Periodico di Mineralogia Volume 93, No. 4, 2024
ISSN: 0369-8963

Analysis and simulation of wormhole attack in wireless sensor networks using NS3 simulation Tool

Mr Prashanth K
Master of Computer Applications
RV College of Engineering
Bangalore, India

Bharath Ramesh H
Master of Computer Applications
RV College of Engineering
Bangalore, India

Abstract*—Wireless sensor networks (WSNs) and ad-hoc networks are increasingly popular due to their ability to solve complex problems and advancements in technology that enable smarter and denser networks. Security in these networks is crucial, particularly when sensors operate in hostile environments. Wormhole attacks pose a significant threat as they can be initiated without compromising sensor bypassing cryptographic defenses. This paper analyzes and simulates wormhole attack in WSN using the NS3 simulation tool, focusing on the AODV routing protocol and TCP for data transmission. Our study proposesa method to detect wormhole attacks and evaluate their impact on network performance, utilizing network connectivity information without relying on specialized measurements.

IndexTerms*—wireless sensor networks, wormhole attack, security, NS3 simulation, AODV protocol, TCP protocol

1. INTRODUCTION

Wireless sensor networks include geographically dispersed, independent sensors that keep an eye on conditions, either environmental or physical, and send them to the central system. Due to their versatility and efficiency, There are numerous uses for these networks,from environmental monitoring to military surveillance. Wireless, detecting, and processing sensor nodes communication capabilities make up wireless sensor networks. that enable data collection over a wide area. However, their deployment in potentially hostile environments and reliance about wireless communication make them vulnerable to security threats,particularly wormhole attacks. In this type of attack, attackers create low-level connections by sending packets between locations, disrupting communications and transactions without affecting sensor nodes or cryptography protection.

The general Structure of WSN is as follows:

Wireless Sensor Networks play a critical role in monitoring and transmitting environmental and physical data across various applications due to their versatility and efficiency.

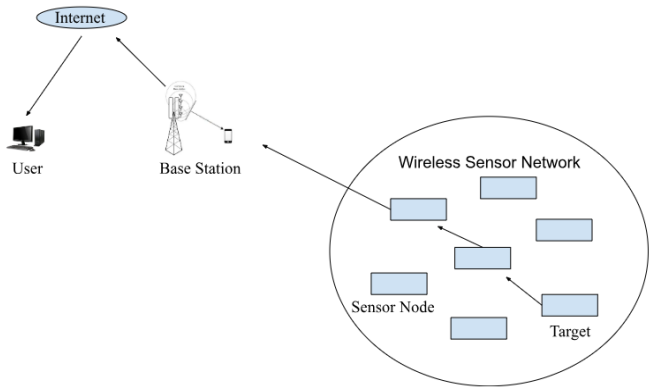

Fig 1. Wireless sensor network Structure

Wireless Sensor Networks play a critical role in monitoring and transmitting environmental and physical data across various applications due to their versatility and efficiency. However, securing these networks against sophisticated attacks like

 https://doi.org/10.5281/zenodo.13355058

wormhole attacks remains a significant challenge that requires ongoing research and innovative solutions.

1.1 Wormhole Attack Description

Significance of wormhole attack

A wormhole attack is a severe security threat in wireless sensor networks where an adversary exploits the networks communication protocols to create a deceptive link between two distant nodes. In this attack, packets from one area of the network is captured by the attacker and tunneled to another, often remote, part of the network through a malicious link, which appears to hold the position of valid communication path. This artificial link, known as the "wormhole," can mislead the network's routing mechanisms and disrupt normal data transmission.

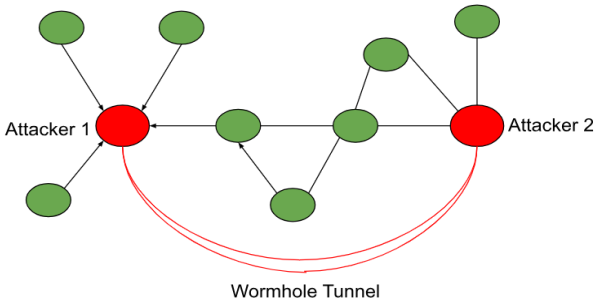

Fig 2.Wormhole attack in WSN

In Wireless Sensor Networks a wormhole attack is a strategy where an attacker establishes a covert link between two remote nodes to tunnel data packets. This deceptive link misguides the network's routing protocols, causing packet misrouting, increased delays, and overall network inefficiency. The attack is difficult to detect since it doesn't require physical alterations or bypassing of encryption.

