International Journal of communication and computer Technologies, ISSN: 2278-9723

Available at http://www.ijccts.org

A SURVEY ON ATTACKS, SECURITY AND CHALLENGES IN WIRELESS SENSOR NETWORKS

[1]K. Suganya, [2]A. Mummoorthy

[1]PG scholar,[2]Assistant Professor, Department of Information Technology, K.S.R.College of Engineering

Received: 08-06-2015, **Revised:** 25-09-2015, **Accepted:** 14-10-2015, **Published online:** 03-12-2015

ABSTRACT

A Wireless Sensor Network is a group of spatially distributed autonomous sensor devices. Because of design and cost restraints, the sensor nodes are not prepared with tamper-resistant hardware. Due to the unattended nature, they are more exposed to physical captures by opponents. Main motive behinds this paper is to introduce different types of attacks bump into during broadcast and communiqué over the wireless sensor network and provides some ideas to overcome from these attacks. Security has also been a major concern in these networks due to restrictions of resources in the sensor nodes and less human intrusion during its operation. The power computation and unsecure communication is main challenging area of wireless sensor network.

Keywords – **Wireless sensor network, characteristics, Attacks, Security, Challenges.**

1. INTRODUCTION

Sensor networks are basically wireless networks consisting of small, low-cost sensors that can be deployed with much ease. Quick scaling and simple neighbor discovery mechanisms make them require neither administrative intervention nor interaction with a Base Station (BS). Sensors are resource-constrained in terms of energy, memory, computational speed and communication bandwidth. Even though each sensor is provided with only a limited processing power, still when information sensed by each node is aggregated, one can measure a given physical environment in greater detail. Sensor nodes thus form a co-operative network. Newly, mobile sensor networks are emerging which found a wide range of applications in health monitoring, tracking of birds' migration, surveillance and environment mapping which are done by attaching sensors to Unmanned Aerial Vehicles. They are capable of reallocating sensing and networking resources to provide required sensing accuracy. They use limited resources to explore an environment and improve the quality of sensed data using information-driven sensor placement.

In the first section discuss about the basic components of sensor networks. There are four basic components in the wireless sensor networks. They are sensing unit, memory, transreceiver and power unit. The components of a wireless sensor network assist wireless connectivity within the network, connecting an application platform at one end of the network with one or more sensor or actuator devices in any part of the network.

In the second section discuss about the features of wireless sensor networks. The main characteristics include, power consumption restraints for nodes using batteries, ability to cope with node failures, nodes of mobility, heterogeneity of nodes, ability to large scale of deployment, ability to endure harsh environmental conditions, ease of use, cross-layer design.

In the third section discuss about the security in wireless sensor network. As the sensor networks can also operate in an adhoc custom the security goals cover both those of the traditional networks and goals suited to the exclusive constraints of adhoc sensor networks. A security goal consists of two different types. They are primary goal and secondary goal. The primary goal consists of data confidentiality, data integrity, data authentication, data availability. A secondary goal consists of data freshness, self-organization, time synchronization, secure localization.

In the fourth section discuss about the attacks. Here, we use some known attacks that pose a significant threat to cluster communications over wireless networks, and categorize these attacks based on their impacts, including data integrity and confidentiality, power consumption, routing, distinctiveness, privacy, and service availability. The attack consists of two types. They are active attack and passive attack.

In the fifth section discuss about the challenges in wireless sensor networks. WSN deal with real world

environments. In many circumstances, sensor data must be delivered within time constraints so that appropriate observations can be made or actions taken. Very scarce results exist to date regarding meeting real-time requirements in WSN. Most protocols one or the other ignore real-time or simply attempt to process as fast as possible and hope that this speed is sufficient to meet deadlines. Some initial results are existent for real-time routing. For example, the RAP protocol proposes a new policy called velocity monotonic scheduling.

2. BASIC COMPONENTS

2.1. SENSING UNIT:

Sensing unit consists of two fill in unit:

- Sensor and
- Analog-to-digital convertor (ADC).

Sensor takes some values from real world. An analog signals fashioned by sensor is converted into digital signal by ADC. And these digital signals fed into the processing unit, which enclose a small storage unit. After processing these data, transfer to transceiver which connects the node to network.

2.2. MEMORY

Small size of a sensor node results in equivalent constraints on memory also. Then sensor nodes have very simple memory architecture. Sensor nodes use flash memories because of their cost and storage capacity. The sensor nodes have two categories of memory constructed on the purpose of storage as user memory used intended for storing application related data and program memory used for programming the devices.

2.3. TRANSRECEIVER

The combination of both transmitter and receiver is called the transreceiver, which are combined and share common circuitry. The similar device includes transponders, transverses and the repeaters. Sensor nodes often use ISM (Industrial, Scientific and Medical) band. This give free radio, spectrum allocation and global availability.RF (radio frequency) transreceiver uses RF modules for high speed data transmission.

2.4. POWER UNIT

The most significant unit of sensor node is power unit who gives power to all the components includes sensing unit, memory, and transceiver. A power unit converts mains AC to low-voltage regulated DC power for the internal components of a computer. Modern personal computers universally 45 KB (5,975 words).The former technique employs a variety of petite batteries made up of thin films of vanadium oxide and molybdenum oxide. The latter technique employs energy foraging from the environment in order that the sensor node can operate uninterrupted.

3. CHARACTERISTICS OF WSN:

The cross-layered is becoming one of the important areas for wireless communication system. It is used to make the optimal modulation to improve the transmission performance. For example data rate, energy efficiency. In addition three problems in traditional layered approach. They are,

- It cannot share different information among different layers, which leads to each layer not having complete information.
- It does not have ability to adapt to the environmental change.
- The interference between the different users, access conflicts, fading, and the amendment of environment in WSN, traditional layered approach for wired networks is not applicable to wireless network

4. SECURITY IN WSN:

In wireless sensor network there are two different types of security goals. They are primary goals and secondary goals.

4.1. PRIMARY GOALS

4.1.1. DATA CONFIDENTIALITY:

Confidentiality means to expose the data to the authorized persons only not to everyone in the networks. It refers to the legislative measures or other recognized provision which prevent unauthorized disclosure of data that identify a moral or physical person either directly or indirectly.

4.1.2. DATA INTEGRITY

Data integrity ensures the data during transition is not altered, tempered by an unauthorized one may be an attacker. It is imposed within a database as its design stage through the use of standard rules and procedures, and is maintained through the use of error checking and validation routines.

4.1.3. DATA AUTHENTICATION

Authentication certifies the trustworthiness of the message by identifying its origin. In the two-party communication case, data authentication can be achieved through a virtuously symmetric mechanism. The sender and the receiver share a secret key to figure a message authentication code of all communication data.

4.1.4. DATA AVAILABILITY

It is the capability of a node to ensure the availability of the resources for use. Availability means having our data accessible and obtainable at all times. Available bandwidth between devices and network connection of mediums prioritization and types of data made be available.

4.2. SECONDARY GOALS

4.2.1. DATA FRESHNESS

All sensor networks torrent some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication. We must ensure each message is fresh. It implies that the sensed data are recent and it ensures that no adversary replayed old messages.

4.2.2. SELF-ORGANIZATION

Ability of a system to spontaneously arrange its computer its components or elements in a purposeful manner, under appropriate condition but without the help of an external agency. The principle of self-organization is,

- The argument is simple adequate in principle we start with the fact that system in general go to equilibrium.
- Going for any state to one of the equilibria, the system is going from a larger number of states to a smaller.

4.2.3. TIME-SYNCHRONIZATION

Time synchronization is extremely important for basic communication, but it also ability to detect movement, location and proximity. The synchronization problem of four parts. They are send time, access time, prorogation time and receive time.

4.2.4. SECURE-LOCALIZATION

Secure localization of anonymous nodes in a wireless sensor network is an important research subjects. The localization of sensors is a basic and crucial knowledge for most WSN algorithms and protocols includes data tagging, routing, node identification.

5. ATTACKS IN WIRELESS SENSOR NETWORKS

Wireless Sensor networks stand susceptible to security attacks due to the broadcast nature of the transmission medium. Additionally, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically threatened. Basically attacks are classified as active attacks and passive attacks. Figure1 shows the classification of attacks beneath general categories.

