ISSN No:-2456-2165

Security Issues in Wireless Sensor Networks: Challenges, & Solutions

*Kalu, Jonah[1]; Oko, Christian Obinna[2]; Njoku Chiemezuo[3], Kenekayoro Ekiokekeme[4]
[1,2]Department of Science Laboratory Technology, Federal Polytechnic, Ebonyi, Nigeria.
[3,4]Department of Electrical & Electronics Engineering Technology, Federal Polytechnic, Ebony, Nigeria

Abstract:- Wireless Sensor Networks (WSN) is a relatively new and promising technology in wireless communication that has wide range of applications. Nonetheless, security threats common with WSNs have continued to cause serious concerns to researchers. This is so as there is no well-defined and holistic security approach covering all forms of WSNs due to the vulnerable nature and complexity of this type of network. Different security threats to WSNs have been reviewed in this paper, as well as their cause, effects, and counter measures. Section 1 of the paper introduces the concept of WSNs, its makeup, design, and applications as well. Section 2 reviews some related works in the area while section 3 presents the security requirements of WSNs. Section 4 deals extensively on different security attacks that are common with WSNs, outlining their causes, impacts, and some defense mechanisms that can be adopted against them. Section 5 highlights some of the factors militating against the achievement of security efficiency in WSNs. Finally, section 6 of the paper makes some observations and recommends on the best approach towards tackling security challenges in WSNs.

Keywords:- *WSNS, Security Challenges, Attacks, Intruder, Information.*

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are a peculiar type of network comprising of sensors that are independent and distributed spatially in space. They are used to monitor, collect, and transmit data regarding environmental conditions and physical states of a given location. Such information may include: pressure, humidity, temperature, of a given geographical location and may be transmitted using the network to a collation centre, analyzed and utilized for several decision making. As a result of its broadcast nature and pattern of deployment, WSNs are usually exposed to many threats in terms of security.

1.1 Basic Architecture of WSNs

Figure 1 shows the basic architecture of WSNs. The layout includes a base station, some sensor nodes, and gateway [1].

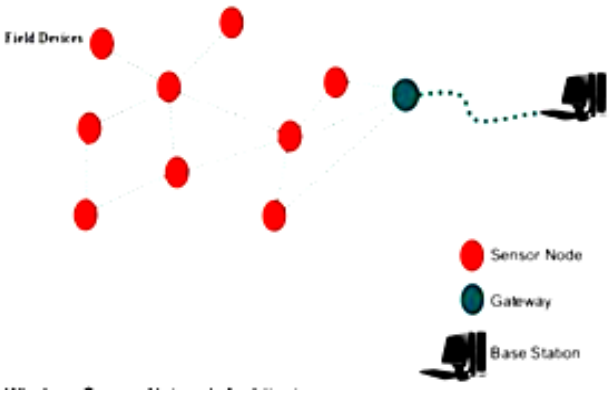

Fig 1: Schematic representation of WSN Architecture (Rahaman & Aziz, 2016).

1.2. APPLICATIONS OF WSN

WSN can be applied in several ways. Figure 2 below outline the different areas where WSNs as a technology have found application [2].

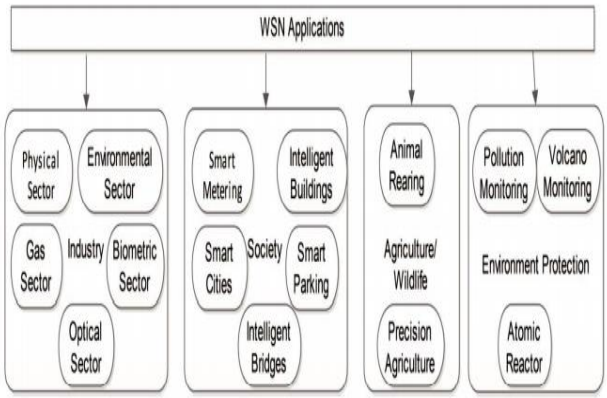

Fig. 2: WSN Application Areas (Bangash *et.al*. 2017)

II. RELATED WORKS

Over the years, lots of interesting results have emanated from various research works dealing with security threats confronting WSNs. It was proven that without a centralized control, WSNs will be largely exposed to high volumes of Sybil attacks, as discovered through tests that confirmed the presence of Sybil nodes in WSNs [1].

