
MISDIRECTION ATTACK IN IOT-WSNS: A THREAT TO SMART CONNECTIVITY

Namrata D. Sohaney

Email - namrata.sohaney@gmail.com

Anupama D. Sakhare

Department of Electronics and Computer
Science

R.T.M. Nagpur University, Nagpur, India

Email : adsakhare616@gmail.com

Crossref DOI – <https://doi.org/10.63665/rh.v7i2.43>

Abstract :

The rapid evolution of the Internet of Things (IoT) has enabled large-scale interconnection of sensing devices for intelligent data-driven applications. Wireless Sensor Networks (WSNs) form the backbone of many IoT systems by enabling distributed sensing and multi-hop data communication. Despite their advantages, IoT-enabled WSNs suffer from inherent security weaknesses due to limited energy, processing capabilities, and the use of open wireless communication channels. One critical routing-layer threat is the misdirection attack, in which compromised nodes deliberately forward packets along incorrect paths. Such behavior disrupts data delivery, increases latency, and accelerates energy depletion, thereby degrading smart connectivity. This paper presents a focused analytical study of misdirection attacks in IoT-WSNs, examining their operational mechanisms, impact on network performance, and existing defense strategies. The study highlights the necessity of lightweight, energy-efficient, and trust-aware security solutions for ensuring reliable smart connectivity in future IoT-WSN deployments.

Keywords : Internet of Things, Wireless Sensor Networks, Misdirection Attack, Smart Connectivity, Network Layer Security

Introduction :

The Internet of Things (IoT) has emerged as a revolutionary paradigm that enables physical objects to sense, process, and exchange data through interconnected networks. By integrating sensing devices with communication technologies, IoT supports intelligent monitoring, automation, and data-driven decision-making across domains such as healthcare, agriculture, industrial automation, smart cities, and energy management.

Wireless Sensor Networks (WSNs) serve as a foundational building block of IoT systems. A typical WSN comprises a large number of sensor nodes deployed over a geographical area to monitor environmental conditions and forward the collected information to a sink or base station using multi-hop communication. Although the integration of WSNs with IoT improves scalability and flexibility, it also introduces significant security challenges. Sensor nodes operate under strict constraints in terms of energy, memory, and processing power, and data transmission often occurs over unsecured wireless channels.



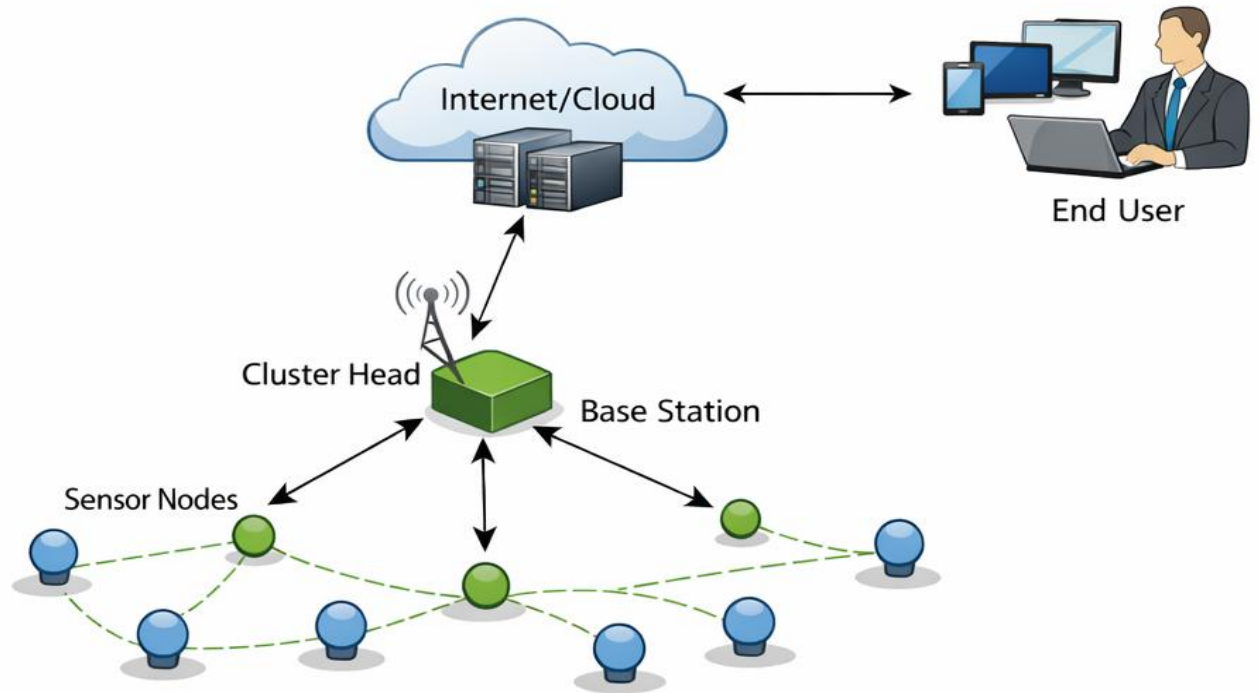


Figure 1: Architecture of Wireless Sensor Networks

This figure illustrates a typical WSN architecture consisting of sensor nodes, cluster heads, sink nodes, and the IoT gateway that connects the sensor network to cloud services.

These limitations make IoT-WSNs particularly vulnerable to routing-layer attacks. One such attack is the misdirection attack, in which malicious nodes intentionally manipulate packet forwarding paths, diverting data away from legitimate destinations. This behavior leads to packet loss, increased latency, excessive energy consumption, and degradation of overall network performance. This paper provides a systematic analysis of misdirection attacks in IoT-WSNs and investigates their impact on the reliability and efficiency of smart connectivity.

Related Work :

Several studies have investigated security challenges in IoT and WSN environments.

- Hassija *et al.* (2019) analyzed security threats across different layers of IoT architectures and discussed emerging technologies aimed at improving trust in IoT applications.
- Razzaq *et al.* (2017) presented a comprehensive survey of IoT security requirements, including confidentiality, integrity, and authentication, and classified attacks into multiple levels based on their severity and behavior.
- Butun *et al.* (2019) categorized IoT attacks into passive and active attacks and highlighted how different attacks target specific layers of the IoT architecture. The authors also discussed open security challenges and possible countermeasures.
- Sonam Lata *et al.* (2021) explored security requirements and threats in WSN-based IoT

architectures, analyzing attacks at different layers and emphasizing the increased risk when WSNs and IoT are integrated.

- Farhan *et al.* (2021) focused on energy-efficient strategies in IoT-WSNs, identifying sources of energy wastage and surveying solutions to prolong network lifetime.
- Sethi and Sarangi (2017) provided a detailed taxonomy of IoT technologies based on layered architectures and reviewed a wide range of IoT applications. Although these works address IoT and WSN security broadly, misdirection attacks at the routing layer require further focused analysis, which this paper aims to provide.
- Zarana Shah and Patel (2016) analyzed the vulnerability of Wireless Sensor Networks (WSNs) to various security threats and identified misdirection attacks as a form of denial-of-service attack in which malicious nodes redirect packets to incorrect destinations. This behavior reduces network throughput and increases end-to-end delay, and their study suggests selecting nodes with higher residual energy as cluster heads to mitigate the impact of such attacks.
- Urvashi Dhaked *et al.* (2021) focused on sinkhole attacks in self-configuring WSNs, explaining how malicious nodes spoof identities to attract network traffic and degrade performance. Their results show that sinkhole attacks increase packet loss, energy consumption, and transmission delay, and they propose identifying malicious nodes based on abnormal delay characteristics.

Misdirection Attacks in IoT-WSNs :

A misdirection attack is a routing-layer attack in which a malicious node intentionally forwards data packets along incorrect or suboptimal paths. In IoT-WSNs, such attacks pose a significant threat to smart connectivity, as they disrupt the normal flow of data between sensor nodes and the sink.

At the network layer, routing protocols such as AODV, DSR, RPL, and LEACH are responsible for route discovery and maintenance. Misdirection attackers exploit vulnerabilities in these protocols by advertising false routing information or impersonating legitimate nodes. As a result, data packets are redirected away from the intended sink node, leading to increased delay, packet loss, energy wastage, or interception by the attacker.

