International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

Optimizing QOS in Mobile Ad Hoc Networks Through Advanced Routing Protocols Under Wormhole Attack Scenarios

Dr. T. Dheepak[1], R. Kayalvizhi [2], Dr. T. Suresh [3]

[1] Assistant Professor of Computer Science, CDOE, Bharathidasan University Tiruchirappalli-620 024, Tamilnadu, India.
[2] Assistant Professor, Department of Computer Science, Thanthai Hans Roever College (Affiliated to Bharathidasan University, Tiruchirappalli), Perambalur, Tamilnadu, India
[3] Assistant Professor in AIML, K. Ramakrishnan College of Engineering, Samayapuram, Trichirappalli, Tamilnadu, India

Abstract
A Mobile Ad hoc Network (MANET) is a wireless network that may autonomously reconfigure itself without relying on a centralised structure. This type of network does not have a fixed quantity and arrangement, but rather, it self-organizes and enables the automatic connection of diverse nodes. Due to its adaptive and strong character, this network is very susceptible to attacks, which may be easily rectified. Consequently, the attacker would then function as a transmitter or recipient for forged packets. The wormhole attack is considered one of the most perilous attacks on this network. A wormhole attack involves the unauthorised movement of data packets from one node to another, which may be a harmful node located either within or outside the network. In this study, we want to investigate the impact of a wormhole attack on two specific routing protocols: Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). The comparison will be conducted based on two primary network performance metrics: throughput and end-to-end delay. The simulation tests in this work will be conducted using Network Simulator-2 (NS-2) to calculate the impacts. This paper provides an alternative contribution to the realm of network attacks. The proposed Worm Hole Attack Model (WHAM) serves as an alternative for MANET routing in NS-2. WHAM has utilised the aforementioned tests to assess their resilience and durability when subjected to an attack.
Keywords: Ad-Hoc Network, Fitness function, QoS, Energy Efficient.

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is designed to establish a network in locations where there is no established infrastructure, enabling users to move freely inside the network. Put simply, a MANET refers to a group of mobile nodes that communicate and interact with each other over wireless connections, following specific guidelines. To distribute and provide the necessary network functionality. Since there is no centralised infrastructure, the node is responsible for doing the routing. MANET can be utilised in several domains such as military operations, sensor networks, disaster rescue missions, and conferences. Regardless of geographical location, this network architecture effortlessly delivers data and services because to its self-reconfigurable structure.

MANET consists of three types of protocols: reactive, proactive, and hybrid routing protocols. This study seeks to examine two types of routing protocols, specifically Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), in the presence of a wormhole assault. To the best of our knowledge, no researcher has conducted such a study thus far. This study brings a novel advantage to the realm of network security. The system offers an alternative Wormhole Attack Model (WHAM), which has been previously mentioned in the context of MANET routing using the network simulator-2 (NS-2). WHAM has utilised the aforementioned protocols to assess their resistance and power in the face of an attack.

In the dynamic realm of Mobile Ad Hoc Networks (MANETs), ensuring a robust Quality of Service (QoS) is paramount for seamless and reliable communication. However, the landscape becomes more intricate when the network faces security threats, such as the sophisticated Wormhole Attack. This research delves into the intricate intersection of QoS optimization and advanced routing protocols in the face of Wormhole Attack scenarios within MANETs. The primary focus is on enhancing both the resilience and performance of mobile networks by leveraging cutting-edge routing protocols under the challenging conditions posed by Wormhole Attacks.

Mobile Ad Hoc Networks represent a unique and decentralized form of communication where nodes collaborate to establish dynamic networks without a fixed

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

infrastructure. QoS, a crucial metric in such environments, encompasses various factors such as latency, reliability, and throughput. However, the advent of security threats, particularly the Wormhole Attack, adds an additional layer of complexity, requiring innovative solutions to maintain optimal QoS levels.

The central objective of this research is to explore and optimize QoS parameters within MANETs when subjected to Wormhole Attacks. By integrating advanced routing protocols, the study aims to enhance the resilience of the network, ensuring reliable communication pathways, and simultaneously improve performance metrics.

Understanding the impact of Wormhole Attacks on QoS in MANETs is crucial for both theoretical advancements and practical implementations. By optimizing routing protocols, the research seeks to not only mitigate the effects of Wormhole Attacks but also elevate the overall performance and user experience in mobile ad hoc environments. The findings of this study can inform the design of secure and efficient communication systems for real-world MANET applications.

The research employs a multifaceted approach, combining theoretical analyses, simulation studies using network simulators like NS-2, and possibly real-world experimentation. Advanced routing protocols known for their resilience against security threats will be implemented and analyzed under various Wormhole Attack scenarios to evaluate their effectiveness in optimizing QoS.

- **Advanced Routing Protocols:** Protocols known for their adaptability to dynamic topologies and robustness against security threats, such as AODV (Ad Hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing), will be a focal point.

- **Wormhole Attack Scenarios:** Simulated Wormhole Attack scenarios will be crafted to mimic real-world threats, assessing the impact on QoS metrics like latency, packet delivery ratio, and throughput.

- **QoS Metrics Optimization:** The study will focus on optimizing key QoS metrics affected by Wormhole Attacks, aiming to strike a balance between security and performance.

