ISSN 2229-5518

Attacks in Wireless Sensor Networks

Rishav Dubey, Vikram Jain, Rohit Singh Thakur, Siddharth Dutt Choubey

Abstract— Wireless Sensor Networks is an emerging technology.WSN has limitations of system resources like battery power, communication range and processing capability.WSNs are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. One of the moajor challenges wireless sensor networks face today is security, so there is the need for effective security mechanism .In this artical we investigate how wireless sensor networks can be attacked in practice.

Index Terms— wireless Sensor Network, Attacks in WSN, Security Attacks, vulnerability,clone Attack,Man in the middle attack,jamming,sinkhole,warmhole attack,tampering,flooding.

1 INTRODUCTION

Sensor node in WSN is the combination *of MEMS technology (micro-electro-mechanical systems), wireless communications, and digital electronics* [8].The sensor node is low-cost, low-power, multifunctional device that is small in size and communicate in short distances. In WSN, a mass of wireless sensors are linked together via RF communication links. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes.

Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. Sensor nodes carry limited, normally not changeable, power sources. Therefore, while traditional networks aim to achieve high quality of service (QoS) provisions, sensor network protocols must focus primarily on power conservation. They must have inbuilt trade-off mechanisms that give the end user the option of prolonging network lifetime at the cost of lower throughput or higher transmission delay.

A WSN is usually collection of hundreds or thousands of sensor nodes. These sensor nodes are often densely deployed in a sensor field and have the capability to collect data and route data back to a base station (BS). A sensor consists of four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit [8]. It may also have additional application-dependent components such as a location finding system, power generator, and mobilizer (Fig. 1). Sensing units are usually composed of two subunits: sensors and analog-to-digital converters (ADCs). The ADCs convert the analog signals produced by the sensors to digital signals based on the observed phenomenon. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes. A transceiver unit connects the node to the network. One of the most important units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells). Most of the sensor network routing techniques and sensing tasks require knowledge of location, which is provided by a location finding system. Finally, a mobilizer may sometimes be needed to move the sensor node, depending on the application.

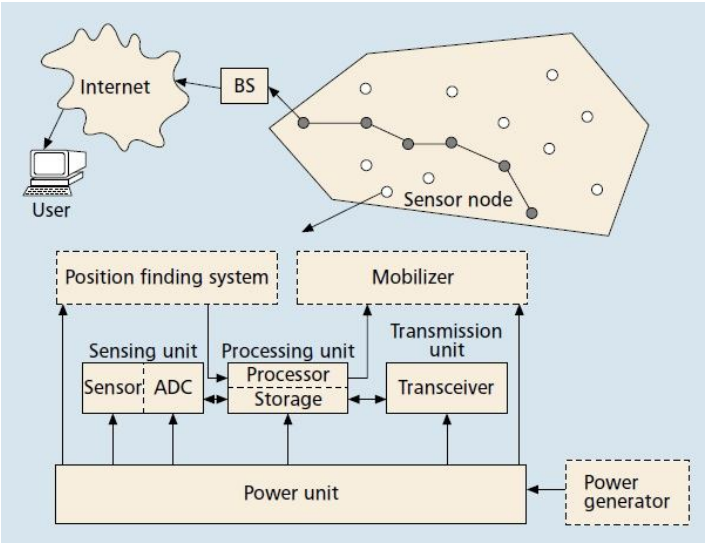

Figure 1: Components of Sensor Nodes [8]

There are a lot of its applications in military, health and industry. Many of WSN applications such as military and healthcare are critical and required certain level of security. Therefore it is necessary to provide wireless sensor network not only with the acceptable reliability of services but also adequate level of security. As sensor devices are restricted, security in WSNs is a challenging task and the networks exposed to various kinds of attacks and conventional defenses against these attacks are not suitable [4][7].

2 WSN & ADHOC NETWORK

As WSNs are lots of similar to traditional wireless ad hoc networks, important distinctions exist which greatly affect how security is achieved. In [8], I. F. Akyildiz et al proposed The differences between sensor networks and ad hoc networks are:

1. The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
2. Sensor nodes are densely deployed.
3. Sensor nodes are prone to failures due to harsh environments and energy constraints.

4. The topology of a sensor network changes very frequently due to failures or mobility.
5. Sensor nodes are limited in computation, memory, and power resources.
6. Sensor nodes may not have global identification.