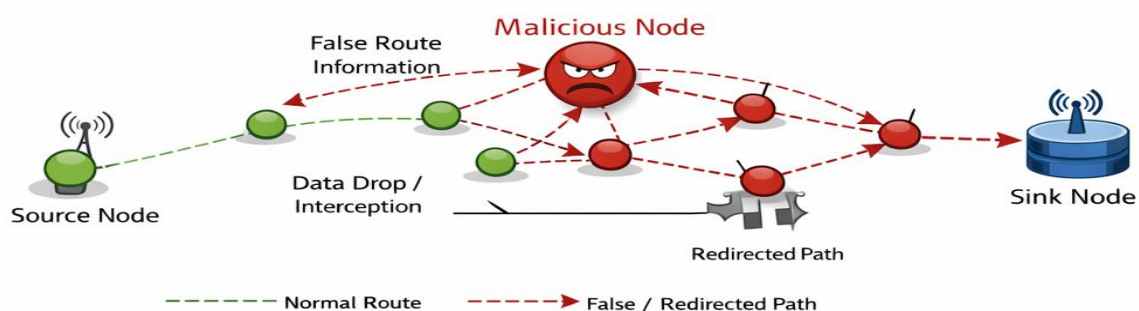


Figure 2: Misdirection Attack in IoT-WSNs

This figure depicts how a malicious node alters routing paths by advertising false routing information, causing data packets to be forwarded toward unintended destinations instead of the legitimate sink node.

Impact on Smart Connectivity :

Smart connectivity in IoT-WSNs refers to the seamless, reliable, and timely exchange of data across interconnected IoT systems. Misdirection attacks disrupt core functionalities of smart IoT applications in several ways.

A. Network Performance Degradation :

Misdirection attacks significantly increase end-to-end delay and reduce the packet delivery ratio. Data packets may traverse longer or looping paths, causing congestion and frequent retransmissions.

B. Energy Consumption and Network Lifetime :

IoT-WSNs rely on battery-powered sensor nodes. Misdirection attacks force nodes to forward packets unnecessarily, rapidly depleting energy and shortening the overall network lifetime.

C. Reliability of Smart Applications :

Smart applications such as healthcare monitoring and industrial control systems require timely and accurate data. Misdirection attacks can result in delayed or missing data, leading to incorrect decisions and system instability.

D. Scalability Issues :

In large-scale IoT deployments, misdirection attacks can propagate across multiple network segments, affecting scalability and network manageability.

IoT-WSNs are widely used in smart cities, smart healthcare, smart agriculture, smart grids, and industrial systems. In healthcare applications, communication delays can endanger patients, while in agriculture, incorrect sensor data may lead to poor crop management decisions. Therefore, secure routing is essential for sustainable smart connectivity.

Types and Variants of Misdirection Attacks :

Misdirection attacks appear in several forms, each impacting the network differently but sharing the common goal of undermining smart connectivity.

- **Blackhole Attack :** A malicious node drops all received packets without forwarding them.
- **Grayhole Attack :** The attacker selectively drops packets, making detection more



difficult.

- **Sinkhole Attack** : A malicious node attracts large volumes of network traffic by advertising false routing metrics.
- **Wormhole Attack** : Two colluding attackers create a tunnel to redirect traffic through a false shortcut.
- **Sybil Attack** : A single node assumes multiple identities to manipulate network topology and routing decisions.

Detection Techniques for Misdirection Attacks :

A. Routing Behavior Monitoring :

Nodes or cluster heads monitor the routing behavior of neighboring nodes to detect anomalies such as frequent route changes or abnormal hop counts.

B. Delay and Hop Count Analysis :

By comparing expected and actual delays or hop counts, misdirected routing paths can be identified.

C. Trust and Reputation-Based Detection :

Each node is assigned a trust value based on its forwarding behavior. Nodes with low trust values are considered suspicious and isolated from routing paths.

D. Machine Learning-Based Detection :

Lightweight machine learning techniques can learn normal routing patterns and detect deviations indicative of misdirection attacks.

Mitigation and Prevention Strategies :

A. Secure Routing Protocols :

Lightweight secure routing protocols incorporating authentication and integrity mechanisms can prevent unauthorized routing manipulation.

B. Trust Management Systems :

Trust and reputation mechanisms help select reliable routes and exclude malicious nodes from the network.

C. Intrusion Detection Systems :

Distributed and collaborative intrusion detection systems enable the identification of



misdirection attacks through shared anomaly information.

D. Energy-Aware Defense Mechanisms :

Energy-efficient defense strategies ensure long-term network operation while mitigating the effects of routing attacks.

Countermeasures and Research Directions :

While this paper identifies key threats posed by misdirection attacks, protecting smart connectivity in IoT-WSNs requires effective and lightweight defense mechanisms. Current research focuses on the following countermeasures and directions:

A. Trust-Based Routing :

Trust-based routing is an active area of research aimed at improving security, performance, and scalability in IoT-WSNs. These protocols evaluate the trustworthiness of sensor nodes based on their forwarding behavior, past interactions, and reliability. By prioritizing trusted nodes for data forwarding and route selection, trust-based routing mitigates risks posed by malicious or unreliable nodes and reduces the likelihood of misdirection attacks.

