ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Security Issues and Challenges in Wireless Sensor Networks (An Overview)

Suhail Ahmad Shah

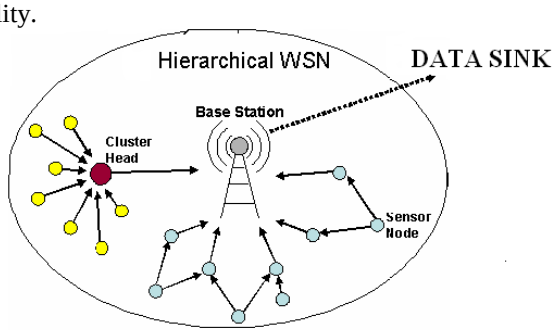
Lecturer, Computer Applications, Govt. Degree College Anantnag. J&K India.

Abstract: Wireless Sensor Network (WSN) is a group of smart sensors, each capable of sensing, processing and communicating, but when deployed in numbers, form a network which collectively monitor the state of the physical world. Its applications and potential benefits are tremendous and seem only limited by imagination. As any technology at its infancy stage, there are plenty of challenges and obstacles lying ahead .The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed mechanisms for wireless sensor networks.

Keywords: WSN, Applications, Security, Attack, Holistic, Challenges.

I. INTRODUCTION

Wireless sensor network is a network system comprised of spatially distributed autonomous sensor nodes, each has the ability to sense or to interact with the surrounding physical world, to process gathered data, and to communicate with each other and outside entities without wires. Thanks to the advance in semiconductor technology, network communications, embedded system and many others, sensor nodes with these abilities can now be integrated into an entity smaller than a penny coin, allowing what **Kris Pister** called "smart dust" to become a reality.



Wireless sensor networks is a new breed of sensory system, although often with limited processing power and communication bandwidth, is nonetheless intelligent when compared to their more traditional relatives, hence often also referred to as smart sensors. Some networks are designed to utilize in-network processing, so decisions can be made on the spot or at least transformed to more abstract and aggregated high-level data before transmitted. An interesting observations have been offered, by **Satyanarayanan** , he mentioned that wireless sensor network can be regarded as the nervous system of the physical world.

These tiny self organizing wireless sensors and actuators can bridge the gap between the digital and physical worlds, it offers the capability to observe the physical world continuously, and proactively transmit data of interest. In some implementations, sensory system can also analyze the data and react to it by sending commands to actuators, and this behavior is indeed a pretty good analogy to biological nervous system.

PARTS OF A SENSOR NODE

- A Radio Transceiver with an internal antenna or connection to an external device.
- A microcontroller (sometimes abbreviated uC or MCU) is a small computer on a single integrated circuit containing a processor core, memory and programmable input/output.
- An electronic circuit for interfacing with the sensors and an energy source, usually a batttery or an embedded form of Energy Harvesting.

II. APPLICATIONS OF SENSOR NETWORKS

Since the availability of realistic miniature sensor units has only come into reality in the last decade, this new interdisciplinary research area has inspired many interesting novel proposals for a wide variety of applications. Culler et al classifies all these applications into three separate categories [3]. The first category monitors space, with applications such as environmental monitoring, agricultural, climate control, surveillance and intelligent alarms. The second category monitors things, such as structural monitoring, condition-based equipment maintenance, asset tracking, and medical diagnostics. The third category monitors the interactions among things and the encompassing space, including wildlife habitat, disaster management, ubiquitous computing environments, healthcare and manufacturing process flow.

The following is a sample of some Applications recently being proposed:

a). Environmental Monitoring.

Martinez et al create GlacsWeb project to monitor glacial environment using embedded probe placed inside the glacier, with on-surface base station, gateway server and a web front end. They are able to automatically get daily readings of various sensors for an extended period of time, but have also discovered that designing a sensor network sustainable in harsh environment presents a tough challenge. Holman et al, on the other hand, created Argus Station using video camera as sensors, which allow

DOI 10.17148/IJARCCE.2015.4740

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

automated multi-sensor sampling based on remote user's high level tasking. The system use image processing technique to collect only appropriate data. In this project, the sensors are much more complex and powerful than most of other wireless sensor networks and the camera transmit collected video stream with wire. Although neither of these two applications use in network processing, they still show the feasibility and how very different approaches can be used for continuous remote monitoring of the environment over a large area and long period of time.

b). Military Applications.

Brennan et al, designed a sensor array for radiation detection, by using a multitude of much smaller portable sensors to form an array, and conclude that gamma counts received indicate the sensor network approach provides higher sensitivity than traditional portal sensor. It is also portable and much cheaper. Matori et al investigated an urban shooter localization system, in which by using acoustic model from multiple sensors around where shooting take place to pinpoint the location of shooter. This project provides an interesting simulation and prototype generating a pretty impressive accuracy of 1 meter using 60 sensors.

c). Smart Environment.