2. BACKGROUND AND RELATED WORK

2.1 Mobile Ad Hoc Network

MANET, or Mobile Ad hoc Network, is a network that can be used in a specific domain, consisting of a group of nodes that are connected to each other without the need for wires. It is a self-configuring network that operates without the need for any external infrastructure or interaction. Each node in the network can function as both a router and a host concurrently. Nodes can be easily assigned in any network topology, regardless of its differences (1, 2). The advancement of communication technology and the expansion of network domains have led to an increase in the utilisation of MANET networks in many sectors such as military operations, wildlife monitoring, medical applications, and disaster response (2, 3).

In the rapidly evolving landscape of wireless communication, Mobile Ad Hoc Networks (MANETs) have emerged as a dynamic and transformative paradigm, redefining how devices connect and communicate. MANETs represent a departure from traditional networks by enabling mobile devices to form spontaneous, decentralized networks without the need for a fixed infrastructure. This introduction provides a comprehensive exploration of MANETs, delving into their foundational concepts, distinctive characteristics, practical applications, and the challenges they pose to researchers and engineers.

At the heart of MANETs lies the concept of a self-configuring, infrastructure-less network where mobile nodes communicate directly with each other, forming a temporary network on-the-fly. Unlike conventional networks that rely on centralized infrastructure, MANETs empower devices to act both as end-users and routers, fostering communication even in scenarios where a fixed infrastructure is impractical or absent. This fundamental shift in network architecture allows for unprecedented flexibility and adaptability.

MANETs exhibit several key characteristics that define their operational framework:

- Dynamic Topology: The topology of a MANET is inherently dynamic, constantly changing due to the mobility of nodes. As nodes move within the network, join, or leave, the topology undergoes frequent modifications, necessitating robust and adaptive routing strategies.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

- Self-Organization: A defining feature of MANETs is their capacity for self-organization. Nodes within the network autonomously establish connections, negotiate routes, and dynamically reconfigure the network as needed. This self-organizing capability is particularly advantageous in scenarios where a predefined infrastructure is impractical or unavailable.

- Resource Constraints: Devices within MANETs often operate with limited resources, including power, processing capabilities, and bandwidth. Efficient utilization of these resources becomes a critical factor for sustaining the network and ensuring optimal performance.

- Multihop Communication: MANETs facilitate multihop communication, wherein data travels through multiple nodes to reach its destination. This enables communication even in situations where a direct link between source and destination nodes is not feasible, contributing to the robustness of the network.

2.2 Ad Hoc On-Demand Distance Vector

In the intricate landscape of Mobile Ad Hoc Networks (MANETs), the Ad Hoc On-Demand Distance Vector (AODV) routing protocol emerges as a dynamic and adaptive solution to the challenges posed by the ever-changing network topology. AODV, a prominent member of the family of reactive routing protocols, has proven its mettle in facilitating efficient communication among mobile devices without the need for a predefined infrastructure. This exploration delves into the workings, advantages, and applications of the AODV routing protocol, shedding light on its role in navigating the dynamic terrain of MANETs.

AODV is a routing protocol specifically designed for MANETs, where nodes often move, join, or leave the network, resulting in a dynamically changing topology. Unlike proactive protocols that maintain routing information for all possible destinations at all times, AODV adopts a reactive approach. It establishes routes on-demand, minimizing the overhead associated with maintaining up-to-date routing information for every node in the network.

AODV operates based on a series of key features that distinguish it in the realm of MANETs:

- **Route Discovery:** When a node in the network wishes to communicate with another node and does not have a valid route, it initiates a route discovery process. This involves broadcasting a Route Request (RREQ) packet throughout the network.

- **Route Reply:** If a node receives a Route Request for which it has a valid route, it replies by sending a Route Reply (RREP) packet back to the source node. The RREP packet contains the route information, which is then stored by the source node for future use.

- **Route Maintenance:** AODV is equipped with mechanisms to handle link breakages and changes in the network topology. If a link in an established route breaks, the affected nodes initiate a route maintenance process to find an alternative path or update the routing tables accordingly.

- **Hello Messages:** AODV uses periodic Hello messages to monitor the liveliness of neighboring nodes. This information is crucial for maintaining accurate routing tables and detecting link failures promptly.

The documentation employs the AODV routing protocol. AODV is an adaptive routing protocol. It has undergone extensive research and development several times, demonstrating its durability and benefits. The AODV protocol offers significant benefits compared to other MANET routing protocols, as it minimises the delay in establishing a message infrastructure with the destination. Furthermore, unlike most ad hoc routing protocols, AODV actively avoids paths that are crowded. Furthermore, the fast and improvised changes in the overall structure of network connections that can impact various routing methods can be effectively managed (1, 4).
During the route discovery phase of the AODV routing protocol in a Mobile Ad hoc Network (MANET), the source node disseminates a Route Request (RREQ) message to its neighbouring nodes, as depicted in Figure 1. Upon examination of the RREQ, it is evident that it includes the IP addresses of the recipient, the broadcast ID, and the subsequent arrangement of the destination. Each intermediate node performs two distinct procedures upon receiving the RREQ packet. First, it verifies if the RREQ packet has been previously transmitted by the same source address as the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

originator of the RREQ. Based on this verification, the node either discards or accepts the RREQ packet. Flooding assaults can be evaded by implementing this verification step. Next, the intermediate node checks the destination sequence number stored in its routing database whether the RREQ packet is accepted. If the RREP packet is higher or composed to the one included in the RREQ packet, it is unicast to the root node. Alternatively, if there are no intermediate nodes with a suitable alternative path to the destination node, the RREQ packet can retain its navigation until it reaches the destination node, allowing the RREP packet to be sent to the root node.

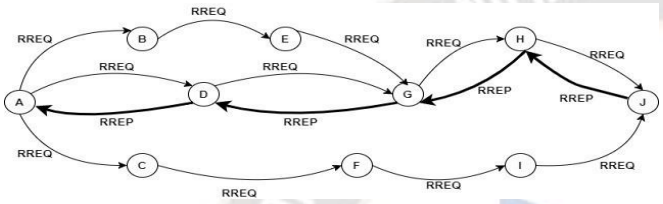


Figure 1: AODV

2.3 Dynamic Source Routing

In the intricate realm of Mobile Ad Hoc Networks (MANETs), the Dynamic Source Routing (DSR) protocol emerges as a prominent and adaptive solution, offering a robust mechanism for efficient communication in the absence of a fixed infrastructure. DSR, a reactive routing protocol, is designed to address the challenges posed by the dynamic and ever-changing topologies inherent in MANETs. This exploration delves into the intricacies of the DSR protocol, shedding light on its operational principles, key features, applications, and the challenges it tackles in navigating the uncharted paths of mobile ad hoc environments.

Dynamic Source Routing (DSR) is a reactive routing protocol specifically tailored for MANETs, where nodes may dynamically join, leave, or move within the network. Unlike proactive protocols that maintain consistent routing information for all nodes, DSR takes a reactive approach by establishing routes on-demand. DSR is known for its adaptability to dynamic network topologies, making it a suitable choice for scenarios where traditional routing protocols face limitations.

DSR operates based on a set of key features that define its functionality:

- **Route Discovery:** When a source node wishes to communicate with a destination and has no pre-existing route information, it initiates a route discovery process. During this process, the source node broadcasts a Route Request (RREQ) packet throughout the network.
- **Route Reply:** If a node receives a Route Request for which it has a valid route, it replies by sending a Route Reply (RREP) packet back to the source. The RREP packet contains the route information, which is then cached by the source for future use.
- **Source Routing:** DSR employs source routing, meaning that the entire route from the source to the destination is included in the packet header. Each intermediate node forwards the packet based on this header, eliminating the need for the nodes to maintain routing tables.
- **Route Maintenance:** DSR is equipped with mechanisms to handle route maintenance, ensuring the reliability of established routes. If a link in an active route breaks, the source node is informed, and a route maintenance process is initiated to find an alternative path.

DSR is a routing protocol categorised as a reactive routing protocol. It has the ability to easily determine or track the path from the starting point to the destination as needed. The DSR protocol utilises the Rout Discovery Method to identify the route from the root node to the destination node.

The path detection and path maintenance steps affect three varieties of communications

1. The RREQ packet is transmitted from the root node to the destination node and includes the packet ID, destination address, and its own address.

2. The RREP packet is sent by the destination node in response to receiving an RREQ packet from the root node. It creates a replacement packet of RREP and sends it to the root.

3. During the delivery of a packet, if the route of a node has changed or if there is no suitable node to transfer the packet, an RERR packet is sent. This RERR message is then transferred to the root of the packet (7).

The DSR Protocol disseminates the route across its neighbouring nodes without causing congestion. The path is accurately traced by measuring the incremental length between the root node and the target node, or by calculating the composition of existing nodes. The number 8. As depicted in Figure 2, we have a network consisting of 7

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: 10 September 2023 ***Revised:*** 20 October 2023 ***Accepted:*** 30 October 2023

nodes. The root node is identified as node N1, and the destination node is identified as node N7.

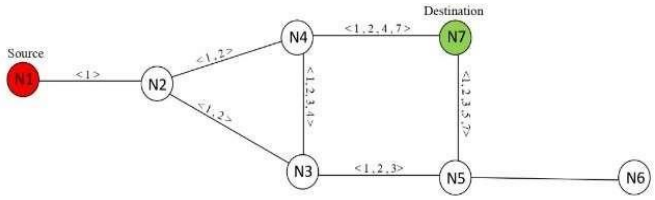


Figure 2: the Route Discovery and Route Maintenance

Step 1 You will begin with node N1 and transmit the data to its neighbouring nodes. The path information in this scenario is < 1> due to the presence of a one-to-one link between node N1 and node N2.

Step 2 Disseminate the path data that comes before to the neighbouring nodes of node N2, specifically nodes N3 and N4. The substitute path will remain unchanged in all circumstances.

Step 3 The path <1, 2> in node N3 is transmitted to the next nodes. Replace the path up to node N5 with nodes 1, 2, and 3, and the same technique can be performed for other nodes.

Step 4 Broadcast the substitutive routes<1, 2, 3, 5>, <1,2, 4> to nodes N6 and N7, individually.

Step 5 all the preceding path are iterated until the root node reaches the destination node via all ways. Three achievable ways are generated

- Route 1<1, 2, 3, 4, 7>
- Route 2<1, 2, 3, 6, 7>
- Route 3<1, 2, 4, 7>

DSR take the shortest path which is path 3 as displayed in Figure 3.