From experimental results, it took about three and half months to decode a data protection key encryption algorithm (consisting of 64-bits) that was employed to ensure privacy using computers that have ultra-fast computational abilities to run at 1012 passwords per second. At this rate, it will take 5.4∗1018 years for a computer that runs at 128-bit to execute exactly the same task, but the logic remains how reasonable it is to deploy such a huge key in WSNs where there already exists heavy constraints in terms of network resources [2].

Results clearly show that most attacks on WSNs arise from false information inputted into the network by intruders using certain compromised nodes [3].

In comparison to other common computer networks, designing an efficient security scheme for WSNs pose greater challenges due to their complex structure [4].

For WSNs, a holistic approach is required to tackle security challenges in the network as providing separate security schemes for the different layers within the network may not provide the desired result of achieving security efficiency within the network. A scheme is required that will guarantee security at every layer within the network, hence achieving a high level of efficiency in the security of the entire network. [5].

III. WSN SECURITY REQUIREMENTS

The overall target of providing security in WSNs in to guarantee protection all levels i.e. network, node, data, and the OS levels. Figure 3 provides an outline of the different forms of security threats identified to be common with most WSNs [2].

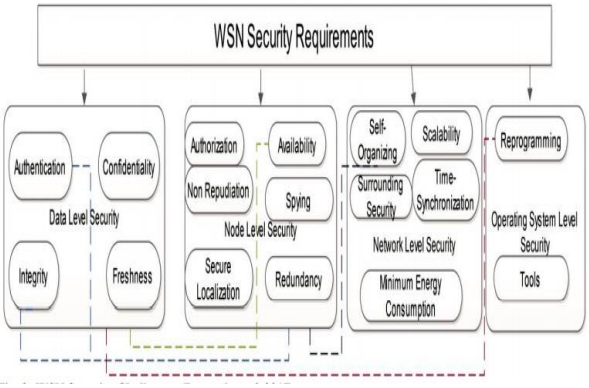

Fig. 3: WSN Security Challenges (Bangash *et.al*, 2017)

IV. SECURITY ATTACKS IN WSN, CAUSES AND DEFENSES

Due to the broadcast nature of its transmission and mode of deployment, WSNs are usually exposed to various security attacks. These attacks are broadly divided into two categories as passive and active attacks [5].

4.1 Passive Attacks

These are attacks that involve an intruder monitoring and listening to channels of communication. Some passive attacks common with WSNs include:

4.1.1 Camouflage Adversaries.

Camouflage adversaries attack occurs when an intruder taps information from the network either through an already existing node that has been compromised or a fake node that has been successfully inserted into the network. The intruder usually does this through the redirection of packets or attracting and withholding such packets [4].

.

4.1.2 Monitoring and Eavesdropping

This occurs when an intruder gains access into the communication channel and can snoops into data being transmitted along the channel. This leads to a compromise in confidentiality of information being transmitted. Of all the forms of attacks on privacy, it is the most common [4]

4.1.3 Traffic Analysis

Even when the data being transmitted along a communication channel have been encrypted, there are times when the sensor nodes may reveal the pattern of communication. An intruder may pick up and decode these revealed traces of communication pattern. The intruder may be able to use this vital information to cause harm within the network [4].

4.2 Active Attacks

If the data that is being transmitted along a channel of communication is accessed and successfully altered by an intruder, an active attack is said to have taken place. The different types of active attacks include [4].

4.2.1 Routing Attacks

The network layer is usually affected by these forms of attack. These attacks normally occur in the course of routing messages along the network and include the following [4].

4.2.1.1 Selective Forwarding

In wireless sensor networks (WSNs), received messages are assumed to be always forwarded on arrival at the nodes hence an intruder will always take advantage of this by generating large amounts of packets through the introduction of disruptive packets at certain nodes. This high data traffic arising from excess packet flow eventually overwhelms the nodes, thereby leading to packet losses as a result of dropping of packets at the nodes [4].

