A Comprehensive Study on Issues and the Respective Solutions: Wireless Sensor Network

Shreshtha Rana, Gunika Lamba, Shefali Singhal

Manav Rachna International Institute of Research and Studies, India

Corresponding author: Shreshtha Rana, Email: ranashreshtha98@gmail.com

Wireless sensor technology is a rising sector of study specifically in exploration because of which there are an enormous number of applications, through which we can take advantage. It has been the major guide to the development of small-scale, cheap, and powered computers, known as sensor nodes. For most of the researchers working on this technology, the challenging part is security, which automatically makes it more difficult to use than the usual conventional networks that we use in our day-to-day lives. But still, there are sensor networks, which help us to track down the challenges to ensure security in the network system. This paper helps us to comprehend the security-related issues attacks and challenges that are faced by wireless sensor technology and how to overcome them. This paper condenses various security schemes like cryptography, stenography which are useful to ensure the security of our information. This paper offers a comprehensive perspective of various issues which are linked to technology that works without wires and at the same time, it also offers various solutions in response to various attacks.

Keywords: Wireless Sensor Networks (WSNs), Security Objectives, Security Mechanism.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 347–355. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-36

1 Introduction

In the IT environment, wireless technology is very relevant. Its main domain for all the ongoing research involves network security programming, management of data, designing of different systems, etc. The basic purpose behind the sensor network is to allocate the various small sensing devices. These small sensor nodes are capable of sensing, detecting, and undergoing some changes in the parameters. These nodes can also communicate with various devices present in the particular area for specific purposes for example targeting, monitoring, surveillance, etc. Today's[8] sensors can also monitor a spectrum of things like various geographical conditions like the temperature of an area, air pressure, humidity and type of soil present in a specific area, or availability and unavailability of various resources and various things. Wireless is used in sensor networks to allow different sensors to converse with one another. Because of the various captivating qualities of this technology, many researchers are fascinated toward working on this. Also, there are many issues, to which they can contribute, but the most preferred issues are strategies related to routing and wireless sensor modeling [1], but still, there are some issues related to security that is yet to gain considerable attention. The various issues related to wireless technology and its important parameters which need considerable exploration are covered in this paper.

The most considerable and challenging factors for availing any well-structured and well-planned scheme related to security in wireless technology are rebuilt by the amount and proportions of sensors that help in processing sensor power. In this paper, we tried to discuss the concerning factors related to security in wireless sensor networks which includes cryptography, steganography as well as other applications of network security. Through this paper, we tried to explore different types of threats as well as attacks against wireless sensor networks. This paper also reviews the work related to WSN and schemes which are proposed to ensure security in a wireless sensor network. Finally, the paper concludes by discussing future trends and research in wireless technology.

2 Security objectives

Wireless networks, like other commonplace systems, are vulnerable to a range of threats. Their restricted functionality and unique application characteristics, on the other hand, necessitate some additional security measures, including those of typical businesses.

- **Data Confidentiality–**

Categorization of information is one of WSN's key security requirements for WSN applications (such as military and key binding applications). Since sensor nodes send sensitive information, it is very important to prevent other adjoining systems from receiving private data that captures the channeling of information. One of the conventional ways to ensure the confidentiality of information is to encrypt the information and use a public key to allow individual recipients to retrieve the compromised information.

- **Authenticity and Integrity–**

To secure knowledge security in the WSN, simply providing information privacy is insufficient. Validation of the knowledge sender is also a critical security requirement because a foe can alter communications on correspondence or inject vengeful remarks. The collector is certain that the data has not been tampered with during transmission through information confirmation.

- **Availability-**

We will not overlook the relevance of node accessibility once they are required. When WSN is used to monitor reason in an assembly system, for example, inaccessibility of nodes may cause the system to miss potential errors. Accessibility ensures that sensor nodes are dynamic inside the system, ensuring the system's utility. It must be ensured that security instruments requiring an interest in the preparation of knowledge or correspondence when their administrations are required are allowing the approved nodes to require an interest in the preparation of knowledge or correspondence when their administrations are required. For security considerations, security arrangements must be inferred so that sensor nodes do not do additional calculations or attempt to transfer additional assets.

3 Attacks on Wireless Sensor Network

There are two different points of view against wireless sensor networks. These attacks are basically against the security mechanism or basic mechanism like the routing mechanism [4]. The major attacks are mentioned in our paper.

- **Denial of Services-**

Unintentional node failures or malicious actions might cause this form of assault. The most basic DoS (Denial of Service) attack attempts to deplete the victim node's resources by sending more useless packets, preventing legitimate network users from obtaining services or resources to which they are entitled. This form of assault is designed to counteract an opponent's attempts to bring a network down, as well as to degrade network proficiency to deliver service. In WSNs, there are many different types of DoS attacks that can be carried out at different tiers. For example, DoS attacks could involve jamming or tampering in the physical layer, collision, exhaustion injustice at the network layer, or avarice, homing, misdirection, and black holes created by desynchronization and spiteful flooding at the transport layer. By investing in a good network system or resources using a strong authentication system or system for identification of traffic one can prevent DoS attacks.

