International Journal For Technological Research In Engineering
Volume 10, Issue 4, December-2022 *ISSN (Online): 2347 - 4718*

WSN AND ITS SECURITY ISSUES: A CONCEPTUAL REVIEW

[1]Amita Pareek, [2]Mr. Nitin Halkara
[1]M.Tech Scholar, [2]Assistant Professor
[1,2]Department of Electronics (Digital Communication)
Shekhawati Institute of Engineering and Technology, Sikar, Rajasthan

Abstract: A Wireless Sensor Network (WSN) is a self-configured and infrastructure-less wireless network used to monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion, or pollution. The data is then passed cooperatively through the network to a main location where it can be observed and analyzed. WSN are very important network, when considering about any of the organization. This paper reviews the concept of the Wireless Sensor Networks, and its Security.

Keywords: Wireless Sensor Network, WSN Security, Nodes.

1. INTRODUCTION

Wireless Sensor Networks are an infrastructure-less wireless network that employs many sensors in an ad-hoc fashion. These networks are used to track real-time information about a system, environment, or physical conditions. In WSN, nodes are used to manage and monitor the environment in a particular area. They are connected to the Bases Station which acts as a processing unit. Base Station in a WSN system connects through the Internet to share data. [1]

Being extremely low-power and having the ability to operate for long periods of time without being connected to a power source, wireless sensor networks (WSNs) are an extremely valuable tool with many civilian and military applications. A wireless sensor network (WSN) is a wireless network that contains distributed independent sensor devices that monitor physical or environmental conditions. [1]

A WSN is made up of a set of tiny sensor nodes, known as motes, which communicate with and exchange information. The motes obtain information on the environment, such as temperature, pressure, humidity or pollutants. They send this data to a base station. The base station then sends the info to either a wired network or activates an alarm or action depending on the type and magnitude of data monitored. [2]

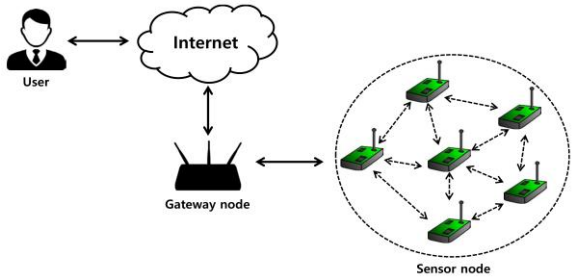

Fig 1. Wireless

Use military-grade, state-of-the-art technology and equipment to get accurate and timely data. Typical applications include monitoring the environment, battlefield surveillance, physical monitoring of [battle] conditions such as pressure, temperature, vibration, pollutants, or tracing human and animal movement in forests or borders. [2]

They use the same transmission medium (the radio waves) to transmit data as wireless local area networks in WLANs. However, devices in networks cannot communicate with one another if they're not using standard protocols like IEEE 802.11. As a result, new protocols that are made specifically for MACs in WSNs are necessary to accommodate the difference in power consumption between devices.[2]

2. APPLICATIONS OF WSN

There are countless applications of Wireless Sensor Networks, some of the applications are discussed below: -

- Military Applications: The military domain was one of the first areas of human activity that adopted WSNs and it is considered to have initiated sensor network research. Smart Dust is a typical example of these initial research efforts, which were performed in the late 90s in order to develop sensor nodes that despite their small size, would be capable of spying activities. With the technological advances that have occurred since those early days, WSNs are now able to support many different solutions. [3]

- Health Applications: In the health sector, WSNs employ advanced medical sensors to monitor patients in hospitals, within their homes, and even inside patient facilities. This allows WSNs to provide real-time monitoring of vital signs by using wearable hardware. The telemedicine applications of WSNs that enable precise GSM location tracking, ECG monitoring, remote video consultation services, as well as non-communicating hospital or individual patient monitoring with sensing data being conveyed to graphical user interfaces. [3]

