IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

Recalling the Security Requirements and Challenges Associated with Wireless Sensor Networks

Neeraj Kaushik, Assistant Professor,
Department of Electronics and Communication Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- neeraj1604@gmail.com

ABSTRACT: In a variety of industries, including agriculture, engineering, environment, transportation, and the military, wireless sensor networks (WSNs) have revolutionized human life. Although WSNs are often utilised for tracking, monitoring, and controlling applications, their resource-constrained nature presents new difficulties. Utilizing a secure network is a fundamental need for all applications. The sensor network's security and energy efficiency are two very complex challenges. The operation of these networks may be impacted by several security threats. Given that WSNs are designed for remote surveillance and that unauthorized changes to sensed data may result in incorrect information being provided to decision makers, it is important to protect them from attack. This includes preventing attackers from obstructing sensor information delivery and from forging sensor information. This paper provides a concise overview of key security concerns and threats in WSN.

KEYWORDS: Sensor, Security, Privacy, Internet of Things (IoT), Wireless sensor networks (WSNs).

1. INTRODUCTION

Today, the Internet has proven to be one of the most useful aspects of daily living. It has altered how people live, play, work, and learn. A Sensor Network is a collection of sensors with characteristics such as cheap cost, lower power consumption, self-organization, and cooperative data processing, as well as benefits with numerous real-world applications. The sensor network is composed of a collection of distributed sensors that perform sensing computations and monitor physical or environmental conditions while transferring data to a base station over the network. The enticing characteristics of the sensor network drew numerous academics to study on various topics connected to these types of networks. While sampling of the wireless sensor and routing algorithms are increasingly accepted, there is still a lot of work to be done on security-related concerns[1].

We discuss recommended security measures for wireless sensor networks and highlight security risks. The infrastructure-less framework, dynamically changing topology, wireless communication among sensor nodes, and finite physical assets, such as memory capacity, source of energy, and extremely low network connectivity, are just a few of the challenges faced by security in wireless sensor networks [2]. Many analysts put out a variety of security protocols and threat management models for safe data transmission and routing in WSN [3].

1.1. Security Requirement

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

The challenging environments and potential threats necessitate additional special security consideration while developing WSN protocols [4]–[6]. For example, authenticity, integrity, freshness, confidentiality, backward and forward secrecy, nonrepudiation, and availability must all be provided as illustrated in Figure 1.

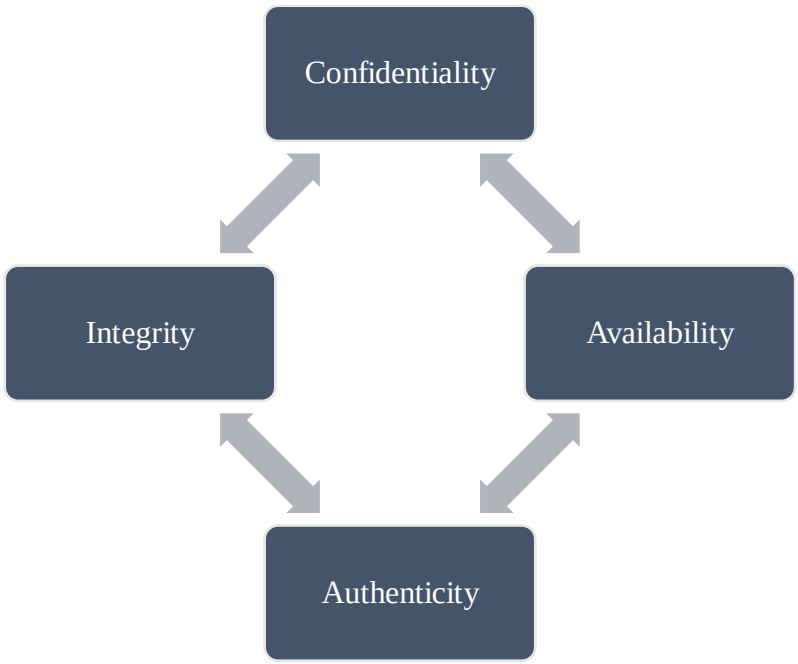

Figure 1: Illustrating the four Security Requirements in Wireless Sensor Networks (WSN).

