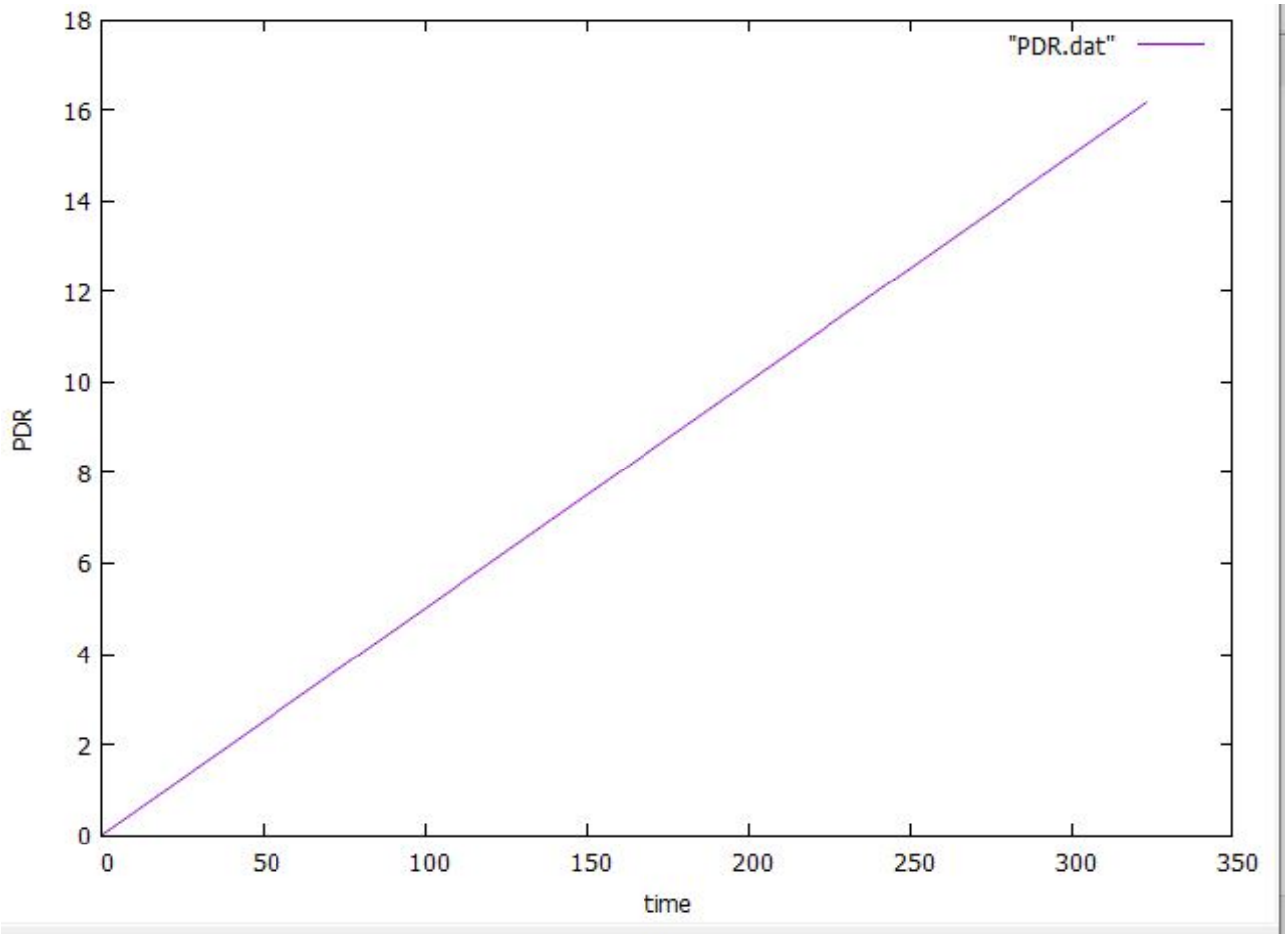


Figure 4.10: packet delivery ratio.