- Environmental Applications: You can use wireless sensor networks to improve ambient conditions in hostile or remote areas. Here are just some of the types of things wireless sensor networks (WSNs) have been used for: water monitoring, air monitoring, etc. [3]

- Flora and Fauna Applications: Both flora and fauna domains are important for every country. The main subcategories of flora and fauna applications that WSNs can be used in are greenhouse monitoring, crop monitoring, and livestock farming. Read on to learn about the types of sensors that are most commonly used in these situations. WSNs are capable of measuring the performance of greenhouses and can be applied to monitor and control climate conditions in order to improve their operational run. With these networks, researchers have been able to study how WSNs can be applied in greenhouses, maximizing opportunities for the growth of crops. In the agriculture industry, preserving these crops is critical. [4]

Fig 2. WSN Applications

- Industrial Applications: A WSN can be applied in many industries, solving a number of related problems. The main categories of industrial applications of WSNs, namely logistics, robotics and machinery health monitoring. With the increase in e-commerce, the logistics industry has become increasingly important. WSNs are especially well-suited to the logistics industry because many shipping systems need real-time monitoring of environmental parameters and better handling of packages. These requirements can be fulfilled by combining systems in the logistics field with WSNs. The transport logistics sector is all about low cost and high-quality during deliveries. In the development and deployment of a WSN monitoring system to track transportation conditions such as temperature and humidity inside a cargo container is described. [5]

- Urban Applications: With the wide range of sensing abilities offered by WSNs, a new opportunity to gather data has emerged--unprecedented levels of information about a target area. Such is the case for indoors, outdoors, or both. Whatever your environment types, WSNs provide countless application possibilities. With so many parameters and insights to monitor, it's important for large cities to have effective networks in place. WSNs can provide real-time data to the authorities that will support optimal city function. Specifically, increased transportation of people creates issues when there are copious amounts of vehicles heading to a single destination. If a network is utilized to monitor traffic patterns, parking locations can be indicated. The light intensity of street lamps is adjusted by vehicles approaching and driving past. Using Doppler sensors, the lights will be at a preset level in the presence of vehicles and reduced in their absence. [5]

3. WSN SECURITY

One of the challenges with wireless sensor networks is providing the high-security requirements while still having limited resources. Security requirements in wireless sensor networks are comprised of node authentication, data confidentiality, anti-compromise and resilience against traffic analysis. [6]

The demand for real-time information has made wireless sensor networks more valuable. Wireless sensor networks most often use multi-hop transmission to overcome their constraints. The major problem with multi-hop transmissions is attacks on the source data and nodes' identities during hopping. [6]

For a resource-constraint wireless sensor network with a source node sending data to the destination through intermediaries, there is the possibility of intrusion, identity tracing by an adversary, or modification of source data by destination nodes. Wireless sensors sometimes operate in hostile environments and can be susceptible to side channel attacks like differential power analysis. In these attacks, an adversary monitors the system then repeats the same operation and takes careful measurements of power consumed in a cycle-by second basis in order to extract your secret key or promiscuously interrupt communication channels used in perturbation. [6]

The issue with multi-hop wireless networks is how to preserve the identities of the source and destination nodes from being revealed by intermediary nodes and adversaries. In short, some form of lightweight security mechanism should be built into data packets between the nodes. Other attacks on WSNs are discussed below. [6]

- Manipulating routing information: A route attacking attack on a sensor, the intermediate node has the capability of generating routing loops. Attacker can also attract or repel traffic to generate a difference. Moreover, attackers can add or reduce the path ID (using key-based hash function of pseudonyms). For example, if attackers record data packets in one location and then retransmit them in another place, they may be able to detect this by comparing the embellished path ID with hash of all appended pseudonyms. [7]
- Sybil attack: In this type of attack, attackers create fake identities to disrupt network protocols. This can lead to denial of service, among other issues. One such attack is a Sybil attack, which consists of creating illegal nodes with the goal of breaking one-to-one mapping between each node. [7]