The Gator Tech Smart House applies sensor networks in the context of assistive living .With a wide array of sensors and actuators in a controlled environment, this house is aimed at integrating data collected from various sensors, and provides a programmable environment by offering more abstract concepts such as context and service composition as part of the middleware. In this project, the focus of interest is less on how long the sensor will last (they are plugged into the outlets) or if sensor networks can form a self-organizing network (the environment is controlled and preset), but rather on smart handling of the collected data, and intelligence on reacting to various context and sensor inputs.

d).Industrial Control and Monitoring.

Many mechanical failures are preceded by noticeable symptoms, such as squeaky bearing or shudder often indicate wearing of the bearing or imbalance of the shaft. The industrial monitoring often requires low maintenance, high reliability, inexpensive, and non-intrusive. It would be even better if it can self-maintained and self-healing. Wireless sensor networks provide a solution that is much closer to this goal than anything previously available.

III. SECURITY GOALS IN WSN.

Confidentiality- Nodes should not reveal data to any unintended recipients.

Integrity- Data should not be changed between transmissions due to environment or malicious activity.

Data Freshness- Old data should not be used as new.

Authentication- Data used in decision making process should originate from correct source.

Robustness- When some nodes are compromised the entire network should not be compromised.

Self-organization- Nodes should be flexible enough to be self-organizing (autonomous) and self-healing (failure tolerant)

Availability- Network should not fail frequently.

Time Synchronization- These protocols should not be manipulated to produce incorrect data.

Secure Localization- Nodes should be able to accurately and securely acquire location information.

Accessibility- Intermediate nodes should be able to perform data aggregation by combining data from different nodes.

Flexibility- Nodes should be replaceable when compromised.

Scalability- WSN should concurrently support at least 3000 nodes even with key management in place.

IV. SECURITY THREATS AND ISSUES IN WSN

Wireless sensor Networks are vulnerable to security attacks due to broadcast nature of transmission medium. Basically attacks are broadly classified into two categories i.e active attacks and passive attacks. This paper points out both in details.

4.1 Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. Some of the more common attacks against sensor privacy are:

4.1.1 Monitor and Eavesdropping:
This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents.

4.1.2 Traffic Analysis:
Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

4.1.3 Camouflage Adversaries:
One can insert their node or compromise the nodes to hide in a sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

4.2 Active Attacks:

The unauthorized attacker monitors, listens to and modifies the data stream in the communication channel. This is called active attack. The following attacks are active in nature:

4.2.1 Routing Attacks in Sensor Networks:

The attacks which act on the network layer are called routing attacks. The following are the attacks:

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

4.2.2.1 Attacks on Information in Transit
In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report the information in transit may be altered, spoofed or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base station or sinks.

4.2.1.2 Selective Forwarding:
A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks it is assumed that nodes faithfully forward received message. But some compromised node might refuse to forward packets, however neighbors might start using another route.

4.2.1.3 Black hole/Sinkhole Attack:
Also known as sink holes attack occurring at the network layer. It builds a covenant node that seems to be very attractive in the sense that it promises zero-cost routes to neighboring nodes with respect to the routing algorithm.
This results maximum traffic to flow towards these fake nodes. Nodes adjoining to these harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction.

4.2.1.4 Wormholes Attacks:
In the wormhole attack, pair of awful nodes firstly discovers a wormhole at the network layer. Then the whole traffic of the network is tunneled in a particular direction at a distant place, which causes deprivation of data receiving in other parts of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This may cause congestion and retransmission of packets squandering the energy on innocent nodes.

4.2.1.5 HELLO flood attacks:
Hello flood attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack the attacker with a high radio transmission (termed as laptop-class attacker) range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

4.2.1.6 Sybil Attacks:
In many cases, the sensors in a WSN might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate node. This type of attack where a node forges the identities of more than one node is Sybil attack. Sybil tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, fair resource allocation and misbehavior detection.
Basically any peer-to-peer network (especially WSN) is vulnerable to Sybil attack.

4.2.2 Denial of Services:
Denial of service (DoS) is produced by the unintentional failure of nodes or malicious action. In wireless sensor networks several types of DoS attacks at different layers might be performed.

4.2.3 Node Subversion:
Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary.

4.2.4 Node Malfunction:
A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is data-aggregation node such as cluster leader.

4.2.5 Node Outage:
Node outrage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outrage by providing an alternate route.