- **Information-in-transit Attacks-**

Various sensors are monitored in a WSN, and they modify certain parameters or values, as well as report to the sink according to the correct specifications. While transmitting the report, the information in transit could be changed, erased, duplicated, or spoofed. In wireless communication, attackers have a significant possibility of controlling the traffic flow and fabricating, disrupting, or amending packets [7]. As a result, incorrect data is transmitted to ground channels or sinks.. Because of the limited set of broadcasts in sensor nodes and a lack of resources, attackers with high computational power and a broad network lifetime may attack sensors installed around the same time to change or amend the actual information while it is being transmitted.

- **Sybil Attack-**

In some circumstances, sensors in a WSN may need to work together to fulfill or complete tasks so that they can take advantage of information redundancy and subtask distribution. In this instance, a unit node can profess to be multiple nodes by assuming the identities of other valid nodes [5]. A Sybil attack is when a node creates its identity in many nodes at the same time. These assaults are always targeted at affecting the strength of the system's security, data, and resource utilization. Routing systems, fair resource allocation, data aggregation, misbehavior detection, and distributed storage are all targets for these assaults [6]. Sybil attacks are unprotected on ad - hoc networks. Because most wireless sensor networks incorporate gateways or base stations, this attack can be avoided by adopting better protocols. Many studies have shown that without a central authority, this attack is always possible, with the exception of unrealistic assumptions like entity parity and coordination. It's difficult to detect Sybil nodes on the network.

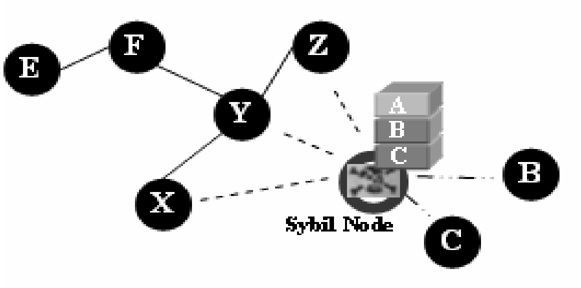

Fig. 1. Shows Sybil attack

- **Blackhole/Sinkhole Attack-**

In a black hole/sinkhole attack, a rogue node functions as a black hole, garnering all traffic in the WSN. [9] In a flooding-based scheme, the attacker watches for connection requests and then responds to the target nodes with the best and shortest pathway to the ground station. Any evil device that can fit between two communication nodes, such as a sink and a sensor, is capable of doing anything [13] with the bits that are passed between them. Such approach can even affect nodes that are located a long distance from the ground stations.

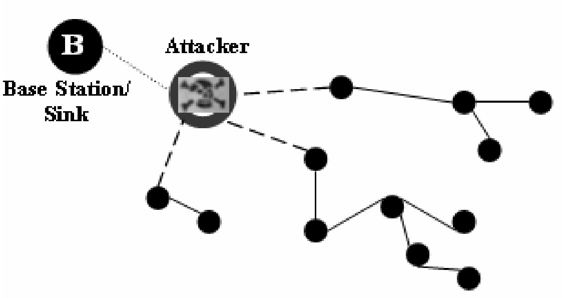

Fig. 2. Blackhole Attack

- **Hello Flood Attack-**

HELLO, packets are employed as a sidearm in this type of attack to ensure the detectors in wireless communication are secure. In this form of attack, the attacker uses high radio transmission to broadcast HELLO packets to monitoring stations that are dispersed across a large area inside the wireless sensor network. The sensors then are persuaded that their adversary is their next-door neighbor. As a consequence, after dispatching information to the base stations, the affected nodes attempt to pass via the intruder since they recognize it as their neighbor and are eventually scammed.

- **Wormhole Attack-**

The intruder records packets at a specific site in the network and then retransmits them to a separate location [12]. Packet forwarding can be done in a specific or selective manner. This sort of attack really doesn't need negotiating with a detector in the network because it may be carried out in the early stages of the sensor's search for surrounding facts, which makes it a significant threat to WSN.