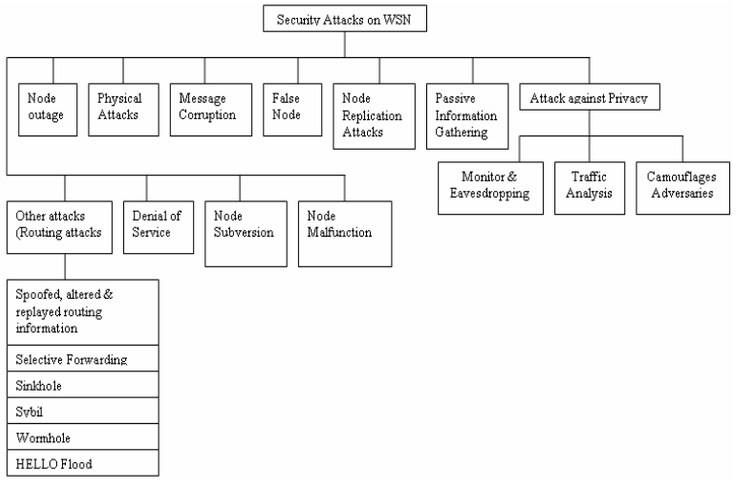

Figure 1. Classification of Security Attacks on WSN

5.1. ACTIVE ATTACKS

In the active attacks, an attacker tries to remove the messages transmitted on the network. He can also inject his own traffic otherwise replay of old messages to disturb the operation of the network or to cause a denial of service. The following attacks are the active attacks.

1. Routing Attacks in Sensor Networks
2. Denial of Service Attacks
3. Node Malfunction
4. Node Outage
5. Physical Attacks
6. Message Corruption

5.1.1 ROUTING ATTACKS IN SENSOR NETWORKS

These attacks attempt to change routing information, and to deploy and benefit from such a change in various ways.

1. **Spoofed, altered and replayed routing Information.**

- An undefended ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly disturb routing information.
- Create routing loops.
- Extend or shorten service routes.
- Generate false error messages.
- Increase end-to-end latency.

2. **Selective forwarding**

In this attack, nodes drop few messages instead of accelerating everything of what they have received. Attacking nodes repudiate routing some messages and globule them. If all the packets are denied for accelerating by a node after receiving, is called black hole attack.

3. **Sinkhole attack**

The sinkhole attack is a particularly severe attack that prevents the base station from obtaining correct sensing data, thus forming a serious threat to higher-layer applications. Sinkhole attacks classically work by making a compromised node look especially attractive to surrounding nodes.

4. **Sybil attack**

A single node spares itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as spread storage, multipath routing and topology maintenance. The attacker can impersonate other nodes identities or simply create multiple uninformed identities in the MAC or network layer. Then the attack poses threats to other protocol layers for example, packets traversed on a route consisting of fake identities are selectively dropped or modified.

5. **Wormhole attack**

Attackers here are purposefully placed at different ends of a network. They can receive messages and replays them in different parts by means of a tunnel.

6. **Hello flood attacks**

Several routing protocols use hello packet to discover neighboring nodes and thus to establish a topology of the network. The simplest attack for an attacker is made up of in sending a flood of such messages to flood the network and to prevent other messages from being substituted. Jamming: a well-known attack on wireless communication.

5.1.2. DENIAL OF SERVICE ATTACKS

Dos attack is an attack which reduces networks capability to perform task and produced by malicious action or unintentional failure of nodes. In this attack, attacker may overload that server in such a way that server can't process request. A Dos attack generally boards physical layer applications in an environment where sensor nodes are located.

5.1.3. NODE MALFUNCTION

A broken node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data accumulating node such as a cluster leader.

5.1.4. NODE OUTAGE

Node outage is the situation that happens when a node stops its function. In the case where a cluster leader stops functioning, the sensor network rules should be robust enough to mitigate the effects of node outages by providing an alternate route.

5.1.5. PHYSICAL ATTACKS

Sensor networks typically operate in outside environments. Due to its unattended and distributed nature it is highly inclined to physical attacks. Physical attacks permanently destroy sensor nodes which may be irreversible. An attacker can extract sensitive information or change its program codes, tamper with its circuitry or may replace with a malicious node.

5.1.6. MESSAGE CORRUPTION

Any modification of the at ease of a message by an attacker compromises its integrity.