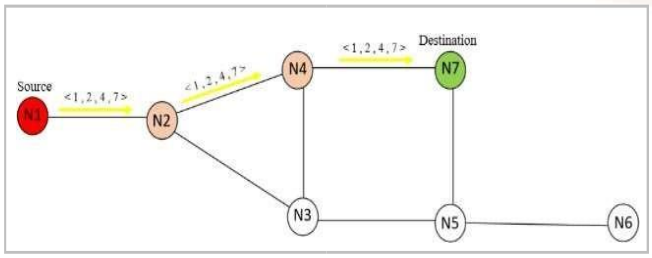


Figure 3: RREP packet sent from destination node N7

3. WORMHOLE ATTACK

In the dynamic and decentralized landscape of Mobile Ad Hoc Networks (MANETs), security concerns loom large, and one formidable threat that has garnered attention is the Wormhole Attack. This sophisticated attack poses a serious challenge to the integrity of communication within MANETs, exploiting vulnerabilities to undermine the trustworthiness of the network. This exploration delves into the intricacies of the Wormhole Attack, shedding light on its characteristics, detection mechanisms, and the impact it can have on the seamless communication that MANETs aim to provide.

A Wormhole Attack in MANETs involves malicious nodes creating a covert and high-speed communication link between them. This tunnel, known as a "wormhole," enables attackers to surreptitiously forward packets between the two ends, making it appear as if the communication is direct. The malicious nodes essentially shortcut the network, compromising the integrity of the routing process.

- **Covert Communication:** A key feature of the Wormhole Attack is its covert nature. Malicious nodes establish a clandestine communication channel, avoiding detection by other nodes in the network.

- **Shortcutting Routes:** The attackers exploit the shortcut created by the wormhole to intercept, modify, or drop packets. This can lead to disruptions in communication, unauthorized access to sensitive information, or the injection of malicious content into the network.

- **Range Limitations:** Wormhole Attacks often have limitations on their range, meaning that the malicious nodes need to be within a certain proximity to establish the tunnel. However, this proximity can still span significant distances within the network.

- **Collusion Between Nodes:** Successful execution of a Wormhole Attack usually requires collusion between malicious nodes. These nodes work in tandem to establish and maintain the covert communication link.

Wormhole Attack in Mobile Ad Hoc Networks (MANETs): Unraveling the Threat to Seamless Communication

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: 10 September 2023 Revised: 20 October 2023 Accepted: 30 October 2023

In the dynamic and decentralized landscape of Mobile Ad Hoc Networks (MANETs), security concerns loom large, and one formidable threat that has garnered attention is the Wormhole Attack. This sophisticated attack poses a serious challenge to the integrity of communication within MANETs, exploiting vulnerabilities to undermine the trustworthiness of the network. This exploration delves into the intricacies of the Wormhole Attack, shedding light on its characteristics, detection mechanisms, and the impact it can have on the seamless communication that MANETs aim to provide.

1. **Understanding the Wormhole Attack:

A Wormhole Attack in MANETs involves malicious nodes creating a covert and high-speed communication link between them. This tunnel, known as a "wormhole," enables attackers to surreptitiously forward packets between the two ends, making it appear as if the communication is direct. The malicious nodes essentially shortcut the network, compromising the integrity of the routing process.

2. **Characteristics of Wormhole Attacks:

- **Covert Communication:** A key feature of the Wormhole Attack is its covert nature. Malicious nodes establish a clandestine communication channel, avoiding detection by other nodes in the network.

- **Shortcutting Routes:** The attackers exploit the shortcut created by the wormhole to intercept, modify, or drop packets. This can lead to disruptions in communication, unauthorized access to sensitive information, or the injection of malicious content into the network.

- **Range Limitations:** Wormhole Attacks often have limitations on their range, meaning that the malicious nodes need to be within a certain proximity to establish the tunnel. However, this proximity can still span significant distances within the network.

- **Collusion Between Nodes:** Successful execution of a Wormhole Attack usually requires collusion between malicious nodes. These nodes work in tandem to establish and maintain the covert communication link.

3. **Impact on MANETs:
The Wormhole Attack poses several threats to the seamless communication envisioned in MANETs:

- **Routing Disruption:** By creating a shortcut, the attackers can disrupt the normal routing paths in the network. This can lead to packet loss, delays, or even denial of service in extreme cases.

- **Data Integrity Compromise:** The attackers can tamper with the content of the intercepted packets, compromising the integrity of the data being communicated. This can have severe consequences, particularly in scenarios where data accuracy is critical.

- **Security Breach:** If the wormhole is used for unauthorized access, it opens the door for potential security breaches. Malicious nodes may gain access to sensitive information or launch further attacks within the network.

- **Trust Erosion:** The covert nature of the Wormhole Attack can erode the trust among nodes in the MANET. Nodes may become hesitant to communicate, leading to a breakdown in the collaborative and cooperative nature of the network.

Detecting Wormhole Attacks in MANETs is a challenging task due to their covert nature. Several detection mechanisms have been proposed:

- **Cryptographic Techniques:** Encryption and authentication mechanisms can be employed to secure communication and detect anomalies that may indicate the presence of a wormhole.

- **Timing Analysis:** Analyzing the timing of packet exchanges between nodes can reveal irregularities that may signify the existence of a wormhole. Deviations from expected time intervals can be indicative of an attack.

- **Distance-Based Approaches:** Utilizing distance information, such as the Received Signal Strength Indicator (RSSI), can help detect inconsistencies in the claimed and actual distances between nodes, revealing potential wormholes.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: 10 September 2023 ***Revised:*** 20 October 2023 ***Accepted:*** 30 October 2023

- **Topology Analysis:** Studying the network topology and observing unexpected changes or disruptions can be a signal of a Wormhole Attack. Anomalies in the established routes and connectivity patterns may indicate malicious activity.

This attack involves the deliberate destruction of a specific route in a Mobile Ad hoc Network (MANET) and is a commonly seen security issue in this type of network. A wormhole attack is a type of tunnel attack in which a malicious node intercepts and redirects a specific package to various locations in the network before returning it. This type of attack significantly undermines network functionality and poses a serious threat to network security.