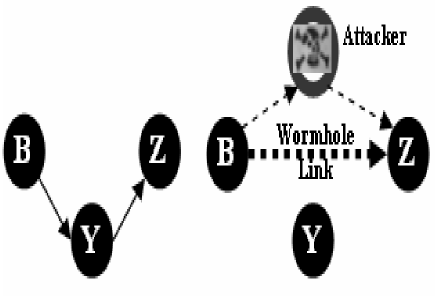

Fig. 3. Wormhole Attack

4 Basic Security Schemes

Security is a wide-ranging term that includes some features of authentication, privacy, integrity. As people's reliance on information (given by the network) grows, so does the risk of secure information transfer. Numerous strategies such as cryptography and steganography are used to assure reliable transfer of various forms of data through networks [11]. We've covered the foundations and strategies of cyber security, as well as how these techniques can be used to build a stable sensor network.

- **Cryptology-**

It is basically a method of keeping and transferring the data in a particular form in order to ensure the privacy of the person who intends to read and process it [15]. Techniques like encryption-decryption which are mainly conceived for the basic wired communicating technology are not attainable and are mostly required for wireless sensor technology [8]. Wireless Sensor Network contains small sensors and these sensors suffer from a lack of battery power and processing memory. To apply any encryption requires transmission of more bits, which can lead to more processing in the system and more consumption of memory and power of the battery. Also applying these mechanisms like encryption can also lead to delay and loss of packets in the network.

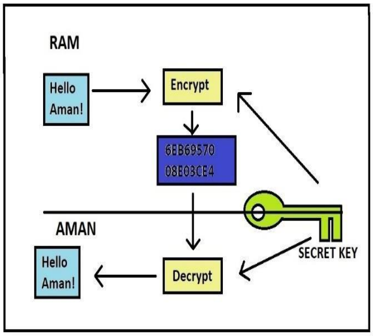

Fig. 4. Shows cryptography

- **Steganography-**

Steganography basically focuses on how to hide the existence of message whereas cryptography focuses on hiding the content of messages. It is basically a way of converting any communication by inserting message into the multimedia form attacks which are basically against the security mechanisms. The primary priority of hiding data is to change the messenger in a quite sense that it is undetectable and therefore appears to be conventional or common. As it suppresses the presence of the secret broadcaster, it's very beneficial if we want to submit secret data without revealing the sender's identity or if we want to publish secret data openly. Nevertheless, possessing or securing WSNs has nothing to do with processing digital evidence.

- **Physical Layer Secure Access-**

Frequency hopping can be used for securing access in the Physical layer of Wireless Sensor Networks. In order to ensure little damage so that storage, processor, and sources of energy and various dynamic combinations of specifications can be used like hopping set, dwell time, and hopping pattern [10]. Physical layer safe access is notable for its effective application, which allows the hopping sequences to be updated in far less time than it takes to discover it, and for applying it to both sender and recipient in order to maintain a synchronized clock. In terms of physical layer providing protection, there are a few key factors to consider, such as optimum organization.

5 Security Solution for Wireless Sensor Networks

Many studies on how to create safe smart sensors with varied voltage supplies in improving the energy efficiency during processing and thereby lengthen the broadcaster's life cycle [17] have been published. For key management in WSN, security systems focus on boosting energy efficiency. To detect the blocked zone in the wireless mesh mapping protocol is present, which also actually prevents the erroneous portion from continuing to route inside the network, consequently managing Dos assaults produced by jamming [3]. Wormholes, which were previously thought to be detrimental to wireless sensor networks, can now be employed as a reactive defense mechanism to avoid DoS assaults jamming.

The en-route filtering security technique is used to identify injected false data in wireless sensor networks, and it focuses on how to filter the data that is fraudulent using collective secrets, limiting any single point from breaching the entire system. SNEP and TESLA are two secure building elements that enable data freshness, broadcast authentication, and data confidentiality. TinySec, for example, proposes a link-layer security method for wireless sensor networks that essentially uses a well-organized symmetrical key encryption protocol.

Table1 summarizes different schemes related to security along with their properties which are proposed so far for WSN. This table also defines various attacks related to these security schemes, the network architecture of security schemes, and their significant features.

Table 1. Different security schemes for WSNs

S.No	Security Scheme	Attacks	Network Architechture	Features
1.	Wormhole Based	Dos Attack	Hybrid sensor network(This type of network is mainly wireless and to some extent wired)	To avoid jamming this type of attack uses a wormhole as a security scheme.
2.	JAM	Dos Attack	Traditional WSN	By using coal neighbour nodes jammed is region is avoided.
3.	Predistribution, Random Key, Radio Resource Testing[19]	Sybil Attack	Traditional WSN	It uses random key predistribution feature[5], Registration procedure, code attestation, and position verification to detect entry of any Sybil entity
4.	Multi- base multi – path station routing or Bidirectional verification.	Hello Flood Attack	Traditional WSN	It uses multi-path multi-base routing and bidirectional verification. It also adopts probabilistic secret sharing.
5.	On communication Security	Data and information Spoofing	Traditional WSN	It protects the network even if some part of the network is compromised. It also has efficient resource management.
6.	Random Key distributio n	Attacks on information in transit. Information and data spoofing.	Traditional WSN	It provides authentication measures for sensor nodes. Even if a portion of the network is compromised, it protects the entire network. It helps to provide resilience to the network [18].
7.	TIK	Information and Data wormhole attack, spoofing	Traditional WSN	It needs accurate time synchronization between all the communicating parties and implements temporal leashes. It is based on symmetrical cryptography.
8.	Statisticalenroutin g Filtering	Information Spoofing	Highly dense WSN. It has a large number of sensors.	It drops and detects the false report during the forwarding process.
9.	Tinysec	Information and data spoofing	Traditional WSN	It works in the link layer. It focuses on providing authenticity, integrity, and confidentiality to message.
10.	SNEP and TESLA[20]	Information and data spoofing	Traditional WSN	It focuses on semantic security, replay protection and data authentication, freshness.