5.2. PASSIVE ATTACKS

The passive attack is imperfect to listening substituted traffic. This type of attacks is easier to and it is difficult to detect. Meanwhile, the attacker does not make any modification on exchanged information. The target of the attacker can be the knowledge of confidential information or the knowledge of the significant nodes in the network by evaluating routing information, to prepare an active attack. Some of the common passive attacks are,

5.2.1 MONITOR AND EAVESDROPPING

This attack is most common and informal attack on privacy. In this attack an adversary snoop the data, by snooping those data an hen the traffic bears the control information about the sensor network configuration, which contains potentially more detailed information than available through the location server, the eavesdropping can act effectively against the privacy protection. Adversary easily understands message contents.

5.2.2. TRAFFIC ANALYSIS

When the messages shifted are encrypted, it still leaves a high network. This attack may create Denial of Service attack and also attack on individual node which plays an important role possibility analysis of the communication patterns.

5.2.3. CAMOUFLAGE ADVERSARIES

It is similarly a passive attack on wireless sensor network on privacy. One can insert their node or compromise the nodes to hide in the sensor network.

5.3. JAMMING ATTACKS

Jamming is one of many activities used to concession the wireless environment. One of the fundamental ways for degrading the network presentation is by jamming wireless transmissions. In the simplest form of jamming, the attacker corrupts the transmitted messages by causing electromagnetic intervention in the network's operational frequencies, and in proximity to the targeted receivers. Handling the jamming at MAC layer needs to control the requests which may exhaust the resources by ignoring them.

6. CHALLENGES IN WIRELESS SENSOR NETWORKS

6.1. CHALLENGES IN REAL TIME:

WSN deal with real world environments. In several cases, sensor data must be delivered within time constraints so that proper observations can be made or actions taken Some initial results exist for real-time routing. For example, the RAP protocol intends a new policy called velocity monotonic scheduling. Here a packet has a deadline and a distance to travel. Using these considerations a packet's average velocity requirement is computed and at each hop packets are programmed for transmission based on the highest velocity requirement of any packets at this node.

6.2. CHALLENGES IN POWER MANAGEMENTS:

Low-cost positioning is one acclaimed advantage of sensor networks. Limited processor bandwidth and small memory are two arguable constrictions in sensor networks, which will disappear with the development of fabrication techniques. On the other hand, the energy constraint is unlikely to be solved soon due to slow progress in developing battery capacity. The scope of middleware for WSN is not regulated to the sensor network alone, but also covers devices and networks connected to the WSN. Conventional mechanisms and infrastructures are typically not well suited for interaction with WSN.

6.3. HOSTILE ENVIRONMENT

The hostile environment is the challenging factor of WSN in which sensor nodes function. Motes face the possibility of destruction or capture by the attacker. Since in hostile environment, an attacker may easily capture a node and extract the important information or change the information of a node. An attacker may also physical access of the node and replace the sensor node by malicious node. The highly hostile environment is the challenging factor of the wireless sensor network.

6.4. WIRELESS MEDIUM

Wireless medium is not much more secure because of its broadcasting nature. An attacker can easily intercept, change and alter any transmission. In Wireless medium an attacker easily track the node and replace that node by malicious one. This is the really challenging field of sensor network.

7. CONCLUSION

In this paper we surveyed on attacks of wireless sensor network. We also covered the security goals and challenges in wireless sensor networks. In security attacks we describe all the attacks. Most of the attacks against security in WSN are caused by the false information by the compromised node within the network. In challenges for wireless sensor networks, we labeled some challenges. This paper helps to better view of security, attacks, and challenges.

REFERENCES

[1] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. SPINS: Security protocols for sensor networks. *J.Wireless Nets. 8*, 5 (Sept. 2002), 521–534.

[2] Wood, A. and Stankovic, J. Denial of service in sensor networks. *IEEE Comput.* (Oct. 2002), 54–62.

[3] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006.

[4]Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006

[5] Yong Wang, Garhan Attebury, and Byrav Ramamurthy "A survey of security issues in wireless sensor networks" 2nd quarter 2006, volume 8, NO. 2 IEEE communication surveys

[6] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009.

[7] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2,page(s): 52-62, year 2009.

[8] Sachin Dev Kanawat and Pankaj Singh Parihar "Attacks in Wireless Networks" IJSSAN 2011.

[9] Fadi Farhat *University of Windsor* "Eavesdropping attack over Wi-Fi".

[10] James Newsome, Elaine Shi, Dawn Song and Adrian Perrig of Carnegie Mellon University "The Sybil Attack in Sensor Networks: Analysis & Defenses".