1.2 Modes of wormhole attack

This section provides a detailed explanation of the several ways that wireless sensor network wormhole attacks might be executed. There are numerous approaches to this, some of which are covered in this particular section.

Packet Encapsulation

In the packet encapsulation mode, attackers capture single-node packets, encapsulate them, and forward them through a wormhole to another node. This creates a deceptive path that misleads protocols for routing and causes data misrouting.

Packet Relay

In the packet relay mode, attackers relay data packets bidirectionally between two distant nodes via a wormhole. This manipulation disrupts normal routing paths, causing network congestion and performance issues.

High Power Transmission

High Power Transmission in Wireless Sensor Networks (WSNs) refers to the use of increased transmission power to extend the range of communication between nodes. While it can improve signal strength and network coverage, it also introduces potential vulnerabilities and considerations for network performance and security.

out of Band

The out-of-band channel mode uses a separate communication channel, like a different frequency or wired link, to tunnel packets between nodes. This hidden method creates an undetectable wormhole that affects network traffic.

2 RELATED WORK

2.1 Literature survey

Wormhole attacks have been a significant concern in Wireless sensor networks due to their potential to severely disrupt network communication. These attacks create a low-latency link between two or more malicious nodes, allowing for manipulation of the network's routing information. The literature

https://doi.org/10.5281/zenodo.13355058

listed below offers information on different methods of wormhole attack detection and prevention.

Mousam A. Patel.[1] Provides a comprehensive analysis of the characteristics of wormhole attacks and their impact on WSNs. The authors discuss various detection techniques and emphasize the significance of implementing security mechanisms across various network protocol layers.

Mohit Kumar Verma.[2] Reviews existing techniques for detecting and preventing wormhole attacks. It classifies these techniques based on different parameters, such as timing, location, and connectivity, and discusses their strengths and limitations.

Manish M Patel .[3] Authors propose a two-phase method for identifying wormhole assaults in dynamic WSNs. The initial stage Involves the recognition of suspicious nodes using neighborhood information, while the second phase confirms the existence of a wormhole through detailed analysis.

2.11 Detection methods

Detection methods have focused on improving accuracy and reducing the additional computing burden related to determining wormhole attacks in WSNs.

Packet Leashes: Packet Leashes are a technique used to combat several kinds of network attacks, including wormhole attacks. They help ensure that packets travel within expected time and distance bounds to detect and prevent malicious activities.

Round-Trip Time (RTT) is the duration how long does a packet take to get from a sender to a receiver and back again. It is an essential measure for assessing network efficiency and detecting anomalies like wormhole attacks.

Shaurya Verma.[4] Wormhole Detection Using Zonal Security Nodes in wireless sensor networks (2021):

This method uses zonal security nodes to monitor wormhole attacks by assigning one node per network zone to collect and analyze data for suspicious patterns. Its main strength is localized detection, which distributes the detection load across the network. Proper placement and configuration each of these nodes is essential for balancing network efficiency and detection accuracy.

Rajendra Kumar Dwivedi.[5] Detection and prevention analysis of wormhole attack in Wireless sensor network(2022):

The author [5] examines various Identification and mitigation of wormhole attacks strategies and proposes a hybrid strategy that combines several methods to enhance robustness and accuracy. This approach leverages the strengths of different techniques to offer a flexible and comprehensive solution for diverse network scenarios.

K´aroly Hars´any.[6] Wormhole detection in wireless sensor networks using spanning Trees(2023):

In this strategy, nodes identify attacks via wormholes by periodically exchanging an information about their spanning tree architectures and evaluating differences between expected and actual tree structures. The method's efficiency and scalability stem from leveraging existing network topologies for detection.

Mariano García-Otero.[7] Detection of wormhole attacks in wireless sensor networks using Range-Free Localization(2024):

The authors present a range-free localization method in order to identify wormhole assaults by analyzing node relative positions instead of exact distance measurements. This technique identifies anomalies by examining relative positions, which is advantageous for resource-limited Wireless Sensor Networks as it requires no extra hardware.

2.12 Prevention methods

 https://doi.org/10.5281/zenodo.13355058

Prevention methods have evolved to incorporate more sophisticated techniques, ensuring that WSNs can effectively mitigate the risks posed by wormhole attacks.

Secure routing protocol

Directly integrating security procedures into the method of routing effectively prevents wormhole attacks by making it more difficult for adversaries to construct bogus routes. Nevertheless, this method may add more overhead and complexity to the routing protocol, requiring a careful balancing act between improving security and preserving performance effectiveness.

