A Security Review in Wireless Networks

Dr Anubhav Soni

SOMC, Sanskriti University, Mathura, Uttar Pradesh, India

Email Id- anubhavs.somc@sanskriti.edu.in

ABSTRACT: ***Wireless Sensor Networks (WSNs) can be defined as auto-configured, non-infrastructure wireless networks to track and transfer their data to the main site or sink in the network, which allows for physical and environmental conditions such as temperature, son, vibration, stress, movement or pollutants to be observed and processed cooperatively. A sink or base station acts as a network-user interface. The data needed may be obtained from the network by placing queries and collecting answers from the drain. It is essential to protect this information since many wireless sensor networks are sensitive to the data. However, the limited nature of the tools accessible in sensor nodes, owing to their computer requirements, power consumption, speed and overhead communication, makes standard wireless networking security technology impossible. We analyze the dangers and assaults presented by WSNs and evaluate the current state-of-the-art WSN Safety Protocols and take into account their different strengths and weaknesses.***

KEYWORDS: ***Communication, Eavesdropping, Injection, sensor, Wireless Sensor Networks (WSNs).***

1. INTRODUCTION

It is preferred that a complete monitoring solution for wireless sensor networks include three characteristics; these are proactive, detective, and reactionary actions, respectively. As the name suggests, preventative measures aim to discourage assaults or, at the very least, make them more difficult to carry out. This is the area that has received the most attention since it provides authentication, integrity, and secrecy via the use of relatively common cryptographic primitives. The detection and differentiation between an attack and a network failure in wireless sensor networks (WSNs) are always challenging while an attack is underway, which is why detective procedures are required. It is critical that the network, whether it be the nodes themselves, the base station, or the end user, distinguish between these two possibilities in order to enable for reactive action to be done. When these reactive actions are performed when they are not required, the network's utility is substantially reduced[1].

Reactive steps may be implemented in a number of ways. First and foremost, by sending an order to each node on the network (which must be properly authenticated, of course), it can be as simple as shutting down the network, instructing them to disable all contact for a period of time, and instructing them to ignore all communication for the same period of time. In the hope that the attacker will eventually leave and that normal functioning will be resumed, this makes it far more difficult for the attacker to operate while preserving the energy capacity of the nodes in the network. Another simple option is to allow the network to continue to function as normal, providing the attacker with no indication of identity before dealing with the attacker, but to disregard all communications. These two methods offer resilience, since the network can recover once the assault has subsided; nevertheless, a determined and patient attacker may disable the network for as long as it is feasible to do so. Responses that are more sophisticated include changing the degree of security while an attack is in progress, silencing just penetrated portions of a network, neutralizing assaults, or even counterattacking an attack that has already begun. The implementation of these processes on wireless sensor nodes is hampered by the limited computing, memory, and energy resources available. Therefore, WSN security is a trade-off between what is required, what is desirable, and what is feasible in a real-world setting. The fact that WSNs are left neglected is the last major impediment to acquiring them. This gives the attacker complete freedom to carry out assaults that would be impossible to carry out on another kind of network. Physical assaults, attacks on replication of nodes, and attacks on the remote administration interface, which is also needed, are all examples of what is covered[2].

1.1 Wireless Sensor Networks (WSNS) Security Requirements:

The Wireless Sensor Network (WSN) is made up of geographically dispersed autonomous sensors that are used to monitor the earth's environmental conditions. Developing wireless sensor networks for military purposes such as battlefield monitoring was a driving force behind the technology's creation. Wireless Sensor Networks (WSN) are used in high-risk areas such as surveillance, monitoring, airports, and combat applications; thus, protecting wireless sensor networks is a difficult job. In Wireless Sensor Networks, the following are the security requirements that must be met[3].