B. Anomaly Detection Systems :

Anomaly detection systems in IoT-WSNs aim to identify deviations from normal network behavior, such as unusual routing patterns, abnormal traffic volumes, or unexpected delays. Such deviations may indicate security breaches, including misdirection attacks. Lightweight anomaly detection mechanisms are essential to ensure timely detection without imposing excessive computational or energy overhead on sensor nodes.

C. Authentication Protocols :

Authentication protocols play a critical role in preventing spoofing and impersonation attacks that enable misdirection. These protocols focus on verifying the identity of communicating nodes and ensuring the integrity of routing and data packets. Lightweight authentication mechanisms are particularly important in IoT-WSNs to balance security requirements with resource constraints.

D. Energy-Aware Routing :

Energy-aware routing protocols are designed to mitigate the impact of compromised nodes while prioritizing energy efficiency and network longevity. Such protocols often integrate trust-based mechanisms, secure clustering algorithms, and malicious node isolation techniques. By considering both security and energy consumption, energy-aware routing helps maintain sustainable and reliable smart connectivity.

The primary challenge lies in designing countermeasures that are both effective against



misdirection attacks and suitable for the resource-constrained nature of WSN nodes.

Challenges and Future Research Directions :

Despite existing solutions, several challenges remain. Security mechanisms must be lightweight to accommodate resource constraints in IoT-WSNs. Dynamic network topologies caused by node mobility and failures complicate attack detection. Detection techniques must scale efficiently for large IoT deployments. Future research should focus on explainable and energy-efficient artificial intelligence-based security solutions.

Conclusion :

Misdirection attacks at the network layer of IoT-WSNs pose a serious threat to smart connectivity. By exploiting routing vulnerabilities, these attacks degrade network performance, waste limited energy resources, and compromise critical data flows. This paper analyzed the mechanisms, impact, and variants of misdirection attacks and reviewed existing detection and mitigation techniques. Strengthening routing security through trust-aware and lightweight defense mechanisms is essential for reliable IoT-WSN deployments. Future work will focus on trust-aware routing protocols and lightweight intrusion detection systems capable of monitoring and penalizing misbehaving nodes.

References :

- V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
- M. A. Razzaq, M. A. Qureshi, S. H. Gill, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 6, pp. 383–388, 2017.
- I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.
- S. Lata, S. Mehruz, and S. Urooj, "Secure and reliable WSN for Internet of Things: Challenges and enabling technologies," *IEEE Access*, vol. 9, 2021.
- L. Farhan, R. S. Hameed, A. S. Ahmed, A. H. Fadel, W. Gheth, L. Alzubaidi, M. A. Fadhel, and M. Al-Amidie, "Energy efficiency for green Internet of Things (IoT) networks: A survey," *Network*, vol. 1, no. 3, pp. 279–314, 2021, doi: 10.3390/network1030017.
- P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, Art. no. 9324035, pp. 1–25, 2017, doi: 10.1155/2017/9324035.
- J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabelo, J. Al-Muhtadi, and V. Korotaev, "Routing protocols for low power and lossy networks in Internet of Things applications," *Sensors*, vol. 19, no. 9, Art. no. 2144, 2019, doi: 10.3390/s19092144.



-
- N. A. Khan, A. Awang, and S. A. A. Karim, “Security in Internet of Things: A review,” *IEEE Access*, vol. 10, pp. 121384–121404, 2022.
 - N. A. Alrajeh, S. Khan, and B. Shams, “Intrusion detection systems in wireless sensor networks: A review,” *International Journal of Distributed Sensor Networks*, vol. 2013, Art. no. 167575, pp. 1–7, 2013.
 - Z. Shah and R. Patel, “Misdirection attack in wireless sensor network: A survey,” *International Journal for Technological Research in Engineering*, vol. 3, no. 9, pp. 2258–2261, May 2016.
 - U. Dhaked, A. Kumar, and B. K. Singh, “Detection and isolation technique for sinkhole attack in wireless sensor networks,” *International Journal of Computer Sciences and Engineering*, vol. 23, no. 10, pp. 1–7, Oct. 2021.
 - G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, “A survey on layer-wise security attacks in IoT: Attacks, countermeasures and open issues,” *Electronics*, vol. 10, Art. no. 2365, 2021.