3 PROTOCOL STACK

The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers defined as follows [4]:

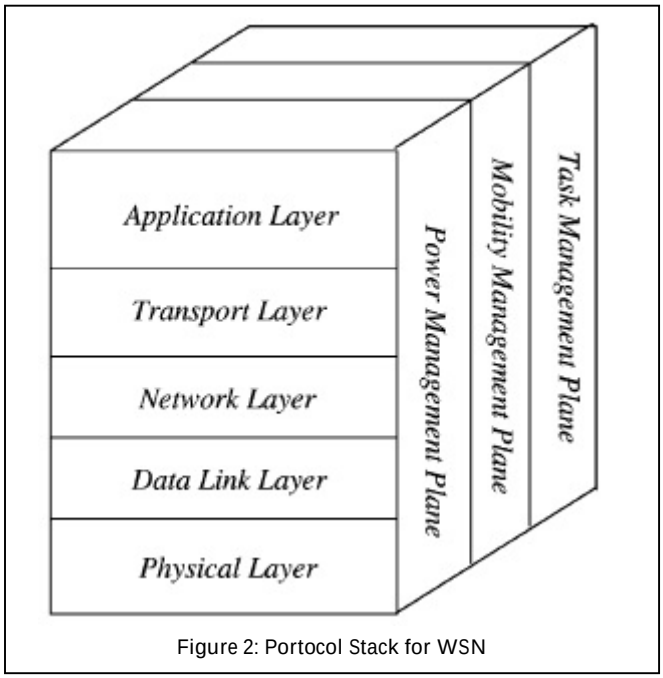

Figure 2: Portocol Stack for WSN

1. **Physical layer:** responsible for frequency selection, carrier frequency generation, signal deflection, modulation, and data encryption.
2. **Data link layer:** responsible for the multiplexing of data streams, data frame detection, medium access, and error
3. control; as well as ensuring reliable point-to-point and point-to-multipoint connections.
4. **Network layer:** responsible for specifying the assignment of addresses and how packets are forwarded.
5. **Transport layer:** responsible for specifying how the reliable transport of packets will take place.
6. **Application layer:** responsible for specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user.

Power management plane manages how a sensor node uses its power. For example, the sensor node may turn off its receiver after receiving a message from one of its neighbours. This is to avoid getting duplicated messages.

Mobility management plane detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who are their neighbor sensor nodes.

Task management plane balances and schedules the sensing tasks given to a specific region.

4 SECURITY REQUIREMENTS

The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. The security requirements in WSNs include:

1. **Availability**, which ensures that the desired network services are available even in the presence of denial-of-service attacks
2. **Authorization,** which ensures that only authorized sensors can be involved in providing information to network services
3. **Authentication,** which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node
4. **Confidentiality,** which ensures that a given message cannot be understood by anyone other than the desired recipients
5. **Integrity,** which ensures that a message sent from one node to another is not modified by malicious intermediate nodes

4 COMMON ATTACKS IN SENSOR NETWORK

4.1 Clone Attack

Clone attack also known as node replication attack, is a severe attack in WSNs. In this attack, an adversary *(WSN Adversary can be person or another entity that only monitors the communication channels which threatens the confidentiality of data)* captures a few of nodes, replicates them and then deploys arbitrary number of replicas throughout the network. In clone attack, an adversary may capture a sensor node and copy the cryptographic information to another node known as cloned node. Then this cloned sensor node can be installed to capture the information of the network. The adversary can also inject false information, or manipulate the information passing through cloned nodes [1][2][3].

Mauro Conti et.al in [7] characterized the clone attack:

1. A clone is considered totally honest by its neighbours. In fact, without global countermeasures, honest nodes cannot be aware of the fact that they have a clone among their neighbours.
2. To have a large amount of compromised nodes, the adversary does not need to compromise a high number of nodes. Indeed, once a single node has been captured and compromised, the main cost of the attack has been sustained. Making further clones of the same node can be considered cheap.

4.2 Man in the Middle Attack

The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection. The attacker will be able to intercept all messages exchanging between the two victims and inject new ones [2].

4.3 Sinkhole

In a sinkhole attack, an attacker makes a compromised node look more attractive to surrounding nodes by forging routing information [10]. The end result is that surrounding nodes will choose the compromised node as the next node to route their data through. This type of attack makes selective forwarding very simple, as all traffic from a large area in the network will flow through the adversary's node.

4.4 Jamming

Jamming is the type of attack which interferes with the radio frequencies used by network nodes. It is a attack on physical layer of wireless network. It interferes with the radio frequencies being used by the nodes of a network. in this , An attacker sequentially transmits over the wireless network refusing the underlying MAC protocol. Jamming can interrupt the network impressive if a single frequency is used throughout the network. In addition jamming can cause excessive energy consumption at a node by injecting impertinent packets. The receiver's nodes will as well consume energy by getting those packets [6].

4.5 Tampering

Another physical layer attack is tampering [3]. Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node which the attacker controls. One defense to this attack involves tamper-proofing the node's physical package [5]. However, it is usually assumed that the sensor nodes are not tamper-proofed in WSNs due to the additional cost. This indicates that a security scheme must consider the situation in which sensor nodes are compromised.

