International Journal of Recent Advances in Multidisciplinary Topics
Volume 7, Issue 2, February 2026
www.ijramt.com | E-ISSN: 2582-7839 | RESAIM Publishing | www.resaim.com

Understanding Denial of Service Attacks in IoT Sensor and Wireless Sensor Networks

Bonsa Guyo[1*], Lucy Gitau[1]
[1]Department of Computing and Information Science, School of Pure and Applied Sciences, Kenyatta University, Nairobi, Kenya

***Abstract*: The Internet of Things (IoT) is a pervasive technology that has been rapidly deployed in various application domains such as smart homes, healthcare and wearables due to its ease of use and cost efficiency. IoT systems make use of sensors to monitor a phenomenon of interest autonomously with little to no human intervention. These widely distributed sensor nodes form a wireless sensor network (WSN) for sensing, task management and data collection. Despite its evolution, security in WSNs remains an ongoing challenge due to its resource constraints and the wireless communication medium. Denial of Service (DoS) attacks, for instance, are the most frequent attacks on these networks, with detrimental consequences like continuous battery drain in sensors, node failure and a degradation in network coverage. However, it remains unclear why DoS attacks are prevalent in WSNs therefore this paper presents a comprehensive study of DoS attacks in WSNs discussing the network architecture, its constraints, the network layers and the types of DoS attacks that target each layer. This layered analysis reveals that energy is the ultimate vulnerability, with 60% of the attacks being battery depletion attacks, the majority of which target the Network Layer.**

***Keywords*: Denial of Service attacks, Internet of Things, Security, Wireless Sensor Networks.**

1. Introduction

The Internet of Things (IoT) is a pervasive technology that connects everyday objects, referred to as 'things' to the internet. This is a form of ubiquitous computing where technology is embedded into the environment to monitor physical and environmental phenomenon autonomously, enabling seamless data exchange among real world physical objects with little to no human intervention. IoT is rapidly gaining attention in the digital world with applications in various fields, including healthcare, agriculture, wearables, logistics, industrial automation, smart homes and smart cities [1]. It is one of the most significant technologies in the twenty first century [2], with estimations that there will be over 29.423 billion devices connected by 2030, with the global annual revenue expected to reach 621.7 billion USD by then [1].

IoT systems make use of sensors to sense a phenomenon and collect data for remote monitoring, so a Wireless Sensor Network (WSN) is a data collection component of an IoT system that comprises of hundreds of spatially distributed sensor nodes that monitor physical or environmental conditions of interest and cooperatively pass their data through the network to a sink node or base station where the data can be observed and analyzed for decision making [3]. The individual sensor nodes in a WSN are inherently resource impoverished with limited battery power, memory capacity, network bandwidth and processing power. Such devices lack the means to implement traditional security measures, such as public key cryptography and firewalls, making the sensor network highly susceptible to sophisticated cyber-attacks [1].

Denial of Service (DoS) attacks, which is the most prominent attack in wireless sensor networks [2], is a packet flooding anomaly that is widely known for disrupting network connectivity and availability [4] with detrimental effects like continuous sensor battery drain, node failure and a degradation in network coverage. It aims to disrupt a system or network, making it inaccessible to the target audience and denying end users access to the resources and services that they need [4]. This paper therefore conducted a systematic review to: 1) investigate the reasons behind the prevalence of DoS attacks in WSNs and to 2) discuss the different types of DoS attacks in the network.

The rest of the sections in the paper are organized as follows: Section 2 explores the background for context, Section 3 explains the methods used, Section 4 explores the findings of the systematic review, Section 5 covers the discussion and Section 6 wraps it up with the conclusion.

2. Background

When multiple resource constrained sensors monitor a large physical area, they form a WSN. WSNs comprise of one sink node and a large number of sensor nodes distributed across a vast area. Data is transmitted from nodes to base station via single hop or multi hop communication, and then to users over the internet [5].

