International Journal of General Engineering and Technology (IJGET)
ISSN (P): 2278–9928; ISSN (E): 2278–9936
Vol. 8, Issue 3, Apr-May 2019; 7–14
© IASET

International Academy of Science, Engineering and Technology
IASET
Connecting Researchers; Nurturing Innovations

SECURITY CHALLENGES AND SOLUTIONS IN WIRELESS SENSOR NETWORKS

***Shyamala*[1], *Sujata S.Ratnakar*[2] & *Vidyavathi D P*[3]**

[1]*Lecturer Electronics & Communication Department Government Polytechnic For Women(142), Ramanagara, Karnataka, India*

[2]*Lecturer, Department of Computer Science, Gricp(123) Bengaluru, Karnataka, India*

[3]*Lecturer, Department of Computer Science, Government Polytechnic, Channasandra, Karnataka, India*

ABSTRACT

In this report, the security issues and opportunities in Wireless Sensor Networks (WSNs) are looked at with regard to security threats including Data control, and Denial of services attacks. They know good encryptions, authentications and IDS as some of the important defense mechanisms. This study is a review that employs qualitative secondary data from Google Scholar, journals, and census data drawn from scholarly sources. The study re-emphasizes the need to adopt security solutions that are considerate with the resources available in WSNs. In the Discussion chapter, these insights are then discussed and suggestions made on how to establish effective and strong efficient securities. In general, the report can help in improving the understanding of WSN security issues and vulnerability and provide suggestions on how to protect networks and data in various applications.

Keywords: *Wireless Sensor Networks, Security Challenges, Data Tampering, Denial of Service Attacks, Encryption, Authentication, Intrusion Detection Systems, Qualitative Data, Energy-Efficient Security, Network Resilience*

Article History

Received:* *02 Mar 2019*| *Revised:* *12 Apr 2019* | *Accepted:* *23 May 2019

1. INTRODUCTION

Wireless Sensor Networks or WSNs came into picture as a revolutionary innovation and has been diversely used in many sectors majoring in environmental, health and military field. It is an array of many small, inexpensive nodes often with limited communication capabilities and is used for gathering real-time data which helps organizations and companies to improve their decision-making make over the world. As for the large-scale implementation of WSNs, the security issues are affecting it considerably. Due to the limitations of resources and functionality in WSNs that consist of limited computational capability, limited energy, and wireless communication, WSNs are prone to a number of serious security threats including eavesdropping, data interferences, and DoS attacks.

2. LITERATURE REVIEW

2.1 Introduction

WSNs are used in different systems where the deployment and supervision of the nodes are important and they are applied in many fields starting from the control of environmental systems to military security. Yet, they have brought out a couple of security issues as they continue to gain popularity.

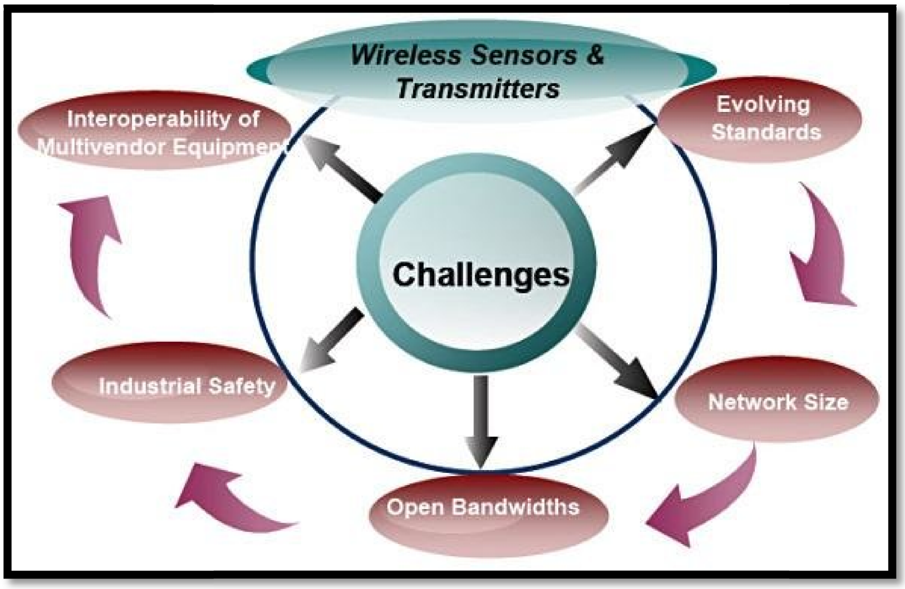
Wireless Sensors & Transmitters
Interoperability of Multivendor Equipment
Evolving Standards
Challenges
Industrial Safety
Network Size
Open Bandwidths

