A THEORETICAL FRAMEWORK FOR EVALUATING MISDIRECTION ATTACKS IN WIRELESS SENSOR NETWORKS USING NETWORK PERFORMANCE METRICS

Namrata D. Sohaney
namrata.sohaney@gmail.com

Anupama D. Sakhare
Department of Electronics and Computer Science, R.T.M. Nagpur University, Nagpur, India
adsakhare616@gmail.com

Abstract
Wireless Sensor Networks (WSNs) will always be a major component in any sort of IoT application, enabling energy-efficient and autonomous data collection in diverse environments. However, the openness and limited resources of WSNs make them vulnerable to routing-based attacks. Among these, misdirection attacks disrupt routing paths by deceiving nodes with false route information, leading to performance degradation. This paper proposes a theoretical framework to assess the impact of misdirection attacks on network behavior, using key metrics such as energy consumption, throughput, packet loss, and average end-to-end delay. Formulas for each metric are presented, providing a quantifiable basis for identifying attack effects and informing future defense strategies.

***Keywords**: Wireless Sensor Networks, IoT Security, Misdirection Attack, Network Layer, Performance Metrics, Energy Consumption, Throughput, Packet Loss, Delay*

I. Introduction

Wireless Sensor Networks (WSNs) are composed of small, resource-constrained sensor nodes deployed to monitor and transmit data about physical environments. They are a key component of IoT applications in areas such as environmental monitoring, smart cities, and industrial automation. Despite their utility, WSNs face unique security challenges especially at the network layer where routing protocols guide data transmission.

Misdirection attacks represent a class of routing-layer threats where attackers deliberately alter the routing paths by sending false information. These actions can lead to inefficient routing, data loss, increased energy usage, and degraded service quality. This research establishes a theoretical framework to evaluate the impact of such attacks through standard network performance metrics.

A malicious node can disrupt a reliable route of packets from the Source to destination, resulting in data loss. Increased energy consumption and degraded network performance.

In this paper, we have discussed about evaluation of given performance parameter like Energy consumption, throughput, packet loss and end to end delay.

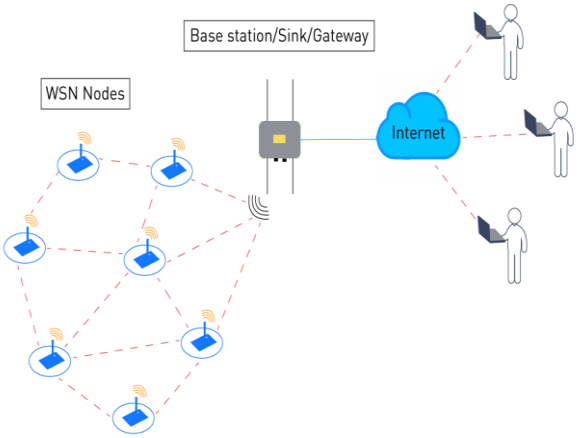

Figure 1: Structure of Wireless Sensor Networks (WSN)

II. Literature Review

- Akyildiz, I.F. et al. (2002) This paper describes that , realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required. The communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored. Open research issues for the realization of sensor networks are also discussed
- Urvashi Dhaked et al (2021) The propose paper explain that, malicious nodes may join WSN because they are self configuring network. Sink hole attack spoof the

identification of malicious nodes which affect network performance. impact of sinkhole attack is shown in form of throughput, packet loss and energy consumption. The paper described that, a malicious nodes in network was identified as one that increase the maximum delay in time.

- Bhavkanwal Kaur, Puspendra Kumar Pateriya (2018) Misdirection attack degrades the throughput of the net- work and increases the delay in the network, as a result devastating the performance of the network. The proposed technique for detection and prevention of misdirection attack.
- Mirza Abdur Razzaq et al (2017) In their paper, the security requirement is discussed such as confidentiality, integrity and authentication. In this survey, different types of attacks are categorized as low-level attack, medium-level attack, high-level attack and extremely high-level attacks along with their nature/ behavior as well as suggested solution to encounter these attacks are discussed.
- Zarana Shah et al (2016) In their proposed paper explain that WSN are vulnerable to different kind of attack. Misdirection attack is type of dos attack in which malicious node misdirect the packet to the other node. So, it reduces network throughput and also increase end to end delay. Their paper suggest that to select highest energy level node is selected as cluster head.
- Laith Farhan et al (2021) The proposed paper state that main aim of any energy-efficient strategy is to keep the sensor nodes alive for longer and thus lengthen the network lifetime. in that survey paper, their goal is to introduce the research trends and recent work on the use of IoT technology, key enabling technologies, various sources of energy wastage and different solutions have been mentioned in the literature.

III. Misdirection Attacks in WSNs

Misdirection attacks target the routing mechanism of WSNs. These attacks manipulate the path that packets take from source to destination by advertising fake routes or metrics. The attacker may drop packets, forward them to non-optimal paths, or create loops to waste network resources. These behaviors degrade Quality of Service (QoS) and drain node energy, affecting the overall system reliability.

How Misdirection Attacks Occur at the Network Layer At the network layer, routing protocols like AODV, DSR, RPL, and LEACH are responsible for route discovery and maintenance. Misdirection attackers exploit these protocols, where malicious nodes advertise false routing protocols to mislead data packets. Instead of reaching the intended sink node, these packets are redirected to incorrect paths, causing delay, drop packets or interception by the attacker.

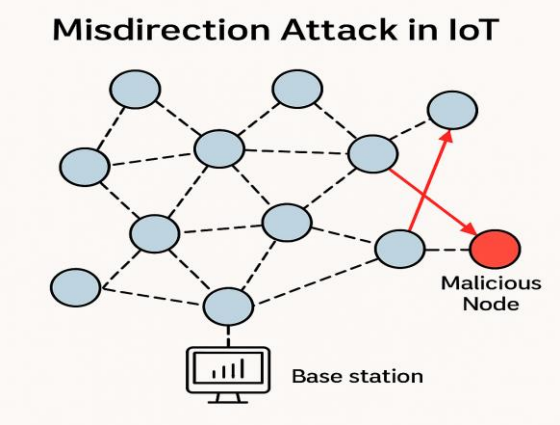

Figure 2: Misdirection Attacks Occur in IoT

Energy Challenges in IoT Based WSN Deployments

WSN consists of multiple sensor nodes that are distributed spatially within a network environment. Sensor nodes are often powered by batteries, and these nodes can only operate for a limited period of time. Sensor nodes that process and transmit data are energy-consuming. The greater distance between nodes, the higher energy consumption. This degrades the lifespan of the network. To enhance the lifespan of the network by balancing path reliability and energy efficiency, which results in one of the most crucial issues for Wireless Sensor Networks (WSNs).

IV. Performance Metrics and Theoretical Formulations

The proposed work is evaluated by using of given performance parameter like Energy consumption, throughput, packet loss and end to end delay

Energy Consumption

Definition: Energy consumed by nodes during transmission, reception, and idle states.

Formula:

$E_{total} = \Sigma (E_{tx} + E_{rx} + E_{idle})$

Where:
- E_{tx}: Transmission energy
- E_{rx}: Reception energy
- E_{idle}: Energy in idle state
- N: Total number of nodes

Misdirection attacks increase energy usage by prolonging routes or triggering unnecessary transmissions.

Throughput
Definition: Number of packets received successfully over time.

Formula:
Throughput = P_recv / T_total

Where:
- P_recv: Packets received
- T_total: Total observation time

Misdirection attacks reduce throughput by causing packet drops or rerouting to incorrect destinations.

Packet Loss Rate
Definition: Ratio of lost packets to total packets sent.

Formula:
Loss Rate (%) = ((P_sent - P_recv) / P_sent) * 100

Misdirection often results in packets being lost in transit or dropped intentionally by malicious nodes.