- Confidentiality: Confidentiality is a key component of security because it protects the private of important data sent between sensor nodes.
- Important elements of a packet are frequently encrypted before being sent from the sending node, and they are then decoded at the node that received the packet. Without identical decryption keys, hackers are prevented from accessing crucial information. The kinds of data that need to be secured are determined by the application.
- Authenticity: Authenticity is essential for preparing the security of communicating node Identities. Even if a message is received from a genuine sender, every node should validate it. In the lack of verification, hackers can easily spread incorrect data into WSNs. In general, an annexed message authentication code may be used to authenticate the origin of a communication.
- Integrity: Integrity should be prepared to ensure that intruders cannot alter the sent messages. Attackers can create disturbance packets in order to change their polarity. Furthermore, a malicious route node might change crucial data in packets prior delivering them. To identify random mistakes in packet communications, a cyclic redundancy checksum (CRC) is used, as is a similarly coded checksum, such as a MAC.
- Availability: Another important capability of a WSN that provides services whenever they are required is availability; otherwise, hackers can launch attacks that limit performance of the network or destroy the entire network. Denials of service is the most dangerous threat

ISSN PRINT 2319 1775 Online 2320 7876
Research paper © 2012 IJFANS. All Rights Reserved, **UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022**

to network availability; it occurs when hackers, by delivering radio interference, diminishing the power of nodes via different devious techniques, or altering network protocols, or render the network unable to provide services.

1.2. Constraints and Obstacles

When compared to other networks of a similar nature, WSN is a wireless network with a number of limitations. The implementation of security measures in WSNs is challenging due to these constraints and limitations as Illustrated in Figure 2. Therefore, in order to design effective security procedures, it is vital to understand and be aware of the following challenges:

- Limited Resources: Because security approaches require a specific level of resources for functioning, such as data memory and computing power, a scarcity of resources makes it more difficult to deploy security techniques.
- Insecure Communication: The level of security depends greatly on the standard protocol as well as the wireless characteristics of the medium of communication.
- Unattended Operation: The sensor nodes may also be left un-attended for extended periods of time depending on the type of applications used by the WSN, making them more susceptible to a variety of cyberattacks. Because of these impediments, the networks and nodes are subjected to several limitations, which have a negative impact on their overall performance. Storage space, memory, limited energy, and computational capacity are the restrictions for nodes. However, as a result of these barriers, the network becomes untrustworthy and unreliable, prone to collisions, and operated remotely with little or no resilience[7].

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

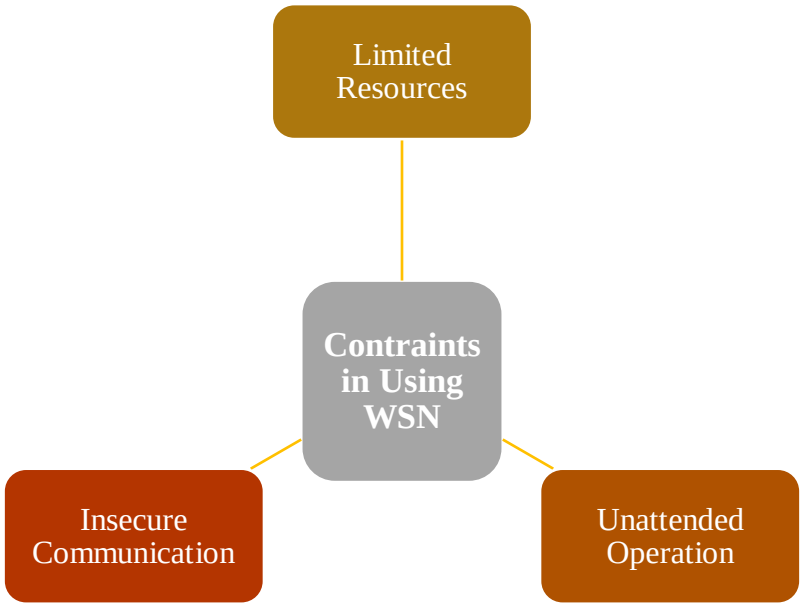

Figure 2: Illustrating the constraints and the obstacles in Using WSN.

2. DISCUSSION

The Internet of Things architecture is complex in nature, with billions of sensors and devices communicating with one another as well as with other things such as humans or virtual entities. It is critical to secure and safeguard every one of these interactions while maintaining the maximum system performance and reducing overall incidents that affect the whole IoT. Because of essential IoT properties such as worldwide connection and accessibility, attackers have various attack routes at their disposal (anyone can access in anyhow and anytime). Various heterogeneous objects exhibited in diverse settings and communicating with one another add to the complexities of the IoT and challenge the implementation of security mechanisms. However, security solutions and services pose a significant problem and are still in their early phases. The existing study on WSN security focuses on solving subjective problems.