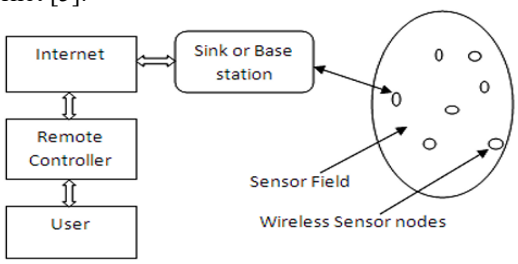

Fig. 1. Architecture of a WSN [5]

*Corresponding author: bonsaguyo@gmail.com

The WSN architecture comprises of the following elements:

1. The sensor nodes which are multiple (in thousands) and are mainly used for sensing the environment, collecting physical and environmental phenomenon and transmitting in a sort of multi hop communication. The individual sensor nodes are also extremely resource impoverished in terms of memory, data processing capabilities and lifetime [6].
2. The sink node which is a more powerful sensor node than the multitude of the nodes that sense the environment. It serves as a gateway between WSNs and the Internet, using wireless communication protocols such as IEEE 802.11b. The sink nodes may have greater processing capability, such as storage space and processor speed, than a standard sensor node, but no greater transmitter power or receiver sensitivity. Depending on application needs, a sensor network may have more than one sink nodes operating concurrently [6].
3. The internet where all the data gets processed and analyzed for insightful decision making by the end user.

A. Layers of WSNs

The sensor nodes are usually dispersed in a sensor field as illustrated in Figure 1. Each of these scattered sensor nodes are the primary field devices in the WSN architecture [7], and they are responsible for collecting and routing data back to the sink node and the end users [3]. The OSI model describes layers that computer systems use to communicate over a network. Based on this model, the wireless sensor network consists of five essential layers: application, transport, network, data link, and physical. Each of the layers has distinct functions regarding reliable data management and transfer between nodes [4].

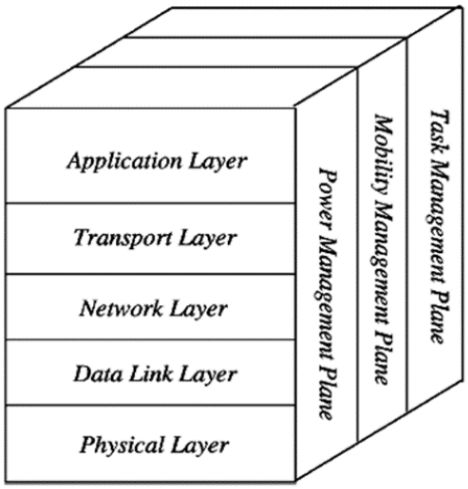

Fig. 2. Layered architecture of a WSN [7]

The physical layer guarantee's reliability by minimizing the effect of packet loss and shadowing. The data link layer ensures reliable node to node communication through error checking and multiplexing. The network layer manages routing and since each node in a WSN acts as a router, this layer is also responsible for securing the paths from malicious attacks. The transport layer is responsible for transmitting data to external networks, and the application layer handles data collection and processing to obtain reliable information [4].

In addition to the five layers, the WSN features three cross layer planes: task management plane, mobility management plane, and power management plane, which boost overall efficiency and allow the sensor nodes to collaborate in the network [7]. The three planes keep track of the power, movement, and task distribution among the sensors and aid the nodes in coordinating the sensing task thus lowering the cumulative energy consumption [3].

B. WSN constraints

Researchers in [7] emphasized that designing effective security measures for a wireless sensor network requires a comprehensive understanding of the network's inherent resource constraints.

The resource limitations in this network include:

1. *Limited power:* Power is limited in a WSN due to the wireless nature of the connection and the small size of the sensor nodes. The individual nodes are battery powered and battery replacement is often impractical in large scale sensor networks. This power limitation has a significant impact on security since encryption algorithms cause communication overhead [7].
2. *Limited storage:* This refers to the storage of the data and the key techniques used to safeguard it. Developing a secure network with robust protocols can be challenging with this limitation since it restricts the complexity of algorithms and the size of data buffers [7].
3. *Low processing power and bandwidth:* The primary design goal for sensor nodes is low cost and energy efficiency, not processing speed. This leads to design decisions that limit computational power for instance, low performance microprocessors (MCUs) that is present in most sensors.

3. Methods

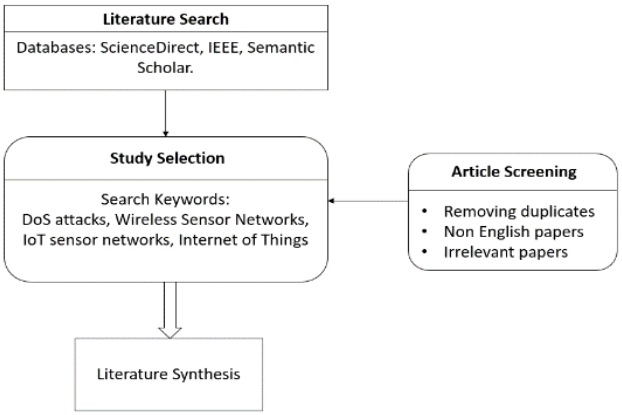

Fig. 3.

A systematic literature review was conducted using the analytical framework in figure 3. Academic databases such as

ScienceDirect, IEEE Xplore and Semantic Scholar were leveraged as the main scientific knowledge sources. Keywords and Boolean operators such as "AND", "OR" and "NOT" were used in the databases to search for all the papers on the topic, and an article screening pipeline was incorporated to filter the articles by relevance.

4. Findings

Denial of service (DoS) attacks are the most prevalent threats to WSNs security. They are simple to launch, requiring minimum effort to inflict maximum damage [8]. Furthermore, while other malicious attacks target different layers, DoS attacks are pervasive across all the five layers of the WSN, making them difficult to defend against [4]. This attack is a network traffic anomaly, with key indicators of a potential DoS attack including a deterioration in network performance, the unresponsiveness of some network components, packet latency or loss, an influx of unnecessary spam messages and the reflexive flooding of packets [2].

A. Types of DoS Attacks in WSNs

The various types of DoS attacks that can occur in the distinct layers of the wireless sensor networks are classified in Table 1.

Table 1

OSI Layer	DoS attack
Physical	Jamming
	Node tampering
MAC	Collision
	Interrogation
	Denial of sleep
	Unfairness
Network	Spoofing
	Blackhole
	Grayhole
	Hello flooding
	Vampire attack
	Wormhole
	Sybil
	Sinkhole
Transport	Synchronize flood attack Desynchronize attack
	Content attack
Application	Overwhelming sensors
	Path based DoS

1) Physical Layer Attacks

The physical layer guarantee's reliability by minimizing the effect of packet loss, shadowing and modulation [4]. The DoS attacks that occur in this layer include:

a) Jamming

This is a relatively popular physical layer attack in which the sensor network is jammed by a flood of unwanted traffic. This can also occur in the form of introduction of noise in the network signal. As a result of the noise, genuine transmissions are disrupted. Jamming attacks can be further classified into four types: constant, deceptive, random and reactive jamming attacks [9].

b) Node Tampering

This is a form of hardware assault where the attacker physically manipulates, destroys or tampers with the nodes in the network so as to damage the devices, extract sensitive information, compromise the security of the network and deny access of resources to the end users [9]. Tampering involves the attacker having physical access to the devices and performing actions such as firmware replacement or implanting hardware trojans so as to leak information and cause malfunctions in the network.

2) Data Link Layer attacks.

The data link layer ensures reliable node to node communication through error checking and multiplexing [4]. Some common DoS attacks in this layer include:

a) Collision attacks

In collision attacks, the attacker attempts to intentionally create packet collisions within the network by infusing collision in one octet of the transmission and causing the entire packet to be destroyed. This corruption can alter the packet's data or the acknowledgement messages, leading to checksum mismatch and errors at the receiver [9].

b) Interrogation attacks

Interrogation attacks are a type of DoS attack that try to deplete a sensor node's resources by exploiting the RTS/CTS handshake protocol. The attacker transmits a high volume of spurious RTS (request to send) packets and this forces the attacked node to allocate its limited resources to generating CTS (clear to send) responses, continuously overloading the node causing it to miss legitimate signals [9].

c) Denial of sleep attacks

This attack specifically targets the sensor node's power supply. Sensor node devices such as Mica2 and Tmote Sky are designed to last for a year or more on a pair of AA batteries, relying on long periods of sleep mode to save power [10]. Denial of sleep attacks manifest in the form of a flood of fraudulent and malicious traffic which keeps the node awake, preventing the node's radio from going into sleep mode and as a result, the battery of the attacked node gets depleted [9]. This attack has a detrimental effect on the sensor network, shortening its lifetime from years to days [10].

d) Unfairness

Unfairness is a weaker form of DoS attack that exploits the MAC Layer priority scheme to cause unfairness. This attack may not necessarily prevent legitimate access into the channel, but can create unwanted delay in access and degrade the channel [11].

3) Network Layer attacks.

The network layer manages routing and since each node in a WSN acts as a router, this layer is also responsible for path selection and securing the paths from malicious attacks [4]. Some common DoS attacks in this layer are:

a) Spoofing attacks

This is a very serious form of DoS attack where the attacker uses a forged identity and attempts to restrict or hinder the operations of sensor nodes in a network. If detected, it adapts by creating multiple fake identities making it a highly alarming and persistent threat [9].

b) Blackhole attacks

Blackhole attacks are common types of DoS attacks in the network layer of a WSN where a fraudulent node infiltrates the network and broadcasts that it has the shortest and optimal path

to the destination. It then drops off all the network packets directed towards it, preventing data from reaching its destination [9].

c) Grayhole attacks

In a Grayhole attack, the attacker node acts more deceptively by partially dropping off some packets and selectively forwarding others, creating the illusion of reliability and genuity. Blackhole and Grayhole attacks are especially effective if the malicious node positions itself near the base station, making it harder to identify and even allowing it to impersonate the base station [9].

d) Hello flooding attack

This is an insidious type of DoS attack in the network layer of a sensor network which exploits the standard "Hello" protocol used by network nodes to discover their neighbors. The attacker sets up the scheme by sending a hello packet to some nodes in the network, which in reality, is not in the range of the sender (attacker node) using a powerful transmitter [9]. The genuine nodes that received the hello message think of the attacker node as one of their neighbors and add it to their neighbor table, assuming the sender is within radio range. The attacker then proceeds to launch a flooding attack onto all these nodes and since each node believes the attacker node is a neighbor, they attempt to process all the incoming traffic. Eventually, this leads to the exhaustion of the limited resources in the network, a disconnection in the network and a denial of service.

e) Vampire attacks

Vampire attacks on the other hand, do not immediately disrupt the availability of the network, but rather target the energy of the sensor nodes by transmitting malicious chunks of data to consume enormous energy, continuously draining the lifetime of the nodes over time. The strength of this attack can be measured by the ratio of energy used in a normal situation to the energy used during the attack [11], with a spike in the battery drain rate indicating an attack.

f) Wormhole attack

This attack involves two malicious wormhole nodes which invade the network and manipulate network routing by creating a tunnel between them. This shortcut disrupts the routing topology since the fraudulent nodes capture packets at one location, tunneling them to another remote location and deceiving the network [12].

g) Sybil attacks

A Sybil attack occurs as a form of an identity multiplication threat where a single malicious entity infiltrates the network and creates a large number of fake identities. The polymorphic node then controls the false identities simultaneous aiming to influence and mislead all the genuine nodes within the network [13].

4) Transport Layer Attacks

The transport layer is responsible for transmitting data to external networks and congestion control [4]. Some common DoS attacks in this layer are:

a) Synchronization Flood Attacks

This attack exhausts the target node's limited resources by overwhelming it with a flood of fake connection requests that are never completed. Each of these fraudulent requests are sent by the attacker and make the target node dedicate a portion of its finite resources to prepare for a new connection, but the attacker never completes the connection requests. These half open requests accumulate, consuming all available resources and preventing the node from responding to legitimate connection requests [9].

b) Desynchronization attacks

Desynchronization attacks aim to disrupt previously established connections between nodes or end points. A malicious attacker sends false sequence numbers or control flags and as a result, unnecessary retransmissions between the endpoints occur leading to a series of disconnections in the existing connections [9].

c) Content attacks

These attacks tamper with the sent messages by changing their order, injecting fraudulent messages or generating false messages [9].

5) Application Layer Attacks

The application layer handles data collection and processing to obtain reliable information [4]. The different types of DoS attack in this layer are:

a) Overwhelming the sensors

In this attack, the attacker node infiltrates the sensor network and attempts to overload the connection using sensor prompts. This causes significant traffic that can be transmitted to one of the base stations which wastes network bandwidth and consumes unnecessary power resources from the nodes [9].

b) Path Based DoS attack

In this attack, fraudulent packets are injected at the edge nodes of the sensor network. As these fake packets move toward the base station, they consume and deplete critical network resources like bandwidth and energy. This flooding blocks legitimate nodes from transmitting data to the base station [9].