Average End-to-End Delay
Definition: Average time taken for a packet to travel from source to destination.

Formula:
Delay_avg = (1 / P_recv) * Σ (t_arrival - t_send)

Routing loops and detours introduced by attackers contribute to increased delay.

Analytical Discussion
The mathematical evaluation of performance parameters under misdirection attacks highlights their disruptive nature. Energy consumption rises due to inefficient paths. Packet loss occurs either through intentional drops or forwarding to void nodes. Throughput declines while delays increase, undermining time-sensitive IoT applications. These impacts collectively hinder network lifetime and reliability. The higher energy consumption that degrades the lifespan of the network.

Conclusion
In the Proposed paper, theoretical study outlines a framework to understand how misdirection attacks affect WSNs using measurable network metrics. Quantitative formulas offer a base for evaluating network degradation and designing anomaly detection systems. The findings help in developing proactive defenses for maintaining secure, high-performance IoT environments.

References

1. Akyildiz, I.F. et al., 'Wireless Sensor Networks: A Survey,' Computer Networks, 2002.
2. Bhavkanwal Kaur , Puspendra Kumar Pateriya “Security Framework For Detection And Prevention Of Misdirection Attack In Wireless Sensor Networks For IOT” International Journal Of Engineering Trends And Applications (IJETA) – Volume 5 Issue 5, Sep-Oct 2018
3. Urvashi Dhaked , Dr. Ashok Kumar , Dr. Brajesh Kumar Singh “Detection And Isolation Technique For Sinkhole Attack In WSN” Volume 23, Issue 10, October – 2021
4. Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah “Security Issues In The Internet Of Things (Iot): A Comprehensive Study” (IJACSA) International Journal Of Advanced Computer Science And Applications, Vol. 8, No. 6, 2017
5. Zarana Shah, Ridhi Patel “MISDIRECTION ATTACK IN WIRELESS SENSOR NETWORK: A SURVEY” International Journal for Technological Research In Engineering Volume 3, Issue 9, May-2016
6. Laith Farhan, Rasha Subhi Hameed, Asraa Safaa Ahmed, Ali Hussein Fadel, Waled Gheth, Laith Alzubaidi, Mohammed A. Fadhel and Muthana Al-Amidie “Energy Efficiency for Green Internet of Things (IoT) Networks: A Survey” https://doi.org/10.3390/network 1030017 Network 2021, 1, 279–314
7. Alrajeh, N., et al., 'Intrusion Detection in Wireless Sensor Networks: A Survey,' IJDSN, 2013.
8. Buttyán, L. and Schaffer, P., 'Security in Wireless Sensor Networks,' Technical Report, 2006.
9. Wang, Y., et al., 'Trust-Based Routing for Wireless Sensor Networks,' ACM Transactions, 2016.
10. Shelby, Z., et al., 'RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,' RFC 6550, IETF, 2012.
11. Er. Himanshi Vashisht, Sanjay Bharadwaj, Sushma Sharma “ Detection & Isolation Of Malicious Nodes In A WSN Using LEACH Protocol” Volume 3, Issue 6, July-August-2018
12. SONAM LATA, SHABANA MEHFUZ, AND SHABANA UROOJ “Secure And Reliable WSN For Internet Of Things: Challenges And Enabling Technologies” IEEE Access VOLUME 9, 2021.
13. Reenu, Amarvir Singh “Detection And Isolation Of Malicious Nodes For Selective Forwarding Attack In Wireless Sensor

Network" International Journal Of Computer Sciences And Engineering Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

14. Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal And Biplab Sikdar "A Survey On Iot Security: Application Areas, Security Threats, And Solution Architectures" IEEE Access VOLUME X, 2019
15. Gaurav Sharma, Stilianos Vidalis, Niharika Anand , Catherine Menon And Somesh Kumar "A Survey On Layer-Wise Security Attacks In Iot: Attacks, Countermeasures And Open-Issues" Electronics 2021, 10, 2365