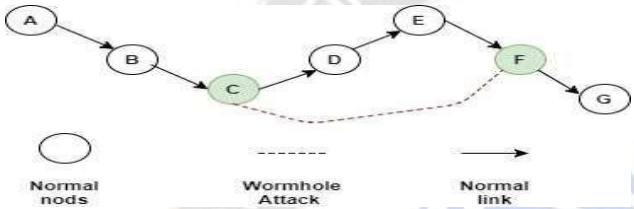


Figure 4 Wormhole Attack

The concept of the attack will be made clear with the following graphic. Firstly, let us consider that we have two networks, named A and B. We assume that one of these networks will initially have a malicious node. Each of these nodes is connected through a link. Specifically, node X in network A and node Y in network B are neighbours and have a secure direct connection between them. Please refer to Figure 5 for a visual representation. This type of assault is considered one of the most advanced forms of attacks in MANET. If the attackers are linked to the normal link instead of the wormhole, they have a flexible environment that allows them to execute wrong instructions.

- The wormhole link refers to a crystallised tunnel established between the attackers.
- This tunnel can be either a wired connection or a high-frequency wireless link (21).

The operational principles of the wormhole attack may be observed in Figure 5 below, and the same procedure is employed for transmitting and receiving packets during the transmission between X and Y.

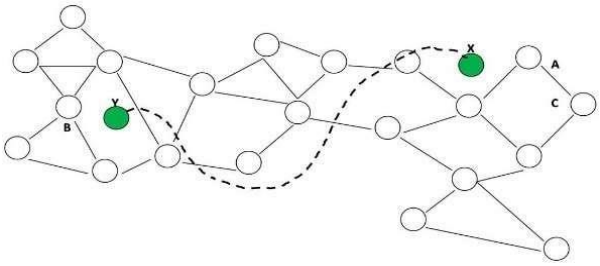
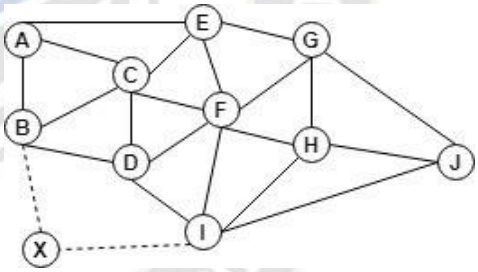


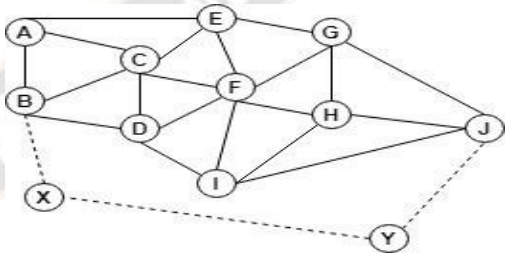
Figure 5 Wormhole Attack

4. AODV AND DSR VULNERABILITY TO WORMHOLE ATTACK

In a wormhole attack, the attacker strategically positions themselves in the network by exploiting the shortest path between nodes. The attacker broadcasts the established route to inform the other nodes of the most efficient path for data circulation. Once the nodes establish a direct connection between one other, the attacker will intercept packets originating from a certain location in the network and encapsulate them using a tunnel to reach another location inside the same network. The packet will then be sent from that location. This is the path to exploit routing protocols of networks. This type of attack poses a significant risk, especially when the network offers confidentiality and security measures.



(a)



(b)

Figure 6: Wormhole Attack in AODV and DSR

AODV and DSR are highly susceptible to wormhole attacks. The assailant can use a wormhole in the network to directly transmit RREQ packets to the destination node. However, if the neighbours of the destination node acknowledge the request, they will promote it and delete all other RREQ packets from the regular node. In cases where routes consist

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

of more than one hop, the attacker can effortlessly generate a packet that bypasses the wormhole link and quickly emerges, as depicted in Figure 6(a). The assailant can employ a comparable method of transmitting the packet incrementally, so diminishing the time of delay, as depicted in Figure 6(b) (21).

5.SIMULATION ENVIRONMENT AND SETTINGS

Figure 7 refers to the advanced wormhole attack model (WHAM) architecture in relation to two routing protocols, namely AODV and DSR. Upon receiving a path request from the IP protocol, the routing protocol initiates the process of identifying routes. In this scenario, WHAM initiates a wormhole assault on a Mobile Ad hoc Network (MANET).

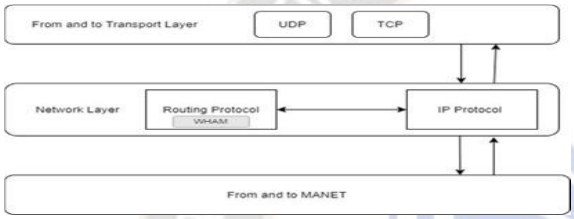


Figure 7: WHAM Architecture

OTcl is a programming extension that adds object-oriented capabilities to Tcl/Tk. NS-2 employs OTcl as a programming language for simulating and creating network objects in memory. NS-2 utilises the ultimate approach, in which the framework file is an OTcl file referred to as the "OTcl simulation Script". The script depicted in Figure 8 includes interpretation Parameters, which specify the composition of Attackers and Radio Range. The network simulation will consist of two routing protocols, namely AODV and DSR. The NS-2 simulation result is stored in a Trace file, which is used by Network Animator (NAM). NAM is an animation tool based on Tcl/TK that displays network emulation traces and authentic packet traces. AWK scripts for NS-2 are used to extract data from trace files. The indicators we analyse in our work are Throughput and End-to-end latency. Ultimately, the results are presented in the form of graphs using Microsoft Excel 2013.