4.1.7 Result Comparison In terms of Average Throughput

Figure 4.11 provides a visual comparison between the proposed AODV (Ad Hoc On-Demand Distance Vector) and the existing AODV in terms of average throughput. The graph clearly illustrates that the proposed AODV outperforms the existing AODV, especially in the presence of malicious nodes. It's worth noting that as the number of malicious nodes increases, the average throughput of the existing protocols decreases. This is because SAODV (presumably the proposed AODV variant) is capable of detecting packet-dropping attacks, which contributes to its higher .

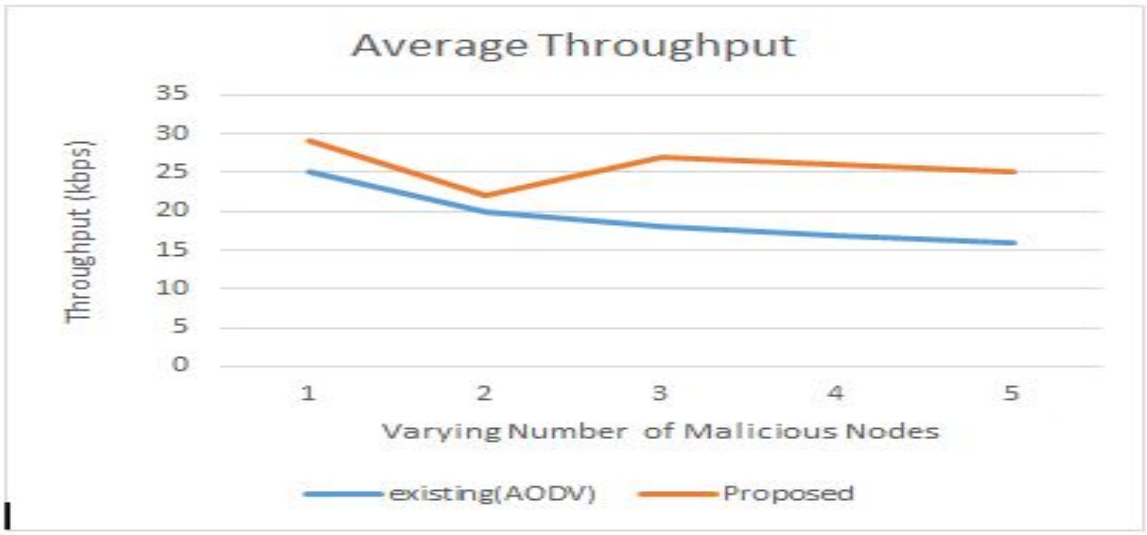


Figure 4.11: Average Throughput in malicious node

4.1.8 Result Comparison In terms of packet loss ratio

Graph 4.12 shows that the proposed SAODV achieves less packet loss ratio under different number of mobile scenarios as compared to existing AODV

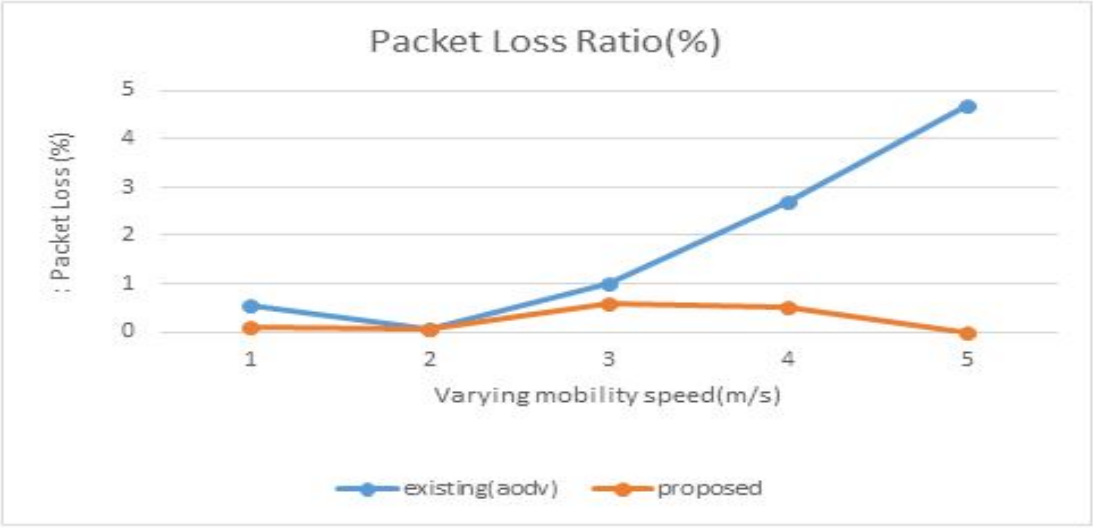


Figure 4.12: packet loss ratio in mobility speed

4.1.9 Evaluation of Result

The performance of both the SAODV protocol and the new AODV with the same simulation environment was evaluated with different metrics. The result of performance metrics is different thus proposed SAODV enhances the performance of AODV by reducing packet loss, increasing packet throughput. When detecting the misbehavior node only normal nodes participate in transferring the data packet, increasing the packet transmitted to the real destination.

CHAPTER FIVE
5. CONCLUSION AND FUTURE WORK

In this chapter, based on the result observation the thesis work was concluded, a contribution summary of the proposed solution and future research directions were described.

5.1 Conclusion

This study resolved and improved the effect of misbehavior in AODV in the process of finding the route to the destination that leads to routing traffic interception, RREQ interruption, and trust value of the node. Furthermore, various MANET and AODV protocol area-related literature and papers were reviewed and assessed to formulate the problem caused by AODV with the existence of active and passive attacks. Afterward, we proposed a SAODV solution that solves the problem and improves the existing AODV protocol. The proposed SAODV provides trusted secure anonymous communication by protecting node anonymity, location privacy, and packet authentication to perform secured communication in an adversary environment. The proposed solution has three basic steps, create encrypted onion routing, RREQ authentication, and trust verification of the node. The simulation result focused on two performance-related metrics: packet loss ratio and average throughput of the packet to evaluate the proposed solution. In this study, the NS-2.35 has been chosen to simulate.

We conclude that the proposed SAODV-based AODV protocol which was based on the speed of mobility of node and node behavior performs better in terms of average throughput and packet loss ratio perform better compared with the existing AODV protocol

5.1.1 Future Work

This study aims to prevent attackers from detecting the routing packet and authenticating the message. It designed secure communication in adversary environments. However, this solution requires computational power and energy to encrypt the routing packet and verify the message. Like security Energy conservation is also a major issue in MANET for established stable communication, In the future, we will improve energy efficiency by designing an anonymous secure energy-efficient algorithm.

REFERENCES

Aggarwal, R. (2013). Security on dynamic source routing protocol using onion routing encryption. International Journal of Engineering and Advanced Technology, ISSN, *2249–8958.*

Ahmed, D. E. M., & Khalifa, O. O. (2017). An overview of manets: applications, characteristics, challenges and recent issues.

Arnous, R., El-kenawy, E., & Saber, M. (2019). A proposed routing protocol for mobile ad hoc networks. Int. J. Comput. Appl, 975*, 8887.*

Azza, M., & Hacene, S. B. (2017). An enhanced reputation-based for detecting misbehaving nodes in manet. International Journal of Wireless and Microwave Technologies (IJWMT), 7*(4), 28–37.*

Boneh, D., Boyen, X., & Shacham, H. (2004). Short group signatures. In Crypto *(Vol. 3152, pp. 41–55).*

Briscoe, N. (2000). Understanding the osi 7-layer model. PC Network Advisor, 120*(2), 13–15.*