Figure 1: Challenges in Industrial Wireless Sensor Networks (IWSN)

Due to the characteristics of the WSNs such as decentralizing, having bandwidth constraint, using wireless link, there are various attacks possible such as eavesdropping, modification of data, denial of service attack. It is for these reasons that proper handling of these concerns is central for the effective and credible extraction of the data.

2.2 Security Vulnerabilities in WSNs: Identifying and Understanding Common Security Weaknesses In WSN Environments

Security threats that affect WSNs are of great concern, especially given the potential and actual challenges that Wireless Sensor Networks present. Since WSNs are comprised of many numbers of sensor nodes with restricted computational power, memory, and bounded energy then it is very difficult to incorporate efficient security solutions (Ghadi *et al.*, 2024). Another weakness pertaining to WSNs is that they are not readily associated with any centralized structure hence posing significant complications over key security and authentication.

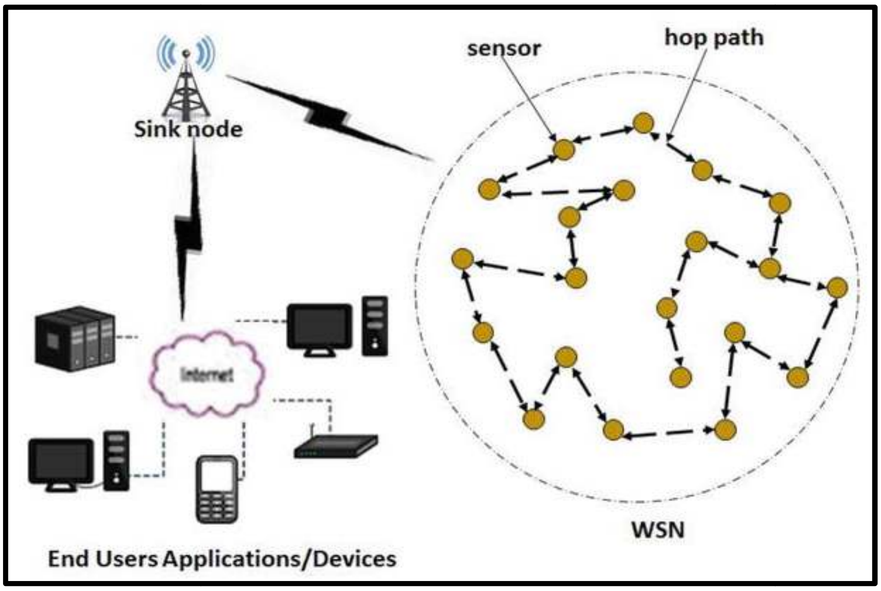

Figure 2: Wireless Sensor Network System Model

Another problem that arises for WSNs is in regard to routing protocols. Dangers such as the Sybil attack where a node impersonates multiple nodes and the sinkhole attack wherein malicious nodes act as local nodes to lure all traffic towards them and deny the network its functionality. In addition, some resource depletion attacks, like the denial of sleep attack, consume energy of the limited time battery life of the sensor nodes and thus reduce the lifetime of the networked system (Priyadarshi, 2024).

2.3 Encryption and Authentication Techniques: Evaluating Methods to Secure Data Transmission and Access in WSNs

Wireless Sensor Networks, WSNs, uses encryption and authentication mechanisms as the most basic measures to provide security to the data transmission and access. As it has been pointed out earlier, WSNs are highly susceptible to various forms of attacks because of the existence of open exposure for receiving and transmitting signals, and scarce computational power that is available on sensor nodes. Encryption changes the form of the information which only those with the code can decipher it and this allows authorized personnel to gain access to the information. For the WSNs, the better algorithms effective for symmetric encryption are AES (Advanced Encryption Standard) because they are not complex to be computed and used effectively (Khan *et al.*, 2024). Being commonplace, recognitive procedures confirm the identity of devices, as well as of the users, in the network, thus eliminating unauthorized access. PKI and digital signatures are used especially in creating secure channels of transmitting information as well as verifying its integrity.