Conducting the experimental simulations. The experimentations were conducted by manipulating one variable, namely the composition of attackers (2, 4, 6, and 8), positioning the attackers in close proximity to the target. This approach facilitated the assessment of the wormhole attack's impact. The CBR message initiates with a traffic load of 2 packets per second from 1.0 second till the simulation ends. The packet size is 1000 bytes and the attacker initiates the simulation at 30 seconds until it ends. The employed mobility model is the arbitrary waypoint model, while the radio propagation model is the two-ray ground reflection model, both used separately.

5.1 Simulation WHAM system components

A wormhole attack is a security threat in wireless networks, particularly in ad-hoc and sensor networks. In a wormhole attack, malicious nodes create a tunnel between two distant points in the network, allowing them to forward packets through this tunnel, bypassing normal network routes. This can lead to various security issues, such as information interception, traffic redirection, and disruption of communication. Simulating a wormhole attack involves modeling the components of the network and the attack itself. Define the topology of the wireless network, including the nodes, their locations, and the communication links between them. Represent the network nodes, which can be either legitimate or malicious. Legitimate nodes communicate with each other, while malicious nodes perform the wormhole attack. Implement the wormhole attack itself. This involves creating a tunnel between two malicious nodes through which they can forward packets. The attack module should be capable of intercepting and redirecting packets to and from the tunnel.

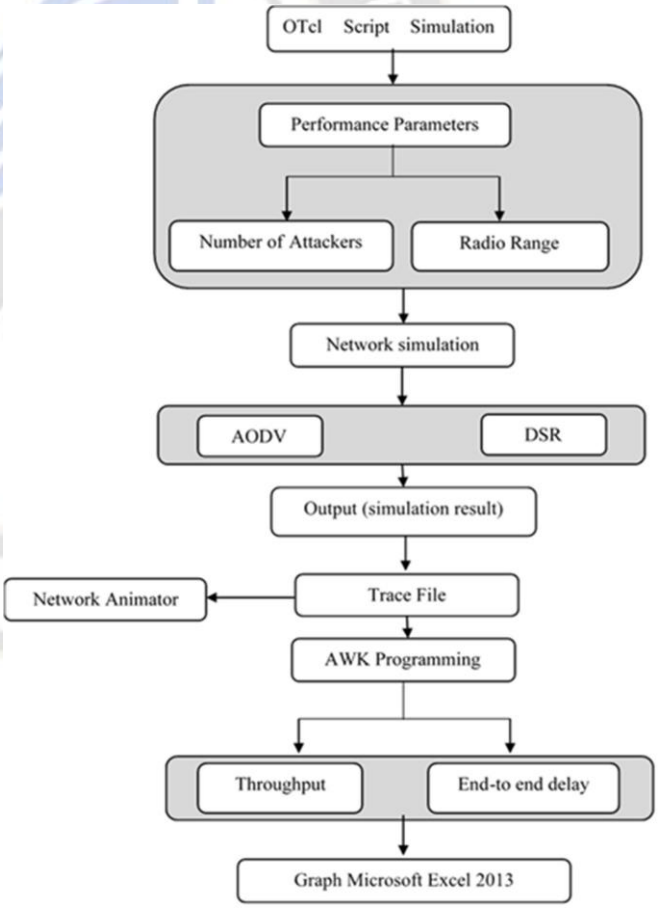


Figure 8: Simulation System Components

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

5.2 Performance metric

Each subsequent evaluation in this study is derived from the average of five trials conducted in the NS-2 experiment. Two performance parameters, namely end-to-end delay and throughput, have been observed for each routing protocol. The following Table 2 presents the node adjuncts that were utilised in our experimentation.

Each subsequent evaluation in this study is derived from the average of 5 experimental runs conducted in NS-2. Two performance parameters, namely end-to-end delay and throughput, have been observed for each routing protocol.

The end-to-end delay refers to the time it takes for a data packet to be transferred to its destination. This refers to any hidden delays that occur during the detection of a route due to the time it takes to store data in a buffer. The criterion for determining the outcome is documented in each experiment.

Throughput refers to the total number of packets successfully delivered for the entire duration of the simulation. It denotes the benchmark for evaluating the throughput values of destinations in each experimental result.

Parameter	Value
Network area	1000m × 1000m
Number of nodes	20
Nodes speed	0 – 7 m/s
Bandwidth	11 mbps
Traffic Packet size	512 bytes
Packet rate	2 packets per second
Traffic type	CBR

6.RESULT AND DISCUSSION

When we altered the composition of worm attack nodes, we found that the AODV protocol exhibited greater intermediate throughput values compared to the DSR protocol. However, the DSR has lower intermediate throughput values. Figure 11 displays the comparison between AODV and DSR. The AODV protocol is shown in red, while the DSR protocol is highlighted in blue.

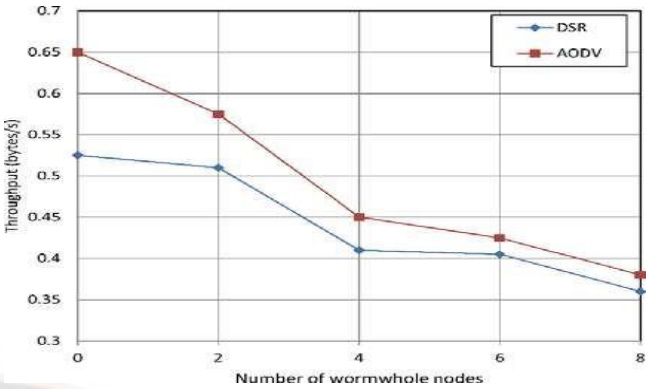


Figure 11: Average Throughput VS Number of Wormhole Nodes

When we alter the composition of worm attack nodes, we observe that the AODV protocol exhibits reduced end-to-end latency values compared to the DSR protocol. Likewise, the DSR exhibits significant latency. The figure 12 below illustrates the comparison between AODV and DSR. The AODV protocol is indicated by a red line, whereas the DSR protocol is indicated by a blue line.

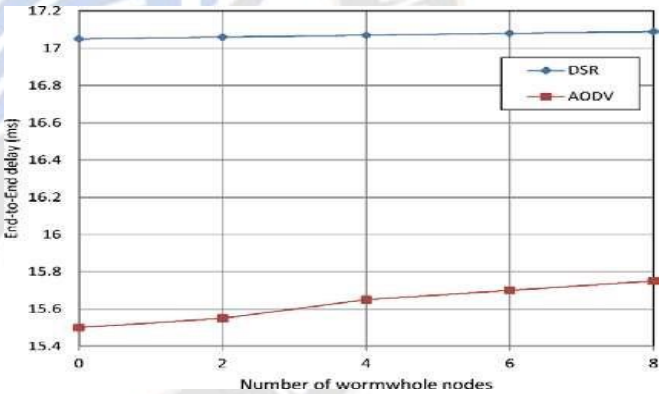


Figure 12: End- To- End Delay vs Number of Wormhole Nodes

The experimental results demonstrate that AODV outperforms DSR. AODV exhibits more efficiency compared to DSR, resulting in higher throughput and shorter end-to-end delay. Dynamic Source Routing (DSR) exhibits vulnerability to wormhole attacks. The results indicate that increasing the radio range across all protocols enhances the throughput and prolongs the end-to-end latency measurements. The results depicted in figure 13 indicate that increasing the evolved radio range leads to a higher throughput. As the radio range increases, it enables the network to enhance its throughput. Figure 13 illustrates the throughput achieved when utilising different radio ranges. The colour red represents the AODV protocol, while the colour blue represents the DSR protocol.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

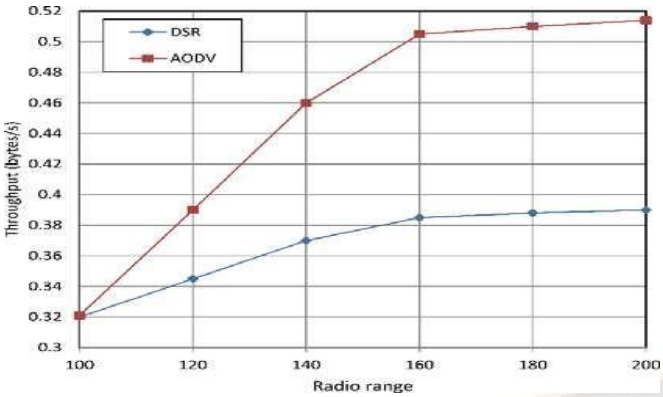


Figure 13: Average Throughput vs Different Radio Range

Regarding the end-to-end delay, we observe that AODV exhibits the least delay compared to DSR. However, as the range rises, DSR has a higher end-to-end delay. Figure 14 illustrates the results of the end-to-end delay when the radio range is adjusted. The AODV protocol is represented by the red line, while the DSR protocol is represented by the blue line.

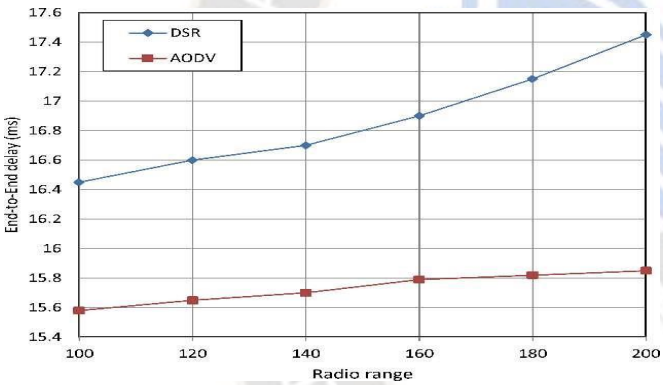


Figure 14: End- To- End Delay vs Different Radio Range

7. CONCLUSION

This study investigated two routing protocols in Mobile Ad hoc Networks (MANET) and introduced a wormhole attack model (WHAM) that generates wormhole nodes within Constant Bit Rate (CBR) traffic. The WHAM was implemented in the AODV and DSR routing protocols using NS2. The two protocols under assault were compared using two network interpretation criteria: throughput and end-to-end delay. The results and their analysis have been presented. As demonstrated in the above figures, AODV exhibited higher levels of throughput and end-to-end delay, and revealed more resilience compared to DSR.

In this study, we did not evaluate the performance of our model using metrics such as jitter, routing overhead, and packet loss rate. In the future, we will evaluate the performance of these protocols based on certain performance criteria and we are preparing for actual deployment.