1.1.1 Maintaining Confidentiality:

The need for confidentiality is necessary in order to guarantee that sensitive information is properly safeguarded and does not become available to unauthorized third parties. The confidentiality goal contributes to the protection of information flowing between sensor nodes in a network or between sensors and a base station from disclosure, since an adversary with the proper equipment may be able to eavesdrop on the connection. The attacker might overhear crucial information such as sensing data and routing information if they were to eavesdrop on the conversation. The sensitivity of the data stolen determines how serious the harm may be caused by an enemy, who can use the sensing data for a variety of unlawful reasons, such as sabotage or blackmail. For example, rivals may utilize the information to improve their products, such as in the case of a safety monitoring sensor application. Aside from that, the attacker may add his own malicious nodes onto the network in an effort to overhear the whole conversation by collecting routing information. The requirements for security in wireless sensor networks are shown in Figure 1.

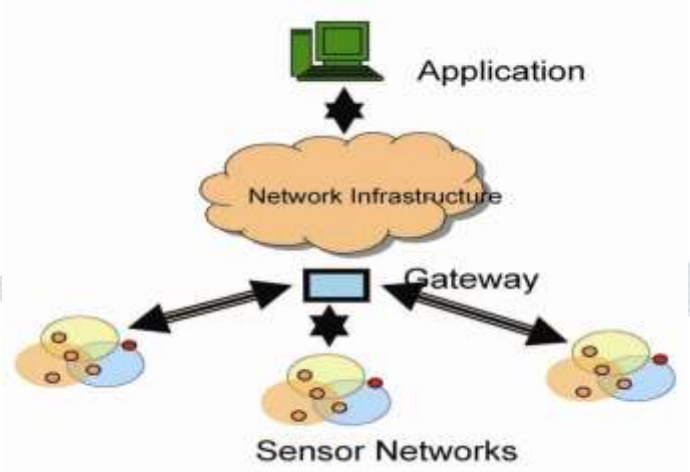

Figure 1: Security requirements in Wireless Sensor Networks [KRAZYTECH].

If we regard eavesdropping to be a network-level danger, then a hacked node that an adversary has in his hands might be considered a local-level threat. In addition, compromised nodes pose a significant danger to the confidentiality goal since the adversary may obtain important data kept on the nodes, such as cryptographic keys that are needed to encrypt the communication, from the compromised nodes[4].

1.1.2 Verification of Identity:

For the same reasons as in traditional systems, authentication methods check the identity of the participants in a communication, differentiating authorized users from intruders as a result of this. As a result, it is critical for each sensor node and base station to have the capability of determining whether or not the data it receives came from an authorized source rather than an enemy who fooled genuine nodes into accepting erroneous information. If this occurs, and incorrect input is given into the network, the behaviour of the network cannot be anticipated, and the majority of the time, the result will be different from what was intended.

When clustering of nodes is done, it is critical that the authentication goal be met in order to be successful. When nodes in a sensor network are clustered, they are grouped based on some attribute such as their location, sensing data, or other similar data. Each cluster has a cluster head, which is a node that connects its cluster to the rest of the sensor network, and each cluster has one or more cluster heads (meaning that the communication among different clusters is performed through the cluster heads). In these situations, where clustering is required, there are two authentication scenarios that should be investigated: first, it is critical to ensure that the nodes contained in each cluster will only exchange data with the authorized nodes contained and which are trusted by the specified cluster; and second, it is critical to ensure that the nodes contained in each cluster will exchange data only with the authorized nodes contained and which are trusted by the specified cluster (based on some authentication protocol). If, on the other hand, nodes within a cluster receive data from nodes that are not trusted by the present community of nodes and proceed to process it, the anticipated data from that cluster will be based on fake data and may result in significant harm. When it comes to the second authentication scenario, it includes communication between the cluster leaders of each cluster; contact must only be made with cluster heads who can provide proof of their identity. No hostile node should be able to pose as a cluster head and interact with a genuine cluster head, transmitting fake data or compromising the data that is transferred between the two nodes in question[5].

1.1.3 Integrity:

As we go on to the integrity goal, there is a risk that information may be tampered with if it is transmitted via an unsecured network. Because the implications of utilizing incorrect information may be catastrophic, for example, in the healthcare industry, where lives are at risk, a lack of integrity could lead to a slew of issues.