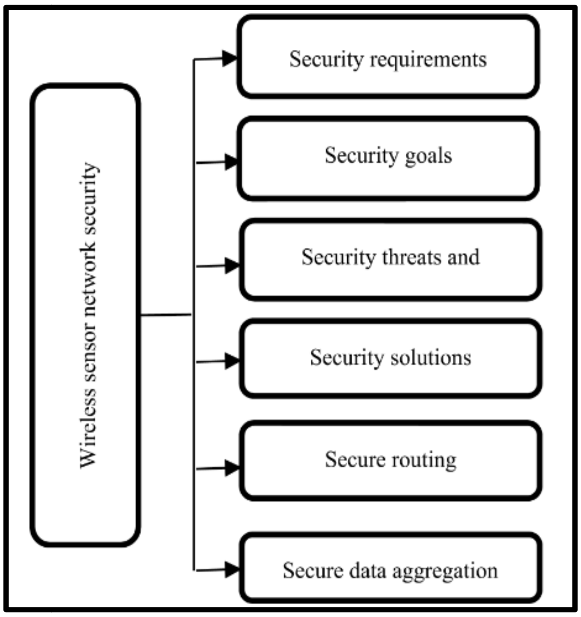

Figure 3: Security Elements Wireless Sensor Networks.

Moreover, key management is also an important function adopted in the WSNs for the purposes of encryption and authentication. Digital encryption is absolutely crucial to ensure secure message exchange while freeing up network resources and preventing overload. Certain strategies such as pre distributing of keys and other key management schemes work to improve the security of the system without a significantly high usage of resources.

2.4 Intrusion Detection Systems: Implementing mechanisms to detect and respond to security breaches in WSNs

An IDS can be implemented to ensure the security of the WSN since it is the main responsibility of checking activities within the network for compliance with security paramount secrets within the network. Due to the inherent nature and constraints of WSNs, traditional IDS mechanisms cannot work effectively in the context of WSNs and hence must be modified. The IDS used in WSNs utilizes both anomaly and signature based and sometimes hybrid in which there is a detection of new and or unexpected patterns or known attacks in the network.

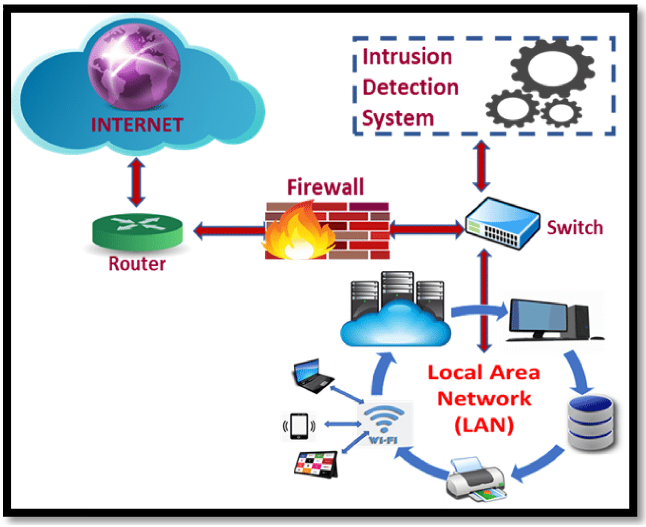

Figure 4: Intrusion Detection Systems and Local Area Networks.

Anomaly-based IDS work on the basis of recognizing normal network traffic and then alerting on variations from this normal behavior which is generally an indication of intrusion (Nzeako *et al.*, 2024). The strength of this approach is that it provides protection against new forms of attacks and threats while the weakness is that in such environments of WSN there might be a large number of false positives.