Mayank Kumar Sharma.[8] A mitigation technique for high transmission power based wormhole attack in Wireless Sensor Networks (2020):

By controlling node transmission power to prevent high-power wormhole linkages, this method reduces the result of wormhole attacks. It effectively limits attackers ability to establish the false connections by confining nodes to a specific power range.

3 PROPOSED MODELLING

The simulation of the detection of wormhole attacks in wireless sensor networks (WSNs) is conducted using NS-3 for its capability to model complex network scenarios. A mesh topology of sensor nodes is used, with transmission power and range configured to mimic real WSN conditions. The Routing using On-Demand Distance Vectors (AODV) protocol is chosen because of its common use and vulnerability to wormhole attacks. Several detection techniques, such as graph-based anomaly detection, packet leash methods, and time-of-flight measurements, are applied and evaluated based on measures such as end-to-end delay and packet delivery ratio, and false positive rate to improve WSN security against wormhole attacks.

Network Simulation Setup

A wireless sensor network is configured by the simulation (WSN) with a mesh topology using NS-3,setting parameters like mobility, communication range, and transmission power for realistic conditions.

3.1 Routing protocol

The simulation uses the fact that wireless sensor networks frequently employ the Ad Hoc On-Demand Distance Vector (AODV) routing technique (WSNs) and susceptibility to wormhole attacks. AODV is a reactive protocol that creates routes only as needed, minimizing overhead compared to proactive protocols. It uses sequence numbers to maintain up-to-date routes and prevent loops. As soon as a route is needed, a node broadcasts a route request (RREQ), which is propagated until the destination or an intermediate node with a valid route is found.

Wormhole attack simulation in ns3

To ensure that a wormhole attack can be executed in NS-3, two malicious nodes must be simulated to construct a tunnel and control network traffic. The purpose of this configuration is to determine how susceptible wireless sensor networks are to these kinds of attacks and how successful detection methods are. This is a succinct methodology.

Network Topology Configuration: Nodes are arranged in a mesh topology. Every node is configured with specific parameters like transmission power and communication range to reflect realistic conditions.

Routing Protocol Setup: Since the Routing using Ad Hoc On-Demand Distance Vectors (AODV) protocol is vulnerable to wormhole attacks and is frequently employed in WSNs, it is put into practice.

Malicious Node Configuration: The network features two nodes with been flagged as malicious. These nodes don't behave in accordance with the

 https://doi.org/10.5281/zenodo.13355058

norm for routing protocols. Rather, they provide a direct conduit or relationship between them.

Wormhole Link Creation: By capturing packets in one location and replaying them at a different location via the tunnel, the malicious nodes provide the impression that a quicker route exists within the network.

Traffic Manipulation: By altering data packets and routing information, the wormhole link deceives other network nodes into thinking that the malevolent nodes are the quickest path between two places.

Simulation Parameters: Node mobility, traffic patterns, and network density are some of the variables that the simulation takes into account. To determine how the wormhole attack would affect various scenarios, several conditions are generated.

Data Gathering and Analysis: Data is gathered on metrics like package delivery ratio, end-to-end latency, and routing overhead. The attack-prone network's performance is contrasted with the unaffected baseline.

Detection Methods: Use NS-3's time-of-flight measurements, packet leash approaches, and graph-based anomaly detection to test the efficacy of these detection mechanisms in locating and thwarting wormhole attacks.

3.2 Analysis of wormhole attack

Analyzing a wormhole assault on a Wireless Sensor Network (WSN), the main goals are to determine how the attack affects network performance and how well detection and mitigation techniques work. This examination, which is usually carried out using simulations, includes a number of crucial elements:

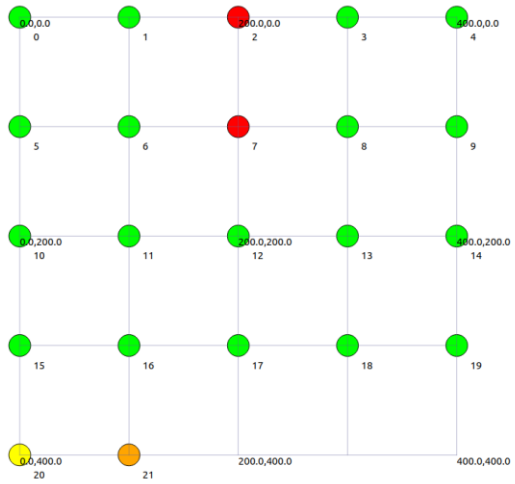

Fig3. Wormhole attack Setup

In this simulation, the consequences of a wormhole attack on a Wireless Sensor Network (WSN) are investigated using the Ad hoc On-Demand Distance Vector (AODV) routing protocol. with 22 nodes. The network is configured with different nodes assigned different functions to be able to mimic an attack and track various network performance indicators.