4.6 Flooding

This attack generates large volume of traffic that prevents legitimate user from accessing services. The main aim of this attack is either to block the node only or blocking link along with the node. As a result network performance decreases greatly. Flooding attacks takes place when adversary starts triggering multiple connection requests towards the target node i.e. greater than the node can handle, as a result of which buffer of target node gets overflowed. Thus, incapacitating the node from providing, any further service to the clients.
The adversary can be a legitimate node which has now been compromised in another case an adversary can have higher capabilities, generating large number of legitimate packets and overwhelming the victim node.

Prateek et.al reported [9],The primary aim of flooding attacks is to cause exhaustion of resources on victim system. This process is analogous to TCP SYN attacks where, attacker sends many connection establishment requests, forcing the victim to store state of each connection request.

4.7 wormhole attack

One of the most severe attacks to detect and defend in wireless sensor network is wormhole attack . In this attack, a malicious attacker receives packets from one location of network, forwards them through the tunnel (wormhole link) and releases them into another location [5][6]. The illustration of wormhole attack in wireless sensor networks is shown in Figure 2. The wormhole link can be established by a variety of means, e.g., by using a Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end [7].

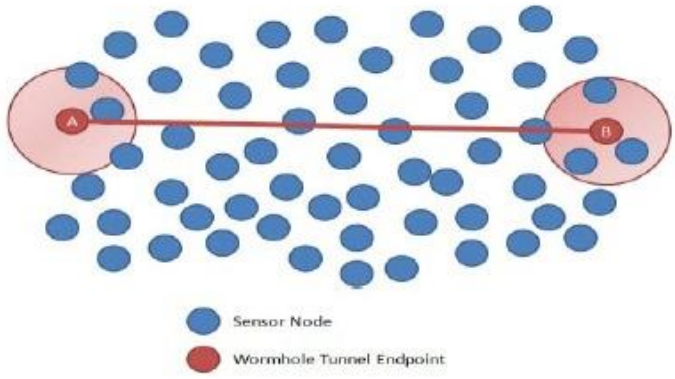

Figure 3. Illustration of wormhole attack [7]

5 CONCLUSION

As WSNs are used more frequently, the need for security in them becomes more apparent. However, the nature of nodes in WSNs gives rise to constraints such as limited energy, processing capability. These constraints make WSNs very different from traditional ad hoc wireless networks. In this article, we have surveyed the some popular security issues in WSNs.

6 FUTURE WORK

In future work we will explore the existing Clone Attack Protection Techniques & will proposed the novel Security model for protection against clone attacks.

REFERENCES

[1] Yingpei Zeng, Jiannong Cao, Senior Member, IEEE, Shigeng Zhang, Shanqing Guo and Li Xie , "Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks", IEEE Journal on selected areas in communications, vol. 28, no. 5, JUNE 2010.

[2] B. Parno, A. Perrig, and V. Gligor, Distributed detection of node replication attacks in sensor networks," in proc. IEEE Symp. Security and Privacy (S&P '05), 2005, pp. 49–63.

[3] H.Choi, S.Zhu, and T.Laporta.,Set: Detecting Node Clones in Sensor Networks. InSecureComm'07, 2007.

[4] Akyildiz, I.F., Su, W., ankarasubramaniam, Y., Cayirci, E.: Wireless

- *Rishav Dubey is currently pursuing masters degree program in CTA at SRIT, Jabalpur, MP, INDIA. E-mail: er.rishavdubey@yahoo.com.*
- *Vikram Jain, Rohit SinghThakur, Siddharth Dutt Choubey are currently with IT Department at SRIT, Vikram Jain is pursuing his Ph.D from Singhania University, Rajasthan, India. E-mail: vikram.srit@gmail.com,rohit.singhthakur2@gmail.com, siddharth.choubey@gmail.com.*

Sensor Networks: A Survey. Computer Networks Journal (Elsevier), Vol. 38, No.4 (2002)pp. 393-422.

[5] Ali Modirkhazeni , Saeedeh Aghamahmoodi, Arsalan Modirkhazeni, Naghmeh Niknejad , "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks" IEEE.

[6] Prasannajit B, Venkatesh, et al , "An Approach towards Detection of Wormhole Attack in Sensor Networks". 2010. WASE International Conference on Information Engineering. pp. 283 – 389

[7] Mauro Conti,Roberto Di Pietro,Luigi Vincenzo Mancini, and Alessandro Mei,"Distributed Detection of Clone Attacks in Wireless Sensor Networks" IEEE Transaction on dependable & secure computing vol.8 n0.5 September 2011.

[8] I. F. Akyildiz et al., "A Survey on Sensor Setworks," IEEE Commun.Mag., vol. 40, no. 8, Aug. 2002, pp. 102–114.

[9] Prateek Suraksha Bhushan ,Abhishek Pandey & R.C.Tripathi "A scheme for Prevention of Flooding Attack in Wireless sensor Network", Vol 1 No. 2 June 2011.

[10] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications, May 2003, pp. 113–27.