4.2.6 Physical Attacks:
Unlike any other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

4.2.7 Message Corruption:
Any modification of the content of a message by an attacker compromises its integrity.

4.2.8 False Node:
A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur.

4.2.9 Node Replication Attacks:
Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted.

4.2.10 Passive Information Gathering:
An adversary with powerful resource can collect information from the sensor network if it is not encrypted.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

To minimize the threats of passive information gathering, strong encryption techniques need to be used.

V. SECURITY CHALLENGES IN WSN

The nature of large, ad-hoc, wireless sensor networks present significant challenges in designing security schemes. A wireless sensor network is a special network which has many constraints compared to traditional computer networks.

5.1 Wireless Medium:

The wireless medium in inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker easily intercept valid packets and easily injects malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks.

5.2 Ad-Hoc Deployment:

The ad-hoc nature of sensor networks means that no structure can be statically defined. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced, the network must support self-configuration. Security schemes must be able to operate within the dynamic environment

5.3 Hostile Environment:

The next challenge factor is the hostile environment in which sensor nodes function. Nodes face the possibility of destruction or capture by attackers. The highly hostile environment represents a serious challenge for security researchers.

5.4 Immense Scale:

The proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes have proven to be substantial task.

VI. SECURITY MECHANISMS IN WSN. (FUTURE RESEARCH SCOPE)

The security mechanisms are actually used to detect, prevent and recover from the security attacks. A wide variety of Security schemes can be framed (Scope of improvement is open) to counter malicious attacks

6.1 Key Establishment and Trust Setup:

The primary requirement offsetting up the sensor network is the establishment of cryptographic keys, generally the sensor devices have limited computational power and the public key cryptographic primitives are too expensive to follow. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes.

6.2 Secrecy and Authentication:

Most of the sensor network applications require protection against eavesdropping, injection, and modification of packets. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network cryptographic approaches.

6.3 Privacy:

Like other traditional networks, the sensor networks have also forced privacy concerns. Initially the sensor networks are deployed for legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is particularly important.

6.4 Secure routing:

Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately current routing protocols suffer from many vulnerability.

HOLISTIC SECURITY IN WSNS

A holistic approach aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such networks, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach has some basic principle like, in a given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient mechanisms working in other layers. By building security layers in a holistic approach, protection could be established for the overall network.

VII.CONCLUSION

Security in sensor networks is new area of research, with a limited but rapidly growing set of research results. In this paper, various applications of WSN along with the knowledge of security issues, security goals, attacks on WSN and proposed security mechanism are discussed. This paper can be helpful for research scholars who are working in this field. Security is an important requirement and complicates enough to setup in different domains of WSN. Adding security in a resource constrained WSNs with minimum overhead provides significant challenges, and is an ongoing area of research. There is currently enormous research potential in the field of WSN.

REFERENCES

[1] Culler, D.E and Hong, W., "Wireless Sensor Networks", Communications of ACM, Vol 47, No 6, June 2004, pp. 30-33.
[2] X.Du, and HH.Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, vil.15, no.4, Aug, 2008, pp 60-66.
[3] Xangojan Chen, Kai Mikki, Kang Yen and Nikka Pissino, "Sensor Network Security: A Survey", IEEE Communications, Vol 11, No 2, Second Quarter 2009, pp 52-73.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

[4] Divya et al , " Analysis of Security Attacks In Wireless Sensor Networks" International Journal of Software and Web Sciences, 8(1), March-May 2014, pp. 26-30.
[5] Hubbub, R. and M. Ouzzif, 2011. Secure Routing in WSN International Journal, pp: 2.
[6] TING, Chuan-Kang et LIAO, Chien-Chih. A memetic Algorithm for extending wireless sensor network lifetime.Informati on Sciences, 2010, vol. 180, no 24, p.4818-4833.
[7] H. Chan and A. Perrig: Peer intermediaries for key establishment in Sensor Networks. IEEE Infocom 2005
[8] J. Deng, R.Han and S. Mishra, "Security, Privacy and Fault Tolerance in WSNs, Artech House, August 2005.
[9] M. Satyanaranayan "Of Smart Dust and Brilliant Rocks", IEEE Pervasive Computing Vol.2, No.4, October-December 2003, pp 2-3.
[10] F. Lewis, "Wireless Sensor Networks", Smart Environment: Technology, Protocols and Applications, Chapter 2, Wiley-Interscience 2005.
[11] Hen-l Yang "Wireless Sensor Network: The challenges Of Design and programmability. " hyang@cise.ufl.edu April 26, 2005

BIOGRAPHY

Suhail Ahmad Shah is MCA (Gold Medalist) with UGC -NET in Computer science and Applications. Has more than one year experience of teaching at college level. Has also one year experience of teaching at PG level in University. His area of interest is Networking, Security and Cryptography.