An Overview of Wireless Sensor Networks Applications and Security

S. Prasanna, Srinivasa Rao

Abstract*— Wireless communication technologies continue to undergo rapid advancement. In recent years, there has been a steep growth in research in the area of wireless sensor networks (WSNs). In WSNs, communication takes place with the help of spatially distributed, autonomous sensor nodes equipped to sense specific information. WSNs can be found in a variety of both military and civilian applications worldwide. Examples include detecting enemy intrusion on the battlefield, object tracking, habitat monitoring, patient monitoring and fire detection. Sensor networks are emerging as an attractive technology with great promise for the future. However, challenges remain to be addressed in issues relating to coverage and deployment, scalability, quality-of-service, size, computational power, energy efficiency and security. This paper presents an overview of the different applications of the wireless sensor networks and various security related issues in WSNs.

***Index Terms*—Network, Security, Sensor, Wireless.**

I. INTRODUCTION

A wireless sensor network (WSN) [1] [2] is a wireless network consisting of spatially distributed autonomous devices that use sensors to monitor physical or environmental conditions. These autonomous devices, or nodes, combine with routers and a gateway to create a typical WSN system. The distributed measurement nodes communicate wirelessly to a central gateway, which provides a connection to the wired world where you can collect, process, analyze, and present your measurement data. To extend distance and reliability in a wireless sensor network, you can use routers to gain an additional communication link between end nodes and the gateway. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet (Figure-1). This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

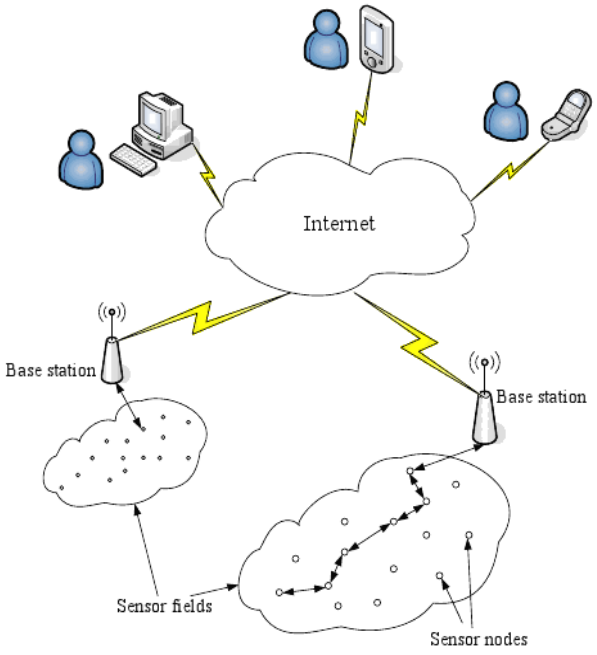

Figure-1 Accessing WSNs through Internet.

The major challenges to be addressed in WSNs are coverage and deployment, scalability, quality- of- service, size, computational power, energy efficiency and security[3]. Among these challenges, security is a major issue in wireless sensor networks. Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In this paper we present an overview of the applications and security issues relating to Wireless Sensor Networks(WSNs).

II. APPLICATIONS OF WIRELESS SENSOR NETWORKS

A. Military or Border Surveillance Applications

WSNs are becoming an integral part of military command, control, communication and intelligence systems. Sensors can be deployed in a battle field to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.

Manuscript received on April 26, 2012.

S. Prasanna Srinivasa Rao, Asst. