Journal of Applied Research and Technology

www.jart.icat.unam.mx

ICAT
Instituto de Ciencias Aplicadas y Tecnología

Journal of Applied Research and Technology 21 (2023) 12-16

Original

A survey on variants of DoS attacks: Issues and defense mechanisms

S.Priyanka* • S.Vijay Bhanu

Department of Computer Science and Engineering,
Annamalai University, Annamalai Nagar, India

Received 11 20 2020; accepted 08 31 2022
Available 02 28 2023

Abstract: Wireless-based networks encompass assisted human life in distinct domains like Agriculture, health, infrastructure, climate, transportation and defense. In particular, the wireless sensor networks have been addressed in this article. Though it has many advancements, providing secure data transmission needs a major focus on these platforms. The disruptions or interference is one of the vulnerable security problems in Wireless Sensor Networks. Inside the network, an intruder can encroach and interrupt the whole transmission process. The involvement of an intruder in the device must be remembered in the network. WSN encompasses a wide geographical region and focus on rectification of issues in protocols for routing, interoperability, connectivity, and defense plays a major role. Hence, this article addresses about routing protocols of WSN, applications, recent network security issues and their variants of defense mechanisms. The conclusion depicts the classification of network security issues, requirements, and descriptive defense mechanisms for secure data transmission.

Keywords: Attacks, comprehensive analysis, defense mechanisms, Denial of Service and Network Security

*Corresponding author.
E-mail address: priyankaselvaraj164@gmail.com (S.Priyanka).
Peer Review under the responsibility of Universidad Nacional Autónoma de México.

1. Introduction

Wireless Sensor Network (WSN) is a wireless network that consisting of independently configured devices that control the conditions of their surroundings utilizing sensing devices (Oladayo & Abass, 2019). In a diverse range of applications, such as security protection, environmental control, target identification, military protection, detection of attack, WSNs are used.

Security throughout the wireless sensor nodes is increasing largely not due to the lack of accessibility of effective security systems, but due to the particularity of WSNs, most of the current systems are not sufficient. Hence, the nodes of WSNs have poor processing power and energy restrictions. Mobile nodes have the ability to connect with each other in WSNs, but their primary role is to detect, store and process information. Such information is transmitted for the sink through several hops that can use it or distribute it for all the other nodes. WSNs need efficient routing protocols to achieve effective communication (Sohrabi et al., 2000; Villalba et al., 2009). The deployment of nodes promotes WSN communication by finding the required data transfer routes and maintaining the routes for future transmissions. Due to the heterogeneity of WSN nodes, various protocols for multiple WSNs have been established based on the existence of the nodes and the specific network.

To address the inherited limitations of storage space, computing power and network lifetime, designing a stable, scalable, resilient, and reliable WSN requires sufficient knowledge. Cryptographic methods and main control resources, as discussed by Messaoudi et al. (2017), offer technological and space limitation hardware problems. The complications of memory control, process timing and power operation are faced by the development and construction of a stable WSN Linux kernel. The technical trend, the convergence of cloud infrastructure, wide range of technologies networking (SDN), and virtualization technology must be discussed through WSNs. An aggressive area, close the enemy, poses protection and safety problems against interference and physical layer attacks.

The focus on wide range of applications as shown in Figure 1 can make the researchers to identify problems or issues in WSNs.

In Industry oriented applications, the monitoring of machine structure and timely broadcast of information to the control room is the main work. Some of the key areas focused here is on environmental WSN, physical WSN, gas sector and optical transmission sector.

In terms of society, the use of wireless sensor networks emphasize on traffic monitoring and surveillance. The disseminated connectivity facilitates on various structural components such as smart parking and cities, wireless body area networks and intelligent buildings/homes and bridges.

The applications such as precision agriculture, animal rearing, pollution monitoring, atomic reactors, volcano monitoring are the major key focus areas with respect to agriculture and wildlife and environment protection.

In spite of the analysis of all the factors, we intend to provide a systematic and state-of-the-art literature review in light of these problems. The other contribution of this paper is to facilitate the types of attacks, requirements and their respective defense mechanisms.

The rest of organization of the paper as follows. The section II depicts the literature review related to network security issues. Section III holds the security level requirements, types of attacks and defense mechanism. Lastly, the section IV provides the conclusion details.

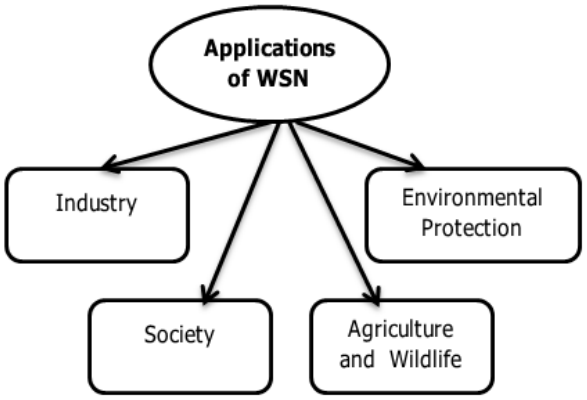

Figure 1. Applications of WSN.

2. Materials and methods

2.1. Levels of Security in WSN

Figure 2. (Olakanmi & Dada, 2020) illustrates the variants of security levels in wireless sensor networks. The first level displayed is Data level security. This consists of concepts such as Integrity, Confidentiality, Authentication and Freshness of data.

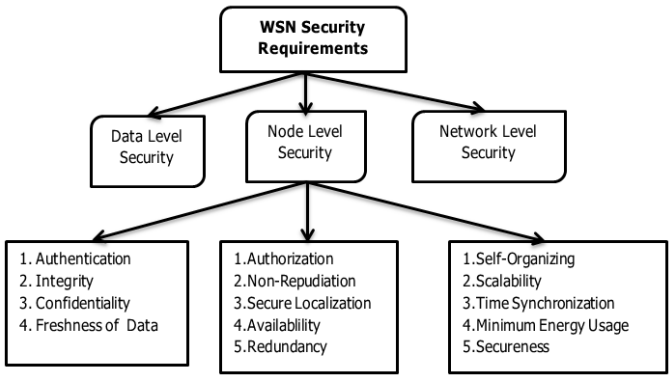

Figure 2. Levels of security.

Integrity focus on authenticity and thoroughness of knowledge. Integrity-focused security mechanisms have been developed to deter an unauthorized entity from modifying or misusing data. Over the expected lifetime, integrity means ensuring the accuracy and honesty of records. Information must not be manipulated in motion and preventative measures can be insisted to confirm that unauthorized individuals cannot modify the information.

Confidentiality applies to denying access and dissemination of information only to approved users/nodes and prohibiting it from those that are unlicensed. Data can be accessed by authorized persons and authorized nodes, whereas intruders including unauthorized nodes cannot obtain information.

Authentication is essential because it allows organizations to maintain their networks secured through allowing just legitimate people (or procedures) can connect their secure properties, including operating systems, networks, files, websites and any software or services that are dependent on the network. Freshness of data deals with allowing new messages in every data transmission by flushing out old data in buffer.

Secondly, the level described is node level security. The requirement that has to be focused in implementation of security are non-repudiation, availability of resources, securing localization data, Checking of redundant data and surveillance of nodes behavior.

The next requirement level of security is Network level security. The factors to be keenly focused for pertaining security such as scalability, to reduce the energy consumption, synchronization of time domain, optimization of routes and the nodes must behave in self-organization.

2.1. Routing protocols in Wsn

There are six classifications of protocol frameworks deployed in wireless sensor networks such as hierarchical routing, location-based routing, quality of service-based routing, data-centric routing, multiple path-based routing and mobility-oriented routing.

The hierarchical routing protocol categorizes network nodes into organizational structure. The protocol chooses nodes of large remaining energy as its cluster head with every cluster node. The observed data within each cluster node is transmitted via the cluster headers of the network (Ibriq & Mahgoub, 2006). Until transmitting it to the drain, every cluster node collates the observed data from all nodes in the cluster. Hierarchical routing protocol via multi-hop transmission lowers energy consumption (Masruroh & Sabran, 2014) mode. Data aggregation carried out by the leader of the cluster also reduces network load. Some of the examples are low adaptive clustering hierarchy (LEACH), secure hierarchical energy-efficient routing (SHEER), threshold-sensitive energy-efficient sensor network protocol (TEEN).

In location-based routing, source and destination nodes are connected consistently for effective data transmission. The energy analysis is performed by calculating the distance between starting nodes and destination nodes. The node incoming strength is utilized to evaluate the total distance. To route the query from the base station to the location, knowledge of the location of sensor network has been manipulated. Knowledge on the location helps the network to choose the right route. Some of the examples of location-based routing are geographic adaptive.

Fidelity (GAF) protocol, energy efficient location-aided routing (EELAR), location-aided routing (LAR), greedy location-aided routing protocol (GLAR), etc.

In QoS routing, pre-encoded metrics of QoS such as end to end delay, throughput has been utilized for efficient delivery of data. Some of the examples of this protocol are QoS-aware and heterogeneously clustered routing (QHCR), Sequential assignment outing (SAR) protocol, stateless geographic nondeterministic forwarding (SGNF), among others.

The main aim of the data-centric protocol is to reduce the redundancy and decrease the data transmission rate before broadcasting it to the base station. This protocol merges the data which is collected from all sensor nodes and transmit through a specific route. Some the examples are sensor protocol for information via negotiation (SPIN) protocol, Directed diffusion and rumor routing.

In multipath-based routing, two paths are generated, named as primary and secondary. To provide an efficient delivery of data, both the paths are utilized. If primary path fails, the protocol uses secondary path for transmission of data. The main objective is to attain the fault tolerance. Some of examples are N to 1 multipath discovery routing protocol, disjoint path routing protocol and braided path routing protocol.

In mobility-based routing, the sensor nodes react based on the dynamic topological structure. This protocol is a light-weight protocol where the closest node nearby the sink nodes carry more information than others. Some of the examples are scalable energy-efficient asynchronous dissemination (SEAD), tree-based efficient data dissemination protocol (TEDD) and two-tier data dissemination (TTDD) protocol.

2.3. Types of attacks

WSNs face a wide list of attacks because of the varied collection of apps: traffic monitoring (Balaji & Sasilatha, 2019), traffic mapping, node theft, node manipulation and modification of data. Although information is at ease, when data is in motion, strategies to protect it are separate. A significant number of devices interact with one another,

performing a task, requiring a considerable amount of input and processing. Table 1 depicts the various types of attacks and their behavior which can be utilized in implementation of novel algorithms in proposed research.

Table 1. WSN security attack types.

Levels / Layers	Types	Description
Physical Attacks	i) Sybil Attack ii) New Node Injection Attack iii)Reverse Engineering Attack	The outside / inside attackers capture quite valuable information in these attacks like machine code, encryption algorithm and design of the node (Suthir et al., 2016).
	i) Jamming attacks ii) DoS attacks	With many fake packets, an attacker can flood the network; sensor tools are used in this attack to rapidly handle false packets.
Base station attacks	i) Source Location Attack ii)Destination Location Attack iii) Traffic Analysis Attack	Packet tracing, traffic analysis are the major procedures followed in identification of these attacks
Routing Protocol Attacks	i) Black Hole Attack ii) Hello Flood Attack	Multiple nodes are generated by an assailant, where other traffic is forwarded, drowned and fell. The whole attack targets the vulnerability of the routing algorithm/protocol Hello flood attack leads to congestion in traffic, drop of data packets due to the use of high radio transmission power.

2.4. Defense mechanisms

To safeguard WSNs from adversaries, different methods are used in precluding these techniques for jamming attack, black-hole attacks and DoS attacks, as well as the source, destination and the privacy of data. Table 2 depicts the levels, causes and defense mechanisms variants of DoS-based attacks.