2.5 Summary

The literature survey on security threats and countermeasures in WSNs present the key shortcomings of security mechanism in WSNs and various threats that include Eavesdropping, Data manipulation and DoS attack. This looks at several security aspects of a computer to ensure that data is protected from outside interference, for example, use of encryption and authentication processes. Moreover, the review brings out the understanding of Intrusion Detection Systems (IDS) on how best to respond to various security threats.

3. METHODOLOGY

3.1 Introduction To Methods

The approach for this security consideration and its remedies within WSNs site used in this report relies on secondary qualitative data. This approach involves collection of data through an analysis of academic journals, technical publications such as research articles, and case studies with an aim of understanding the current state of security within the WSN. In an effort to present a broad picture of security concerns, this report seeks to present common threats encountered in computer systems and networks as well as assess the merits and demerits of different security measures; this paper also seeks to present trends regarding the improvement of security technologies. The strength of this type of data is that it provides a broad and detailed view of the subject under consideration as it is collected from multiple primary sources of secondary nature, including researchers and practitioners.

3.2 Types of Datasets Used

The paper employs secondary qualitative data prevalent in peer-reviewed literary works and information databases, indicating a systems approach to the study of Security Challenges and Solutions in Wireless Sensor Networks (WSNs) (Ali *et al.*, 2024). The types of datasets employed include:

- **Google Scholar and Online Journals:** Vanacore, Marano, Aloi, Russo & Giordano (2013) and West & McEwan (2012) have presented research papers on Google Scholar and couple of other online journals for a comparative analysis of WSN security challenges and prevention mechanism.
- **Books and Directories:** Source includes textbooks and directories contain basic information and recommendations as well as comprehensive evaluations of WSN technologies, threats, and protection measures.
- **Non-governmental Statistical Data:**Survey results presented by non-governmental organizations (NGOs) provide real life statistics on the occurrence and effects of security violation in SNWs across various domain.
- **Census Data:** Details such as the populations numbers, rates, percentages, age distributions and sex distributions as well as geography, nationality or country of origin of people involved, derived from national or international census reports help in contextualizing WSN application and risks in various areas (Rajasoundaran *et al.*, 2024).
- **Internet Sources:** SEC information collected from Web sites such as industry reports, technical mailing lists and discussions, and white papers includes genuine WSN security incidents and solutions from real-life cases.

In combining these varied data sets, the report seeks to provide an objective survey and critique of WSN security at the present time, while giving especial consideration to qualitative information and paradigms generated from various fields.

4. RESULTS

4.1 Introduction

The Results chapter of this report seeks to highlight findings inferred from the secondary qualitative data that relate to the topic Understanding of Security Challenges and Solutions in Wireless Sensor Networks (WSNs). This chapter to, approach the presented data systematically to analyses and interpret the collected data sources from different books, internet sites, journals, directories, statistical data from the non-governmental organization and census data. WSNs security threats are reviewed in terms of their potential impact on WSN systems, and the efficiency of the security measures proposed in the literature is assessed together with concerns about the implementation of the different cases or examples described.

4.2 Findings

The last but not the least; the findings chapter of the report offers a complex discussion on the key ideas, problems, and the solutions unveiled after a critical evaluation of the Secondary Qualitative Data. That is why, based on the information received, it is known that WSNs have numerous security threats, such as the interception and manipulation of incoming information, as well as denial of service attacks that can endanger data integrity and network stability. As seen, encryption and authentication come out as strategies that can help in combating these threats since they enable secured data transmission and access in the WSN setting (Alsumayt *et al.*, 2024). Also, the results of this research also confirm the use of Intrusion Detection Systems (IDS) in handling and detecting security threats within wired WSNs.