Roles within the Network and Node Configuration

Regular Nodes:

- **Color:** Green
- **Count:** 20 nodes
- **Role:** These nodes represent the standard WSN environment and perform routine network functions such as data transmission and routing.

Wormhole Attackers:

Attackers 1:

- **Node Number:** 2
- **Color:** Red
- **Role:** This node functions as one of the wormhole tunnels, capturing packets from one end and sending them to the appropriate section

https://doi.org/10.5281/zenodo.13355058

of the network at the at the other end of the tunnel.

Attacker 2:

- **Node Number:** 7
- **Color:** Red
- **Role:** This node serves as the other end of the passage through worms, forwarding packets received from Attacker 1 to the final location or back to the network.

Start Node :

- **Node Number:** 20
- **Color:** Yellow
- **Role:** This node initiates data transmissions, sending packets through the network to the sink node.

Sink Node :

- **Node Number:** 21
- **Color:** Orange
- **Role:** This node obtains packets of data from the start node and acts as the final destination for all network traffic.

3.3 The first phase of wormhole attack communication

A wormhole attack is made possible when nodes find and join neighboring nodes during the network's early communication phase. To locate additional nodes that are within its transmission range and verify bidirectional connectivity, each node broadcasts "Hello" or dummy packets. These are placeholder packets used by attackers in wormhole attacks to construct a false tunnel between remote network areas. This alteration affects routing decisions and reports distances incorrectly. Unintentionally, network nodes that get these packets and reply with acknowledgments create linkages via the wormhole tunnel. This first exchange aids in creating a local topology map.

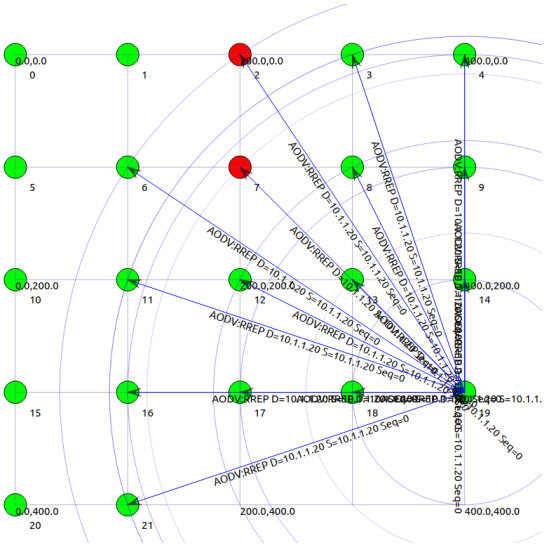

Fig 4. Simulation Working

3.4 Interpret Results for Wormhole Attack

Impact on Power Parameters

Increased Communication Overhead: Malicious nodes establish a false connection across far-flung network locations during a wormhole attack. The network has to control the false relationships that arise from this manipulation, which increases communication overhead. Nodes use more energy handling bogus routing information and directing packets through the wormhole tunnel.

Routing Inefficiencies: By reducing the perceived distance between nodes, the wormhole attack leads routing systems to make less-than-ideal judgments. Consequently, there are inefficient routing paths that cause legitimate nodes to use more energy while processing and forwarding packets via these longer routes.

Higher Energy Consumption: More computing power is required to check the legitimacy of routes, and more packet forwarding is involved in addressing the wormhole attack. This causes the processing and communication demands to grow, which accelerates the depletion of batteries in real nodes.

4 RESULTS AND DISCUSSIONS

https://doi.org/10.5281/zenodo.13355058

4.1 Graphical Representation

Plotting the change in residual energy over time for every node in a simulated wireless sensor network allows one to assess the effect of a wormhole assault. The simulation time in seconds is shown on the x-axis, while the amount of energy left is shown on the y-axis. At first, every node begins with similar energy levels, which decrease due to network activities. Sharp declines at certain intervals indicate high activity influenced by wormhole nodes, followed by stabilization phases.