Implementing integrity controls will guarantee that information is not changed in an unanticipated manner. Many sensor applications, such as pollution and healthcare monitoring, rely on the integrity of the information to function properly and produce accurate results. It would be unacceptable to measure the magnitude of pollution caused by chemical waste only to discover later that the information provided had been improperly altered by a factory located near the monitored lake. Because of this, it is critical to ensure that information is sent from one end to the other without being intercepted or changed during the transmission process[6].

1.1.4 The State of Being Fresh:

Assaults on sensor networks include a variety of different types of attacks such as message replay attacks, in which an adversary captures messages sent between nodes and replays them later to create confusion in the sensor network. Using the data freshness goal, you can verify that messages are new, which means that they follow the message ordering and have not been repeated. In order to maintain freshness, network protocols must be built in such a manner that duplicate packets are identified and discarded, thus avoiding possible mix-ups.

1.1.5 Secure Management:

Every system that is composed of several components and that handles sensitive information need the involvement of management. In the case of sensor networks, secure management at the base station level is required; because all communication between sensor nodes and the base station is terminated at the base station, issues such as key distribution to sensor nodes in order to establish encryption and routing information need to be managed securely. Furthermore, clustering necessitates safe administration, since each group of nodes may include a significant number of nodes, all of which must be authenticated with one another and communicate data in a secure way. Furthermore, the clustering inside each sensor network may vary in a dynamic and fast manner. As a result, secure group management protocols are needed for the purposes of adding and deleting members, as well as authenticating data from groups of nodes[7].

1.1.6 Availability of Resources:

When services and information are available, it means that they may be accessible at the moment of need. There are many dangers in sensor networks that may result in a loss of availability, including sensor node capture and denial of service assaults. Because many important real-time applications, such as those in the healthcare industry, need continuous operation around the clock, a lack of availability may have a detrimental effect on their functioning, and may even result in the loss of life. As a result, it is essential to guarantee system resilience against assaults aimed at reducing system availability and to devise methods of filling in the vacuum left by the capture or disablement of a particular node by delegating its responsibilities to other nodes in the network.

1.1.7 The Level of Service Quality:

The achievement of the Quality of Service goal is a major source of concern for security. And when we're talking about sensor networks, with all of its inherent constraints, the ability to provide high-quality service becomes much more limited. Security methods must be lightweight in order for the overhead imposed by, for example, encryption to be kept to a minimum and the network's performance not to be adversely affected. Performance and quality in sensor networks include the prompt transmission of data in order to avoid, for example, the spread of pollution, as well as the precision with which the data provided matches what is really happening in their surroundings, among other things[8].

1.2 Threats:

Malware assaults on wireless sensor networks are more common than on regular wireless networks, making them more susceptible. Challenges to WSNs may be classified in a number of ways depending on the skills of the attacker, the degree to which the attacker has control over the network, and the level of interference caused by the attacker. First and foremost, computers having the same functionality as the sensor nodes on the network may be exploited by an attacker, either by adding sensor nodes to the network distribution area or by subverting any of the sensor nodes under assault on the network, to get access to sensitive information. Because the attacker only has the same resources, especially in terms of energy and computing capability, as the nodes under assault, the spectrum of attacks is limited when using this approach. A second possibility is that the intruder makes use of a

personal computer or laptop equipped with the necessary radio, or maybe an even more powerful dedicated device, which would be able to communicate at a much greater power level than the radios on the sensor motors. Because of the much increased energy supply, processing capability, and memory, as well as the significantly reduced contact latency, this option offers up even more potential attack vectors[9].