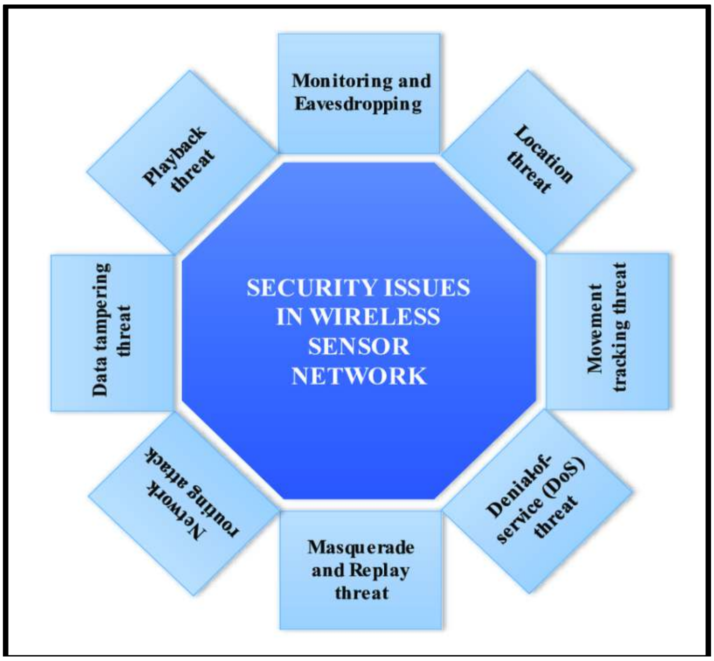
Monitoring and Eavesdropping
Location threat
Movement tracking threat
Denial-of-service (DoS) threat
Masquerade and Replay threat
Network routing attack
Data tampering threat
Playback threat
SECURITY ISSUES IN WIRELESS SENSOR NETWORK

Figure 5: Security Issues in a Wireless Sensor Network.

The report also emphasizes the need to have security motivations and mechanisms that are lighter and energy efficient for WSNs due to the limited resource capacity of the sensor nodes. It delves into how organizations are moving towards adopting IDSs that are a fusion of the anomaly and signature detection mechanisms in order to have broader detection of threats while at the same time reducing the production of false alarms.

4.3 Summary

The last chapter of the report is one that ties the concepts pinpointed in the course of the research into broader discoveries. It notes the crucial weaknesses associated with WSNs; which include capabilities of being attacked by other categories of cyber-threats including eavesdropping and data manipulation. The chapter also draws attention to security and privacy that require effective encryption and authentication techniques for security in WSN deployments. Additionally, it emphasizes the dependency on IDS to timely and effectively address security threats and calls for research on IDS that is less resource-demanding to address the limitations in WSN networks.

5. DISCUSSION

5.1 Introduction

The heading is used at the beginning of the Discussion chapter of the report following the conclusion of the Literature Review and serves as an approach for the enhancement of the synthesis of research findings. It brings into focus the security threats that were earlier discussed in the context of WSNs including data control and denial of service attacks and their impact on the integrity of the communicated data and the overall dependability of the network.

5.2 Discussion

There are two major issues articulated in the discussion: encryption and authentication as ways to reduce security threats in WSNs (Qiu *et al.*, 2024). It compares the existing solutions in terms of the efficiency and reveals the existing problems of the current approach, focusing on the requirement of practical, light-weight solutions for typically low-Arduino sensor nodes.

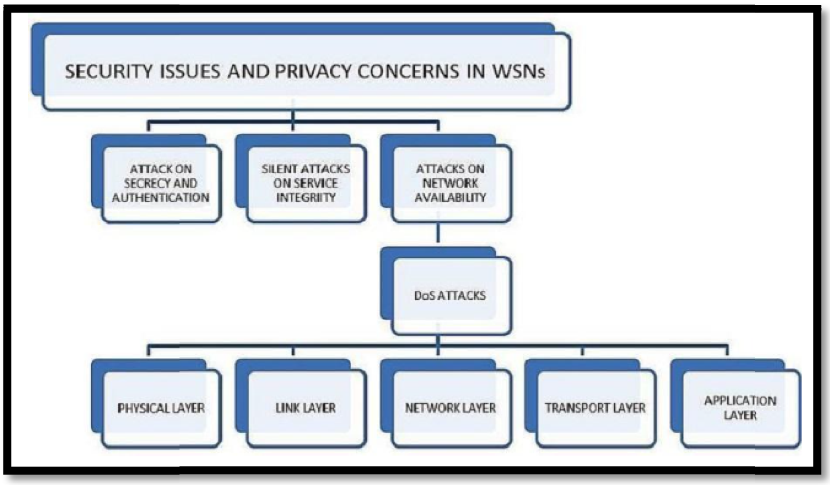
SECURITY ISSUES AND PRIVACY CONCERNS IN WSNs
ATTACK ON SECRECY AND AUTHENTICATION
SILENT ATTACKS ON SERVICE INTEGRITY
ATTACKS ON NETWORK AVAILABILITY
DoS ATTACKS
PHYSICAL LAYER
LINK LAYER
NETWORK LAYER
TRANSPORT LAYER
APPLICATION LAYER

Figure 6: Security Issues and Privacy Concerns in WSNs.