2.1.Confidentiality Challenges

The most complicated situation in IoT security is maintaining the privacy of communication information and data. To ensure data privacy between communication parties, there are a number of common encryption functions that may be utilised, including shared secret keys and popular encryption algorithms like Blowfish, the AES block cypher, and Triple DES. Nevertheless, using data encryption as the sole security measure is insufficient to safeguard the privacy of the data. The eavesdropped encrypted data can be subjected to a traffic analysis by the attacker, making it simple to reveal important details about this data. Furthermore, node compromise is making the confidentiality difficulties more difficult when a malicious node is used as being one of endpoints of the communication, making it possible for critical data and information to escape[8], [9].

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

2.2. Authentication Challenges

In ordinary sensor networks, assailants not only change communication packets; their assaults may also include extra inserted bogus packets. Because WSNs are utilised in a shared wireless communication channel and are employed in unsupervised contexts, data authentication is a difficult task. Source authentication can be achieved through asymmetric and symmetric processes where the receiving and sending nodes communicate secret keys to confirm the resource identity, which is required to enable sensor nodes to differentiate between maliciously infused and spoofed data packet and the original packets from the legitimate source.

2.3. Integrity Challenges

Once the WSNs have effective confidentiality safeguards in place, the communication data may not be stolen by the adversaries. There is a chance that alterations might endanger WSNs, though. This occurs when a rogue node introduces fake data into the network or even when a wireless channel's unstable circumstances result in data loss or damage. As an example, some malicious nodes could insert fake data or alter the data included in communication packets. These altered packets will then be transmitted to the recipient, which may be the WSN base station in this case. Nevertheless, because to the challenging communication environment, the detected data may be lost or damaged even when no malicious nodes are involved[10].

2.4.Availability Challenges

The WSNs can be attacked with jammed communications using excessive communications or calculations, which may target the sensor nodes or any other portion of the WSNs and thus damage the network's survivability. But ultimately, the entire WSN operation should be in danger if base station availability collapses. Practically speaking, the consequence of losing accessibility might result in a disappointment in sensing possible accidents and ultimately a financial loss. Take the monitoring application in manufacturing processes as an example. By allowing for a small number of benign node failures or corrupted nodes, WSN availability may be increased. In order to meet the security needs of WSNs, typical encryption methods must be modified, which adds to the cost.

3. CONCLUSION

Although wireless sensor networks are important in both military and civilian applications, they must be protected from various security threats and intrusions. There is currently no unified or generic model to guarantee overall security, hence the majority of the security mechanisms that are supplied are based on specific network models or attacks. Combining several security methods to work with one another will provide researchers with a difficult challenge. The flexibility, energy-efficiency and cost-effectiveness of the deployment of such systems in various WSN applications would also need to be taken into consideration.

REFERENCES

[1] L. J. G. Villalba, A. L. S. Orozco, A. T. Cabrera, and C. J. B. Abbas, “Routing protocols in wireless sensor networks,” *Sensors*. 2009. doi: 10.3390/s91108399.

[2] H. Modares, A. Moravejosharieh, R. Salleh, and J. Lloret, “Security overview of wireless sensor network,” *Life Sci. J.*,

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022**

2013.

[3] M. Pule, A. Yahya, and J. Chuma, "Wireless sensor networks: A survey on monitoring water quality," *J. Appl. Res. Technol.*, 2017, doi: 10.1016/j.jart.2017.07.004.

[4] J. Undercoffer and S. Avancha, "Security for sensor networks," *CADIP Res. ...*, 2002.

[5] V. Ekong and U. Ekong, "A SURVEY OF SECURITY VULNERABILITIES IN WIRELESS SENSOR NETWORKS," *Niger. J. Technol.*, 2016, doi: 10.4314/njt.v35i2.21.

[6] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, 2012, doi: 10.1007/s10916-010-9449-4.

[7] F. Hassani Bijarbooneh, "Constraint programming for wireless sensor networks," *Constraints*, 2015, doi: 10.1007/s10601-015-9228-4.

[8] J. A. Stankovic, "Research challenges for wireless sensor networks," *ACM SIGBED Rev.*, 2004, doi: 10.1145/1121776.1121780.

[9] S. Tarannum, "Energy Conservation Challenges in Wireless Sensor Networks: A Comprehensive Study," *Wirel. Sens. Netw.*, 2010, doi: 10.4236/wsn.2010.26060.

[10] P. M. Chanal and M. S. Kakkasageri, "Security and Privacy in IoT: A Survey," *Wireless Personal Communications*. 2020. doi: 10.1007/s11277-020-07649-9.