When trying to secure a sensor network, the most difficult issue is preventing this kind of invader from entering the network. Assaults may also be divided into two categories: attacks by outsiders and attacks by insiders. An attacker would not become a member of the network if he or she was attacking from the outside. In order to actively listen to the contact on the network, an external intruder may choose to use a method that is extremely difficult to detect. To defend against this kind of assault, however, the only safeguard usually needed is the adoption of an extremely strong cryptographic algorithm that ensures secrecy is maintained. An external invader may also be able to alter the contact medium in a direct manner. This may be accomplished by interfering with (i.e. jamming) or altering network packets, or by introducing bogus packets into the network. Techniques for packet modification and injection will be detected and stopped by techniques for authentication, integrity, and replay protection. Interruptions assaults are tough to defend against, despite the fact that they are often simple to detect, especially when dealing with an invader from the PC/laptop class. An insider attack occurs when malicious code is run on nodes that are legitimate network users, as in a computer network. In this scenario, the attacker always has access to at least a subset of valid concealed cryptographic keys that are utilized on the network in question. Identifying and revocation of the keys held by those infected nodes, as well as ignoring any potential communication from such nodes, is the greatest protection against an insider attack. However, this is a very tough issue to solve in general[10].

Because of the possibility that an intruder may get physical access to the sensor nodes, WSNs provide a unique set of challenges that are not encountered by conventional ad-hoc wireless networks. The reason for this is because WSN installations are unmanaged and open in nature, as previously stated. This physical access opens the door to a variety of dangers, including the reprogramming of malicious code sensor nodes, the extraction of secret information from the nodes, such as cryptographic keys, and even the physical destruction of the sensor nodes. Tamper-proof hardware is your sole option for protecting yourself against the first two types of attackers. However, for one particular kind of attacker, this is both very expensive and not always effective. There is only one way to protect nodes from physical destruction: to encase them in robust enclosures that are impervious to destruction. However, this method is usually prohibitively expensive, not to mention the effect that such circumstances may have on radio contact or the sensors themselves.

1.3 The Difficulties of Sensor Networks:

In developing security methods for large, ad hoc wireless sensor networks, the nature of the networks poses major difficulties. A wireless sensor network (WSN) is a unique network that differs from a conventional computer network in that it has numerous restrictions.

- *Wireless Medium*: The wireless medium is intrinsically less secure due to the fact that it broadcasts information, making eavesdropping easy to do. Almost every communication may be intercepted, changed, or replayed by a malicious party with relative ease. An attacker may simply intercept legitimate packets and insert malicious ones via the wireless channel, which makes it difficult to detect them.
- *Ad-Hoc Deployment:* Because sensor networks are ad-hoc in nature, no static structure can be established for them. The topology of a network is constantly susceptible to change as a result of node failure, addition, and movement. Nodes may be delivered by airdrop, in which case the topology of the network is unknown prior to deployment.
- *Hostile Environment:* The next difficult element to overcome is the hostile environment in which sensor nodes operate, which warns them of the risk of destruction or capture by attackers as they operate. Because nodes may be located in a hostile environment, attackers may be able to obtain physical access to the device with relative ease.

1.4 WSN Security Mechanism Technology:

Security mechanisms are really used in order to identify, prevent, and recover from security-related incidents. A broad range of security schemes may be developed to defend against malicious assaults, and they can be divided into two categories: high-level security schemes and low-level security schemes. The following are examples of low-level security mechanisms primitives for security sensor networks:

- Key establishment and trust establishment: One of the most essential aspects of sensor network security is programmable and controlled group communication, which is one of the most significant aspects of sensor network security. The creation of cryptographic keys is the first and most important step in the process of setting up a sensor network. To expand the network to hundreds of nodes, a key-establishing method is used.
- Most sensor network applications need security against eavesdropping, injection, and alteration of packets. Secrecy and authentication are two important aspects of this protection. The most common kind of defense is cryptography. The usage of link layer cryptography in the early stages of sensor networks is likely due to the fact that it is the most straightforward of the network cryptographic methods presently available.
- Providing secure routing or data forwarding is a crucial function in sensor networks since it allows for communication to take place. Unfortunately, the present routing system is plagued by a slew of security flaws and vulnerabilities.
- Privacy: Sensor networks, like any other conventional network, have prompted privacy concerns among its users. It is possible that sensor networks that are first deployed for legal purposes may be utilized in unexpected ways in the future. Making people aware of the existence of sensor nodes and the data collection process is especially essential.