Furthermore, the topic of this discussion consists in considering the possibilities of Improving Resilience of Networks against Intrusion Techniques based on IDS systems, while stressing on the necessity of the adaptation process and the rationalization of resource usage. Prospective research directions are thus identified as encompassing a more comprehensive investigation of associated insecurity risks using advanced encryption and the establishment of power-conscious IDS that will be relevant for the complex nature of WSN settings.

5.3 Summary

The Discussion chapter summative melds research evidence on security threats and responses concerning WSNs. It identifies risks such as data manipulation and a denial-of-service attack, stresses encryption and authentication as the essential proactive shield. This chapter also ensures that the concept of IDS is made clear to the readers with a special focus on its ability to quickly detect intrusions. To mitigate identified risks, recommendations include adoption of effective and energy-sensitive security solutions that are compatible with WSN environment.

6. CONCLUSION

Conclusively, this report offers an extensive focus on the vulnerabilities and defensive measures possible in WSN surroundings. It has provided potential problems like data manipulation and Dosing situations which requires increased focus on Information Insurance, proper authentication schemes, and strong IDS. The results hint at the existence of a peculiarity and a necessity for designing security methods that should be capable of servicing WSNs under present contexts of available resources and general operational features. Subsequently, forward-looking academics, industrial pioneers, and policy makers must strive for lightweight, energy-sensitive security platforms to improve the availability and steadfastness of WSN contexts across numerous areas of application.

REFERENCES

1. *Akinsanya, M.O., Ekechi, C.C. and Okeke, C.D., 2024. Security paradigms for iot in telecom networks: conceptual challenges and solution pathways. Engineering Science & Technology Journal, 5(4), pp.1431-1451.*

2. *Ali, R., Pal, A.K., Kumari, S., Sangaiah, A.K., Li, X. and Wu, F., 2024. An enhanced three factor-based*

authentication protocol using wireless medical sensor networks for healthcare monitoring. Journal of Ambient Intelligence and Humanized Computing, pp.1-22.

3. *Alsumayt, A., Alshammari, M., Alfawaer, Z.M., Al-Wesabi, F.N., El-Haggar, N., Aljameel, S.S., Albassam, S., AlGhareeb, S., Alghamdi, N.M. and Aldossary, N., 2024. Efficient security level in wireless sensor networks (WSNs) using four-factors authentication over the Internet of Things (IoT). PeerJ Computer Science, 10, p.e2091.*
4. *Ghadi, Y.Y., Mazhar, T., Al Shloul, T., Shahzad, T., Salaria, U.A., Ahmed, A. and Hamam, H., 2024. Machine learning solution for the security of wireless sensor networks. IEEE Access.*
5. *Khan, S., Khan, M.A. and Alnazzawi, N., 2024. Artificial neural network-based mechanism to detect security threats in wireless sensor networks. Sensors, 24(5), p.1641.*
6. *Nzeako, G., Okeke, C.D., Akinsanya, M.O., Popoola, O.A. and Chukwurah, E.G., 2024. Security paradigms for IoT in telecom networks: Conceptual challenges and solution pathways. Engineering Science & Technology Journal, 5(5), pp.1606-1626.*
7. *Priyadarshi, R., 2024. Exploring machine learning solutions for overcoming challenges in IoT-based wireless sensor network routing: a comprehensive review. Wireless Networks, pp.1-27.*
8. *Qiu, Y., Ma, L. and Priyadarshi, R., 2024. Deep learning challenges and prospects in wireless sensor network deployment. Archives of Computational Methods in Engineering, pp.1-24.*
9. *Rajasoundaran, S., Kumar, S.S., Selvi, M., Thangaramya, K. and Arputharaj, K., 2024. Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks. Wireless Networks, 30(1), pp.209-231.*