REFERENCES

[1] A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET: CRC press, NW, USA,2016.

[2] S. Mishra, P. Varshney, S. Choudhary, and R. Purohit, "Performance Evolution of Conventional and Swarm based Routing MethodsinMobileAd-HocNetworks,"in2019 2ndInternationalConferenceonPowerEnergy, Environment and Intelligent Control (PEEIC), 2019, pp.528-531.

[3] Umakant Dinkar Butkar, et.al "Accident Detection and Alert System (Current Location) Using Global Positioning System" JOURNAL OF ALGEBRAIC STATISTICSVol. 13 No. 3 (2022) e-ISSN: 1309-3452.

[4] R. Singh, "An Overview of MANET: Characteristics, Applications Attacks and Security Parameters as well as Security Mechanism,"InternationalResearchJournalof Engineering and Technology (IRJET), vol. 5, pp. 1155-1159,2018.

[5] K. Rajani, P. Aishwarya, and S. Meenakshi, "A review on multicasting routing protocols for mobile ad-hoc wireless networks," in 2016 International Conference on Communication and Signal Processing (ICCSP), 2016, pp. 1045-1052.

[6] R. Sadakale, A. Bhosale, and N. Ramesh, "Performance Analysis of Traffic Types in AODVRoutingProtocolforVANETs,"in2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp.1-5.

[7] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Advanced robotic manipulator renewable energy and smart applications. Computer Integrated Manufacturing Systems, 29(2), 19–31. Retrieved from http://cims-journal.com/index.php/CN/article/view/782

[8] N. Jain, A. Rahman, and A. K. Dubey, "Code Aware Dynamic Source Routing for Distributed Sensor Network," in 2013 International Conference on Communication Systems and Network Technologies, 2013, pp.272-276.

[9] I.-R. R. P.1546, "Method for point-to-area predictions for terrestrial services in the frequency range 30 MHz to 3 000 MHz," International Telecommunication Union Radiocommunication Sector (ITU-R)P.1546-4, 2009.

[10] Butkar Uamakant, "A Formation of Cloud Data Sharing With Integrity and User Revocation",

International Journal Of Engineering And Computer Science, Vol 6, Issue 5, 2017

[11] S. Ali and P. Nand, "Comparative performance analysis of AODV and DSR routing protocols under wormhole attack in mobile ad hoc network on different node's speeds," in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp.641-644.

[12] H.Moudni,M.Er-rouidi,H.Mouncif,andB.El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," in 2016 International Conference on Electrical and Information Technologies (ICEIT), 2016, pp.536-542.

[13] S. Garg, "Performance analysis of AODV and TORA under DDoS attack in MANETs," IJSR International journal of science and research, vol. 3, pp. 297-304,2014.

[14] G. Gupta and A. Mishra, "Simulation Based Study of Cooperative Black Hole Attack Resolution using Cross-Checking Algorithm," International Journal on AdHoc Networking Systems (IJANS), vol. 5, pp.17-28.

[15] S. Ruj and R. Sachdeva, "Analysis of Selfish Node Attack in AODV Routing Protocol using GLOMOSIM," International Journal of Engineering Development and Research, vol.5, pp. 784-789,2017.

[16] Y. Bai, Y. Mai, and N. Wang, "Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs," in 2017 Wireless Telecommunications Symposium (WTS), Chicago, IL, 2017, pp.1-5.

[17] Umakant Butkar, "An execution of intrusion detection system by using generic algorithm",IJIFR, Vol 1, Issue 10, 2014

[18] R. Singh and T. P. Sharma, "Present Status of Distributed Denial of service (DDoS) attacks in internet world," International Journal of Mathematical, Engineering and Management Sciences, vol. 4, pp. 1008-1017,2019. P. Oberoi, S. Mittal, and R. K. Gujral, "ADRCN: A framework to detect and mitigate malicious insider attacks incloud-based environment on IaaS," International Journal of Mathematical, Engineering and Management Sciences, vol. 4, pp. 654-670, 2019.

[19] A. A. Ajibesin, M. M. Kah, A. T. Ishaq, andC. Ajibesin, "Performance Analysis of Topology and Destination Based Routing Protocols in Mobile Ad-Hoc Network Using NS2," in 2019 IEEE 13th International Conference on Application of Information and CommunicationTechnologies(AICT),2019,pp. 1-6.

[20] Umakant Butkar, "A Fuzzy Filtering Rule Based Median Filter For Artifacts Reduction of Compressed Images", IJIFR, Vol 1, Issue 11, 2014

[21] A. Sahoo, A. Shreya, C. S. Dash, I. Priyadarshini, S. Sobhanayak, S. S. Panda, et al., "Performance Evaluation of AODV, DSDV and DSR Routing Protocol For Wireless Adhoc Network," in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN),2018,pp. 348-351.

[22] S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Securing DSR against wormhole attacks in multirate ad hoc networks," Journal of Network and Computer Applications, vol. 36, pp. 582- 592,2013.

[23] E. Hyytiä and J. Virtamo, "Random waypoint model in n-dimensional space," Operations Research Letters, vol. 33, pp. 567-571,2005.

[24] Umakant Butkar, "Review On- Efficient Data Transfer for Mobile devices By Using AdHoc Network", International Journal of Engineering and Computer Science, vol 5, Issue 3, 2016

[25] A. M. Kanthe, D. Simunic, and R. Prasad, "Effects of propagation models on AODV in mobile ad-hoc networks," Wireless personal communications, vol. 79, pp. 389-403,2014.