2. DISCUSSION

Attacks on wireless sensor networks may be either noninvasive or intrusive, depending on their nature. Non-invasive assaults, in general, consist of side-channel attacks, such as attacks based on strength, timing, or frequency, or attacks based on a combination of these. Although there has not been any published work on side channel attacks specifically targeting WSNs, many of the problems identified with other embedded systems, such as timing attacks against MAC generation or encryption, may be applied to sensor nodes. Invasive attacks are considerably more common than other types of assaults, and they are the ones that are discussed in the following sections as the most serious.

The most common attacks against WSNs are those that rely on information in transit between nodes. The transmission of information is susceptible to eavesdropping, modification, injection, interruption, and inspection of traffic while in route. As previously mentioned, utilizing well-established protocols of secrecy, authentication, credibility, and replay protection, it is feasible to prevent eavesdropping, alteration, and injection while maintaining confidentiality, authenticity, credibility, and replay protection. For attackers in WSNs, traffic analysis may potentially be a major problem since it allows them to map a network's routing topology, enabling them to launch extremely narrowly targeted assaults that have a disproportionately large effect.

A node duplication attack consists of an attacker injecting a new node into a network that has been cloned from an existing node, which is a very simple operation given the ease with which contemporary sensor node hardware can be copied. In some cases, this new node will behave precisely like the previous node, but in other others, it may exhibit some extra behaviour, such as openly sending important information to the attacker. The issue with the second scenario is obvious, but the first condition will have a subtle but significant effect on the network, causing routing algorithms, data aggregation algorithms, and querying algorithms to fail, among other things. The consequences of a node duplication assault are more severe when the base station has been cloned. Nonetheless, since the base station is located in a protected area and is much more efficient than the rest of the sensor nodes in some deployments, cloning it is significantly more difficult.

3. CONCLUSION

The security methods described here can all be used to secure a WSN effectively, but there is presently no single solution that can be 'plugged-in' to an application and offer all of the primitives required for security. This article discusses the many assaults that may be launched against the Bluetooth network. Specifically, it has been shown that the Bluetooth network is vulnerable to a variety of attacks. In the conclusion, we think that wireless sensor networks are particularly susceptible to denial of service (DOS) assaults because of the availability of PC/laptop-type attackers. A distributed denial of service (DDoS) attack on the physical layer is characterized by the continuous transmission of a signal that interferes with the radio frequencies utilized by the sensor network. This jamming may be either persistent or periodic in nature, and it can be carried out by a number of devices in the node class or by a single high-capacity computer.

REFERENCES

[1] K. S. Mulyarchik and A. S. Polochanskiy, “Quality of service in wireless sensor networks,” *Zhurnal Beloruss. Gos. Univ. Mat. Inform.*, 2017,

doi: 10.5120/ijca2020920036.

[2] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements," *IEEE Access*. 2017, doi: 10.1109/ACCESS.2017.2666200.

[3] 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.

[4] S. Srivastava, M. Singh, and S. Gupta, "Wireless Sensor Network: A Survey," 2018, doi: 10.1109/ICACE.2018.8687059.

[5] C. B. Priya and S. Sivakumar, "A survey on localization techniques in wireless sensor networks," *Int. J. Eng. Technol.*, 2018, doi: 10.14419/ijet.v7i1.3.9671.

[6] F. Kiani and A. Seyyedabbasi, "Wireless sensor network and Internet of Things in precision agriculture," *Int. J. Adv. Comput. Sci. Appl.*, 2018, doi: 10.14569/IJACSA.2018.090614.

[7] K. B. Vikhyath and S. H. Brahmanand, "Wireless sensor networks security issues and challenges: A survey," *Int. J. Eng. Technol.*, 2018, doi: 10.14419/ijet.v7i2.33.13861.

[8] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Networks*, 2008, doi: 10.1016/j.comnet.2008.04.002.

[9] S. Sweta and B. Maram, "Underwater wireless sensor networks," *Int. J. Informatics Vis.*, 2018, doi: 10.30630/joiv.2.1.99.

[10] H. Modares, A. Moravejosharieh, R. Salleh, and J. Lloret, "Security overview of wireless sensor network," *Life Sci. J.*, 2013.