To stay safe from a Sybil attack, identity validation of every node involved in routing is required. This can be done reactively or proactively. Reactively, one of the nodes involved has to provide enough identification parameters to differentiate themselves from all the other nodes. The most common method is a resource test. Another way is to decrease the benefits of creating identities and increasing their costs. By doing this, you keep Sybil attacks from happening because the goal of a Sybil attacker is to create more identities for themselves. One way to do this is by using traceable pseudonyms in combination with networks-node identity that's generated by base stations like cell towers. [7]

- Sinkhole attack: Some attacks on WSN use a sink node to disrupt communication between the sensor nodes and base station. This is done by preventing the sink node from obtaining complete or correct data from sensors, which could pose a threat to higher-level applications. Using this attack, an adversary attracts traffic towards themselves by being attractively receptive towards their neighboring nodes in order to capture more of the traffic meant for the sink node. Once an adversary has made themselves attractive to those around them, they can launch other more severe attacks on the network, like selective forwarding or packet modification. WSN is more vulnerable to this attack because nodes typically send data to the base station (sink node). [8]

4. CONCLUSION

WSN is being widely used in industrial and consumer applications. Privacy is a key factor of WSN, so it's imperative to make sure you secure your data. Wireless communication technologies, such as Bluetooth and WiFi, expose users to a plethora of potential security flaws. With compromised sensor nodes, attackers can use them to establish communication channels with non-compromised sensors, which means that the compromised nodes in a network can launch more severe attacks. To solve these problems, wireless sensor networks must maintain safety by preserving privacy, integrity, and reliability.

5. REFERENCES

1. G. Yıldırım and Y. Tatar, "Simplified Agent-Based Resource Sharing Approach for WSN-WSN Interaction in IoT/CPS Projects," in IEEE Access, vol. 6, pp. 78077-78091, 2018.
2. P. Li, C. Xu, H. Xu, L. Dong and R. Wang, "Research on data privacy protection algorithm with homomorphism mechanism based on redundant slice technology in wireless sensor networks," in China Communications, vol. 16, no. 5, pp. 158-170, May 2019.
3. M. U. H. Al Rasyid, D. Prasetyo, I. U. Nadhori and A. H. Alasiry, "Mobile monitoring of muscular strain sensor based on Wireless Body Area Network," 2015 International Electronics Symposium (IES), 2015, pp. 284-287.
4. J. Nelson et al., "Wireless Sensor Network with Mesh Topology for Carbon Dioxide Monitoring in a Winery," 2021 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNeT), 2021, pp. 30-33.
5. H. Wang, G. Yang, J. Xu, Z. Chen, L. Chen and Z. Yang, "A noval data collection approach for Wirelsee Sensor Networks," 2011 International Conference on Electrical and Control Engineering, 2011, pp. 4287-4290.
6. M. U. H. Al Rasyid, I. U. Nadhori, A. Sudarsono and R. Luberski, "Analysis of slotted and unslotted CSMA/CA Wireless Sensor Network for E-healthcare system," 2014 International Conference on Computer, Control, Informatics and Its Applications (IC3INA), 2014, pp. 53-57.
7. Fei Gao, Hongli Wen, Lifen Zhao and Yuebin Chen, "Design and optimization of a cross-layer routing protocol for multi-hop wireless sensor networks," PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, 2013, pp. 5-8.
8. H. Kim, J. Han and Y. Lee, "Scalable network joining mechanism in wireless sensor networks," 2012 IEEE Topical Conference on Wireless Sensors and Sensor Networks, 2012, pp. 45-48.
9. Y. Nishikawa et al., "Design of stable wireless sensor network for slope monitoring," 2018 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet), 2018, pp. 8-11.
10. K. Fukuda et al., "Transmit control and data separation in physical wireless parameter conversion sensor networks with event driven sensors," 2018 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet), 2018, pp. 12-14.
11. L. Zhang, J. Qu and J. Fan, "Topology Evolution Based on the Complex Networks of Heterogeneous Wireless Sensor Network," 2016 9th International Symposium on Computational Intelligence and Design (ISCID), 2016, pp. 317-320.