4.2.1.2 Hello Flood Attacks

In this type of attack an intruder deploys “HELLO packets” to be used as tools in deceiving sensor nodes within the WSN. Hello flood attacks usually involve the use of “laptop class attacker”, which are a form of high radio transmission. The HELLO packets is processed and then introduced into the network by this high class attacker using some sensors that are distributed within the WSN. Within the network, the sensors that are affected mistake the compromised nodes as complimentary nodes. During signal relay, the compromised node is spoofed by the attacking

node while the former passes over the latter thinking it is one of the neighboring sensor nodes [5].

4.2.1.3 Information-in-Transit Attacks

Information-in-transit attacks usually occur during the transmission of information gathered within the network to the base station through the sensors. This form of attacks usually arises when an intruder eavesdrops into the network to monitor data traffic and intercept data so as to either corrupt the original information or falsify it by introducing fake packets. It can involve deletion of some portions of the original information, or replication of some parts of the information so as to render it either meaningless or alter the meaning [4].

4.2.1.4 Black hole Attack

In WSNs, a black hole attack otherwise known as a sinkhole attack involves sending a route reply (RREP) message into the source node through a malicious node. This establishes the shortest path to the destination node which eventually allows the intruder to send data packets to the malicious node who in turn distributes these packets within the entire network [6].

The diagram below shows a conceptual image of black hole or sinkhole attack [5].

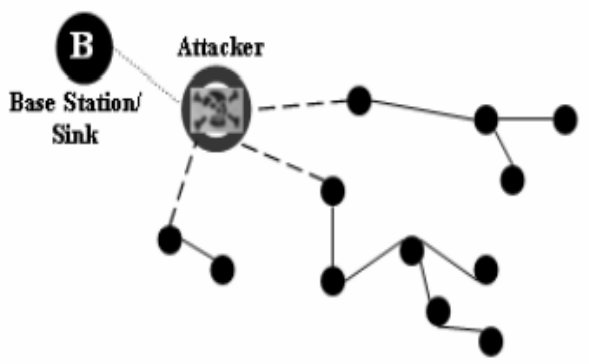

Fig. 4: Concept of Black Hole or Sinkhole Attacks (Pathan *et al,* 2006)

4.2.1.5 Sybil Attack

This type of attack involves a node compromising data integrity, network security, and network resources which the distributed algorithm has been adapted to utilize. This usually occurs by the malicious node faking its appearance to assume the form of several nodes within the network and hence compromise he network by distorting the routing mechanism, network resource distribution, storage, voting, data aggregation, as well as detection of malfunction.

Though it seems a common occurrence with Peer-to-Peer networks, Sybil attacks in WSNs can be prevented to some extent due to the presence of well defined gateways like base stations. Though not so easy, this however can possibly be achieved with the use of very effective protocols [5].

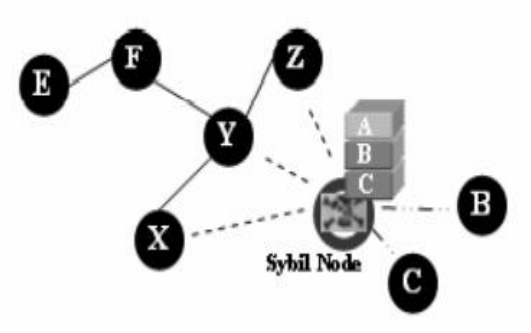

Fig. 5: Sybil Attack (Pathan *et al,* 2006)

4.2.1.6 Wormhole Attack

Wormhole attack is a serious form of attack that involves retransmission or tunneling of packets by an intruder within a network. It can occur at the signaling stages when information exchanges occur between neighboring sensors. It poses serious threats to wireless sensor networks as it can occur even without compromising any of the sensor nodes within the network. It is a situation whereby within a network, an intruder gains access, intercepts data packets at one point and tunnels or retransmits same packets to some other points within the same network. The retransmission or tunneling of the data packets could be selective or non-selective thereby either changing the original meaning of the message or rendering the message completely meaningless [5].

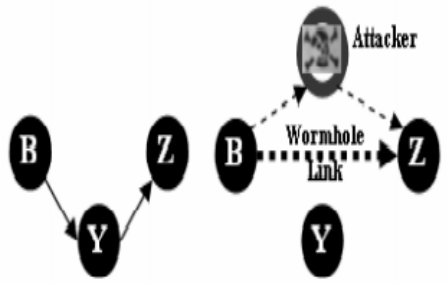

Fig. 6: Worm Hole Attack (Pathan *et al,* 2006)

Taxonomy of the different forms of security attacks common with WSN as well as their causes and defenses is as shown in figure 7 below [2].