Chang, Z., Gaydadjiev, G., & Vassiliadis, S. (2005). Routing protocols for mobile ad-hoc networks: current development and evaluation. In Annual workshop on circuits, systems and signal processing *(pp. 489–494).*

Chitkara, M., & Ahmad, M. W. (2014). Review on manet: characteristics, challenges, imperatives and routing protocols. International journal of computer science and mobile computing, 3*(2), 432–437.*

Fazeldehkordi, E., Amiri, I. S., & Akanbi, O. A. (2015). A study of black hole attack solutions: On aodv routing protocol in manet. *Syngress.*

Goldschlag, D., Reed, M., & Syverson, P. (1999). Onion routing. Communications of the ACM, 42*(2), 39–41.*

Gonzalez, O., Ansa, G., Howarth, M., & Pavlou, G. (2008). Detection and accusation of packet forwarding misbehaviour in mobile ad-hoc networks. Journal of Internet Engineering, 2*(1), 181–192.*

Gupta, A., Verma, P., & Sambyal, R. S. (2018). An overview of manet: features, challenges and applications. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 4*(1), 122–126.*

Habib, S., Saleem, S., & Saqib, K. M. (2013). Review on manet routing protocols and challenges. In 2013 ieee student conference on research and developement *(pp. 529–533).*

Jayasuriya, A., Perreau, S., Dadej, A., Gordon, S., et al. (2004). Hidden vs exposed terminal

problem in ad hoc networks *(Unpublished doctoral dissertation). ATNAC 2004.*

Kale, M. R. A., Gupta, S., & Prmit, B. (2013). An overview of manet ad hoc network. International journal of computer science and applications, 6*(2), 257–264.*

Kargl, F., Geis, A., Schlott, S., & Weber, M. (2005). Secure dynamic source routing. In Proceedings of the 38th annual hawaii international conference on system sciences *(pp. 320c–320c).*

Kaur, H., Sahni, V., & Bala, M. (2013). A survey of reactive, proactive and hybrid routing protocols in manet: a review. network, 4*(3), 498–500.*

Kong, J., & Hong, X. (2003). Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In Proceedings of the 4th acm international symposium on mobile ad hoc networking & computing *(pp. 291–302).*

Kumar, M., & Mishra, R. (2012). An overview of manet: History, challenges and applications. Indian Journal of Computer Science and Engineering (IJCSE), 3*(1), 121–125.*

Li, Y., Li, D., Cui, W., & Zhang, R. (2011). Research based on osi model. In 2011 ieee 3rd international conference on communication software and networks *(pp. 554–557).*

Lo, N.-W., Chiang, M.-C., & Hsu, C. Y. (2015). Hash-based anonymous secure routing protocol in mobile ad hoc networks. In 2015 10th asia joint conference on information security *(pp. 55–62).*

Mahmood, S., Mohsin, S. M., & Akber, S. M. A. (2020). Network security issues of data link layer: an overview. In 2020 3rd international conference on computing, mathematics and engineering technologies (icomet) *(pp. 1–6).*

Mandhata, S., Patro, S., & Mohanty, S. (2012). Exploration of security threats and its performance impact on mobile ad-hoc networks using ns-2. International Journal of Computer Applications, 975, *8887.*

Maurya, P. K., Sharma, G., Sahu, V., Roberts, A., Srivastava, M., Scholar, M., et al. (2012). An overview of aodv routing protocol. International Journal of Modern Engineering Research (IJMER), 2*(3), 728–732.*

Meddeb, R., Triki, B., Jemili, F., & Korbaa, O. (2017). A survey of attacks in mobile ad hoc networks. In 2017 international conference on engineering & mis (icemis) *(pp. 1–7).*

Molva, R., & Michiardi, P. (2003). Security in ad hoc networks. In Personal wireless communications: Ifip-tc6 8th international conference, pwc 2003, venice, italy, september 23-25, 2003. proceedings 8 *(pp. 756–775).*

Ochola, E. O., & Eloff, M. M. (2011). A review of black hole attack on aodv routing in manet. In Issa.