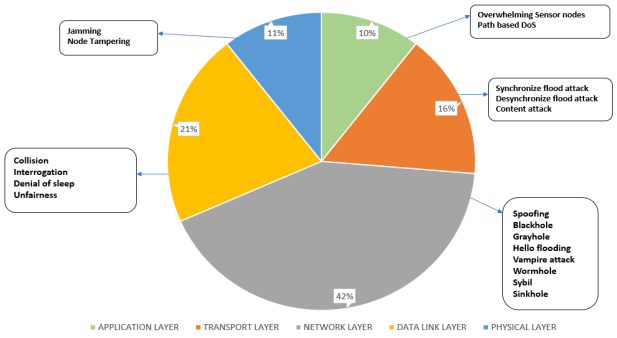

Fig. 4. Distribution of DoS attacks at different layers of the WSN

5. Discussion

Security is still an ongoing challenge when it comes to IoT wireless sensor networks. The inherent resource constraints that the network embodies limit common security mechanisms such as firewalls and authentication, and the wireless medium of communication leaves the network vulnerable to multiple attacks. Denial of Service attacks remain a dominant attack

paradigm in WSNs because the attack is hard to defend against, requiring minimal attacker effort but inflicting the maximum damage, with energy being the ultimate vulnerability.

From the illustration in Figure 4, it can be deduced that 47% of the Denial-of-Service attacks target the network layer. This layer is a crucial component, responsible for energy aware routing and multihop communication in the network. The Network layer is targeted by the DoS attacks due to its role in communication coordination and routing, which is paramount for sensor network operations. Devastating DoS attacks like Blackhole, Grayhole, Flooding and Sinkhole attacks aim to disrupt routing and intercept traffic which negatively impacts the Quality of Service, leading to substantial data loss, continuous energy drain and the acceleration of node death.

21% of the DoS attacks target the MAC layer that is responsible for error control, sleep scheduling and channel access. 16% of the DoS attacks occur within the Transport layer, which is responsible for congestion control and data transportation. 10% of the DoS attacks target the application layer which is crucial in terms of sensing, task management and data collection. Finally, 11% of the DoS attacks target the physical layer that is responsible for modulation and the physical connection. This breakdown suggests that there is need for energy aware security solutions that are specifically tailored for WSNs in order to ensure its availability and continuity at all times.

6. Conclusion

This paper presented a comprehensive and in-depth discussion on WSNs architecture, constraints, layers and the types of DoS attacks that target each layer of the wireless sensor network OSI model. This layered analysis highlighted that 60% of the Denial-of-Service attacks are battery depletion attacks with the majority of the attacks targeting the Network Layer. DoS attacks are prevalent in this network because they are simple to launch yet difficult to defend against. It is also observed that WSNs are severely resource constrained, with common security measures like firewalls and authentication not applicable. These findings emphasize the need for energy aware security solutions and intrusion detection systems specifically designed for the resource constrained domain of sensor networks.

References

[1] M. Fatima, O. Rehman, I. M. H. Rahman, A. Ajmal, and S. J. Park, "Towards ensemble feature selection for lightweight intrusion detection in resource-constrained IoT devices," *Future Internet*, vol. 16, no. 10, Art. no. 368, Oct. 2024.

[2] M. A. Elsadig, "Detection of denial-of-service attack in wireless sensor networks: A lightweight machine learning approach," *IEEE Access*, vol. 11, pp. 83537–83552, 2023.

[3] M. A. Matin and M. M. Islam, "Overview of wireless sensor network," in *Wireless Sensor Networks—Technology and Protocols*, Sep. 2012.

[4] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," *Sensors*, vol. 22, no. 13, Art. no. 4730, Jul. 2022.

[5] M. K. Singh, S. I. Amin, S. A. Imam, V. K. Sachan, and A. Choudhary, "A survey of wireless sensor network and its types," in *Proc. 2018 Int. Conf. Advances Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 326–330.

[6] L. Yang, "Determining sink node locations in wireless sensor networks," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, vol. 4, 2006, pp. 3400–3404, doi: 10.1109/ICSMC.2006.384644.

[7] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: Active and passive attacks—Vulnerabilities and countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362–367, Nov. 2021.

[8] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," *Journal of Big Data*, vol. 10, no. 1, Dec. 2023.

[9] M. N. U. Islam, A. Fahmin, M. S. Hossain, and M. Atiquzzaman, "Denial-of-service attacks on wireless sensor network and defense techniques," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1993–2021, Feb. 2021.

[10] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 367–380, 2009.

[11] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, Jan. 2018.

[12] M. Patel, "A comparative analysis of machine learning models for enhancing wormhole attack detection in wireless sensor networks," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 53s, pp. 317–329, Jun. 2025.

[13] S. Ghildiyal, A. Mishra, A. Gupta, and N. Garg, "Analysis of denial of service (DoS) attacks in wireless sensor networks," *Int. J. Res. Eng. Technol.*, vol. 3, no. 22, pp. 140–143, Jun. 2014.