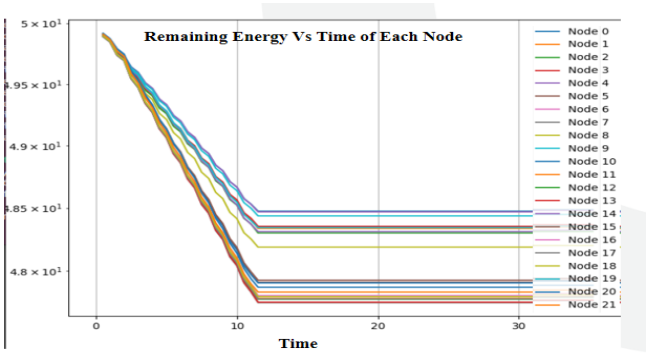

Fig 5 . energy consumption graph

4.2 Initial high activity phase

The graph Remaining Energy vs. Time for Each node depicts the amount of energy used by patterns of 22 nodes in a wireless network over a 50-second simulation period. Initially, all nodes have an energy level of 50 joules. During the first 10 seconds, there is a sharp decline in energy levels for all nodes. This steep drop indicates high activity and substantial energy usage, likely because of the network setup and initial data transmissions. This phase represents the network's intensive operation period.

4.3 Stabilization phase

After the initial 10 seconds, the energy consumption rate stabilizes for most nodes. This stabilization phase shows a much slower rate of energy decline, suggesting that the network transitions into a steady state. In this phase, the operations are less energy-intensive compared to the initial setup. The steady state is characterized by regular, ongoing network activity that consumes energy at a more consistent and lower rate. This phase reflects the routine operation of the network after the initial burst of activity.

4.4 Variations in Node Energy Consumption

Differences in energy levels among nodes increase in apparent magnitude after stabilization. Some nodes exhibit somewhat more energy usage than others, indicating varied roles or activities within the network. Nodes involved in more frequent data handling or relaying, especially those under attack conditions, show more significant energy depletion.

6 CONCLUSION

The study Analysis of Wormhole Attack Detection in Wireless Sensor Networks Using NS3 Simulation Tools aims to solve the grave problem of wormhole attacks, which compromise network integrity by establishing fictitious communication channels. Through the use of mesh topology in NS-3 simulations, the work leverages the redundancy of topology to help identify these attacks more effectively. Even though there are difficulties with some NS-3 features, a methodical approach guarantees comprehensive testing at every stage. The goal of this research is to create reliable detection techniques that will improve wireless sensor network security and dependability.

7 ACKNOWLEDGMENT

This work was supported by the Intelligent information processing research team of R. V. College of Engineering.

REFERENCES

[1] M. K. Verma and R. K. Dwivedi, "A Survey on Wormhole Attack Detection and Prevention Techniques in Wireless Sensor Networks," *2020*

https://doi.org/10.5281/zenodo.13355058

International Conference on Electrical and Electronics Engineering (ICE3), Gorakhpur, India, 2020, pp.326-331.

[2] M. M. Patel and A. Aggarwal, "Two phase wormhole detection approach for dynamic wireless sensor networks," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2016, pp. 2109-2112.

[3] S. Verma, S. Arora and A. Rawat, "Wormhole Detection using Zonal Security Nodes in Wireless Sensor Networks," *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, Ghaziabad, India, 2023, pp. 353-358.

[4] R. Kumar Dwivedi, P. Sharma and R. Kumar, "Detection and Prevention Analysis of Wormhole Attack in Wireless Sensor Network," *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2018, pp. 727-732

[5] K. Harsányi, A. Kiss and T. Szirányi, "Wormhole detection in wireless sensor networks using spanning trees," *2018 IEEE International Conference on Future IoT Technologies (Future IoT)*, Eger, Hungary, 2018, pp. 1-6.

[6] M. García-Otero and A. Población-Hernández, "Detection of wormhole attacks in wireless sensor networks using range-free localization," *2012 IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Barcelona, Spain, 2012, pp. 21-25.

[7] M. K. Sharma and B. K. Joshi, "A mitigation technique for high transmission power based wormhole attack in Wireless Sensor Networks," *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, India, 2016, pp. 1-6.

[8] P. S. Rathore and M. K. Sarkar, "Defending Against Wormhole Attacks in Wireless Networks Using the Twofish Algorithm: A Performance Analysis," *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2024, pp. 0583-0588

[9] W. A. Aliady and S. A. Al-Ahmadi, "Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks," in *IEEE Access*, vol. 7, pp. 84132-84141.

Author 1

Mr. Prashanth K. Assistant Professor, Department of Master of Computer Application, affiliated to Visvesvaraya Technological University, Belagavi, had completed a master degree at Sidhganga Institute of Technology in the year 2006, pursuing a PhD in Visvesvaraya Technological University, Belagavi. Specialization on wireless sensor networks, cloud computing, and cloud native full stack application development.

Author 2

Bharath Ramesh H, Persuing a Master of Computer Applications in RV College of Engineering Bangalore, completed Bachelor of Science in Sarada Vilas College, Mysuru.

 https://doi.org/10.5281/zenodo.13355058