Padiya, S., Pandit, R., & Patel, S. (2013). Survey of innovated techniques to detect selfish nodes in manet. IJCNWMC, 3*(1), 221–230.*

Pan, J., & Jain, R. (2008). A survey of network simulation tools: Current status and future

developments. Email: jp10@ cse. wustl. edu, 2*(4), 45.*

Patel, D. N., Patel, S. B., Kothadiya, H. R., Jethwa, P. D., & Jhaveri, R. H. (2014). A survey of reactive routing protocols in manet. In International conference on information communication and embedded systems (icices2014) *(pp. 1–6).*

Raghu, R., & Menakadevi, T. (2016). A survey on anonymous secure on-demand routing protocols in manets. Middle East J. Sci. Res, 24, *3869–80.*

Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. Journal of computer security, 15*(1), 39–68.*

Rukhande, S., & Shete, P. (2015). Optimized routing by excluding selfish nodes for manet. Communications on Applied Electronics, 3*(5), 43–49.*

Shivahare, B. D., Wahi, C., & Shivhare, S. (2012). Comparison of proactive and reactive routing protocols in mobile adhoc network using routing protocol property. International Journal of Emerging Technology and Advanced Engineering, 2*(3), 356–359.*

Singh, R. (2018). An overview of manet: characteristics, applications attacks and security parameters as well as security mechanism. Int. Res. J. Eng. Technol, 5*(9).*

Singh, U. K., Mewada, S., Iaddhani, L., & Bunkar, K. (2011). An overview and study of security issues & challenges in mobile ad-hoc networks(manet). International Journal of Computer Science and Information Security, 9*(4), 106–111.*

Siraj, S., Gupta, A., & Badgujar, R. (2012). Network simulation tools survey. International Journal of Advanced Research in Computer and Communication Engineering, 1*(4), 199–206.*

Song, R., Korba, L., & Yee, G. (2005). Anondsr: efficient anonymous dynamic source routing for mobile ad-hoc networks. In Proceedings of the 3rd acm workshop on security of ad hoc and sensor networks *(pp. 33–42).*

Srivastava, A., Mishra, A., Upadhyay, B., & kumar Yadav, A. (2014). Survey and overview of mobile ad-hoc network routing protocols. In 2014 international conference on advances in engineering & technology research (icaetr-2014) *(pp. 1–6).*

Sullivan, S., Brighente, A., Kumar, S. A., & Conti, M. (2021). 5g security challenges and solutions: a review by osi layers. IEEE Access, 9, *116294–116314.*

Venkatesan, T. P., Rajakumar, P., & Pitchaikkannu, A. (2014). Overview of proactive routing protocols in manet. In 2014 fourth international conference on communication systems and network technologies *(pp. 173–177).*

Wan, Z., Ren, K., & Gu, M. (2012). Usor: An unobservable secure on-demand routing protocol for mobile ad hoc networks. IEEE transactions on wireless communications, 11*(5), 1922–1932.*

Wang, L., Wu, K., & Hamdi, M. (2012). Combating hidden and exposed terminal problems in wireless networks. IEEE Transactions on Wireless Communications, 11*(11), 4204–*

4213.

Wei, Z., Tang, H., Yu, F. R., Wang, M., & Mason, P. (2014). Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. IEEE Transactions on Vehicular Technology, 63*(9), 4647–4658.*

Yadav, M., & Uparosiya, N. (2014). Survey on manet: Routing protocols, advantages, problems and security. International Journal of Innovative Computer Science & Engineering, 1*(2), 12–17.*

Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). Mask: anonymous on-demand routing in mobile ad hoc networks. IEEE transactions on wireless communications, 5*(9), 2376–2385.*