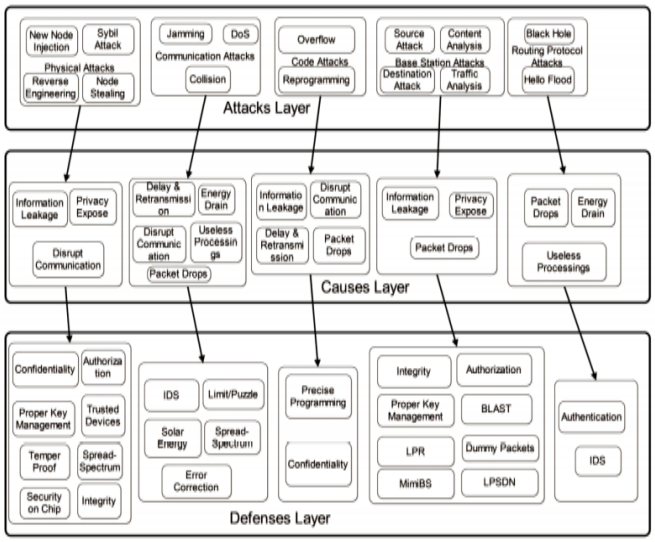

Fig. 7: Taxonomy of WSN Attacks, Causes, and Defenses (Bangash *et.al,* 2017).

V. CONSTRAINTS MILITATING AGAINGST EFFECTIVE SECURITY IN WSNs

Wireless Sensor Networks (WSNs) are unique in their nature in that they are confronted with some limitations that are alien to regular computer networks. In designing and deploying WSNs, these peculiar attacks need to be given special considerations before adopting any security approach or architecture [3].

Some major factors constraining the development or actualization of effective security architecture for WSNs as outlined in [1] include:

1. Scarcity and cost of network resources.
2. Vulnerability of the communication channels in WSNs,
3. Large sizes of the networks.
4. Unmanned nature of the network operations.
5. Ad-hoc mode of deploying the networks.
6. Crude nature of their operating environments.
7. Wireless medium of communication.

VI. CONCLUSION

As much as Wireless Sensor Networks (WSNs) hold great potentials in terms of their applicability, their nature and modes of operations makes them very vulnerable to many security attacks. These security challenges have continually been a source of great concern to many scientific researchers. Up till this moment, providing a clear-cut approach in solving these issues holistically has been elusive as achieving efficient security in WSNs will require a scheme that has the capacity to detect all the possible entry points for attacks within the entire network. This huge task calls for further research as most of the schemes for providing network security are modeled after certain networks that which most often are not as complex as WSNs.

REFERENCES

[1]. Rahaman, M., & Aziz, A. (2016). Security Issue and Challenges in Wireless Sensor Networks: A Survey and Attacks. International Journal of Scientific and Engineering Research, 7(8), Pp 1960- 1970

[2]. Bangash, Y.B., Abid, Q.D., Ali A.A., Al-Salhi, Y.E.A.0 2017. Security Issues and Challenges in Wireless Sensor Networks: A Survey. IAENG International Journal of Computer Science, 44(2), Pp 135-149.

[3]. Thirumalaimuthu, G., Lawrence, E.E., and Meenakshi, S. (2016). Security in Wireless Sensor Networks: Issue and Challenges. International Journal of Computer Application, 6(2), Pp 145- 151.

[4]. Kumar, V., Jain, A., Barwal. P.N. (2014). Wireless Sensor Networks: Security Issues, Challenges and Solutions. International Journal of Information and Communication Technology, 4(8), Pp 859-868.

[5]. Pathan, K.A., Lee, H., & Hong, C.S. (2006). Security in Wireless Sensor Networks: Issues and Challenges. ICACT, Pp 1043-1047.

[6]. Ghujar U., and Pradhan J. (2016). A Study on Black Hole Attack in Wireless Sensor Networks in Conference of Next Generation Computing and its Applications in Science and Technology, IGIT, Sarang, pp 1-3.