6 Conclusion

It is seen that most of the attacks which are against security in WSN are mainly caused by the interjection of the false information which is mostly given by the compromised nodes which are present within the network. In order to defend the insertion of false information by the compromised nodes, a plan or mean is required to detect that false information or false report. Although, developing different detection mechanisms and making them resourceful and efficient constitutes is a great challenge for research. The major research issue is to ensure comprehensive security in WSN. Nowadays many security schemes are established on the specific type of network models, As there is a lack of united or grouped effort which is needed to take a common model in order to ensure security for each individual layer, though the security mechanisms will become well-established in coming future for each individual layer, it is important to combine or group all the mechanisms together in order to make them work in alliance or collaboration with each other which will ultimately incite a hard research challenge. Energy efficiency or cost-effectiveness is still the two biggest challenges in ensuring holistic security in wireless sensor networks.

References

[1] Yick, J., Mukherjee, B. and Ghosal, D. (2008). Wireless sensor network survey. *Computer networks*, 52(12): 2292-2330.

[2] Raghavendra, C. S., Sivalingam, K. M. and Znati, T. (2006). *Wireless sensor networks*. Springer.

[3] Xu, N. et al. (2004). A wireless sensor network for structural monitoring. In *Proceedings of the 2nd International Conference on Embedded networked sensor systems*, 13-24.

[4] Pottie, G. J. (1998). Wireless sensor networks. In *Information Theory Workshop (Cat. No. 98EX131),* 139-140.

[5] Perrig, A., Stankovic, J. and Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, 47(6): 53-57.

[6] Sohrabi, K. et al. (2000). Protocols for self- organization of a wireless sensor network. *IEEE personal communications*, 7(5): 16-27.

[7] Guy, C. (2006). Wireless sensor networks. In 6th I*nternational Symposium on Instrumentation and Control Technology: Signal Analysis, Measurement Theory, Photo-electronic Technology, and Artificial Intelligence*, 6357: 63571.

[8] Matin, M. A. and Islam, M. M. (2012). Overview of wireless sensor network. *Wireless sensor networks-technology and protocols*, 1-3.

[9] Rajaravivarma, V., Yang, Y. and Yang, T. (2003). An overview of wireless sensor network and appl networks. In *Proceedings of the 35th Southeastern Symposium on System Theory,* 432-436.

[10] Dargie, W. and Poellabauer, C. (2010). *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons.

[11] Li, J. et al. (2018). *Wireless Sensor Networks*. In *11th China Wireless Sensor Network Conference, CWSN*. 812.

[12] Du, X. and Chen, H. H. (2008). Security in wireless sensor networks. *IEEE Wireless Communications*, 15(4): 60-66.

[13] Li, Y. and Thai, M.T. (2008). *Wireless sensor networks and applications*. Springer Science & Business

Media.

[14] Werner, A. G. et al. (2006). Deploying a wireless sensor network on an active volcano. *IEEE Internet Computing*, 10(2): 18-25.

[15] Mainwaring, A. et al. (2002). Wireless sensor networks for habitat monitoring. In *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, 88-97.

[16] Mao, G., Fidan, B. and Anderson, B. D. (2007). Wireless sensor network localization techniques. *Computer Networks*, 51(10): 2529-2553.

[17] Pathan, A. S. K., Lee, H. W. and Hong, C. S. (2006). Security in wireless sensor networks: issues and challenges. In *8th International Conference Advanced Communication Technology*, 2: 6.

[18] Yoneki, E. and Jones, J. (2005). A survey of Wireless Sensor Network technologies.*UCAM-CL-TR-646*.

[19] Huang, C. F. and Tseng, Y.C. (2005). The coverage problem in a wireless sensor network. *Mobile Networks and Applications*, 10(4): 519-528.

[20] Wadaa, A. et al. (2005). Training a wireless send or network. *Mobile Networks and Applications*, 10(1): 151-168.