Table 2. Table 2. Defense mechanisms.

Layers	Causes	Defense Types
Physical Attacks	Leakage of Information, interruptive communication, exposure of privacy data.	Efficient key management, devices of trust, integrity of data, cryptographic techniques
Communication Attacks	Drain of energy, drop of data packets, high delay and retransmission, unwanted data, processing	Intrusion detection system, error correction codes, use of threshold limits (Suthir et al., 2016).
Base station attacks	Leakage of Information, interruptive communication, exposure of privacy data, eavesdropping	Use of dummy packets, integrity, authorization, use of some of the tools such as BLAST, MimiBS
Routing Protocol Attacks	Drain of energy, drop of data packets	Intrusion detection system, authentication

3. Conclusions

The market for promising technologies for sensor networks emerging is developing day to day. Protection needs improved strategies, Confidentiality, control, interoperability and algorithmic capability. The paper discussed on description of security in wireless sensor networks Also, it gives readers an in-depth analysis of WSNs-related security and privacy concerns. Many current analyses have been addressed in WSN routing protocols. This chapter also lets researchers consider the latest developments in security measures and connectivity protocols for WSNs. This paper offers a reading and understanding of network security issues, types of attacks and their defense mechanisms in wireless sensor networks. In future, DoS attacks can be addressed by many researchers to find optimal solutions with novel bio-inspired algorithms. Also, cloud opportunities, challenges and technologies of virtualization can be addressed by means of implementation of recent algorithms with additional care.

Conflict of interest

The authors has no conflict of interest to declare.

Financing

The authors received no specific funding for this work.

References

Balaji, S., & Sasilatha, T. (2019). Detection of denial of service attacks by domination graph application in wireless sensor networks. *Cluster Computing*, *22*(6), 15121-15126. https://doi.org/10.1007/s10586-018-2504-5

Ibriq, J., & Mahgoub, I. (2006). A secure hierarchical routing protocol for wireless sensor networks. In *2006 10th IEEE Singapore International Conference on Communication Systems* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCS.2006.301509

Masruroh, S. U., & Sabran, K. U. (2014). Emergency-aware and QoS based routing protocol in wireless sensor network. In 2014 International Conference on Intelligent Autonomous Agents, Networks and Systems (pp. 47-51). IEEE. https://doi.org/10.1109/INAGENTSYS.2014.7005724

Messaoudi, A., Elkamel, R., Helali, A., & Bouallegue, R. (2017). Cross-layer based routing protocol for wireless sensor networks using a fuzzy logic module. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 764-769). IEEE. https://doi.org/10.1109/IWCMC.2017.7986381

Oladayo, O., & Ashraf, A. (2019). A secure and energy-aware routing protocol for optimal routing in mobile wireless sensor networks (MWSNs). *International Journal of Sensors Wireless Communications and Control*, *9*(4), 507-520. http://dx.doi.org/10.2174/2210327909666181217105028

Olakanmi, O. O., & Dada, A. (2020). Wireless sensor networks (WSNs): Security and privacy issues and solutions. *Wireless mesh networks-security, architectures and protocols*, 13. pp.1-16. http://dx.doi.org/10.5772/intechopen.84989

Sohrabi, K., Gao, J., Ailawadhi, V., & Pottie, G. J. (2000). Protocols for self-organization of a wireless sensor network. *IEEE personal communications*, *7*(5), 16-27. https://doi.org/10.1109/98.878532

Suthir, S., Janakiraman, S., Srividya, M., & Anusha, N. (2016). A contemporary network security technique using smokescreen SSL in huddle network server. In *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)* (pp. 673-676). IEEE. https://doi.org/10.1109/AEEICB.2016.7538376

Villalba, L. J. G., Orozco, A. L. S., Cabrera, A. T., & Abbas, C. J. B. (2009). Routing protocols in wireless sensor networks. *sensors*, *9*(11), 8399-8421. https://doi.org/10.3390/s91108399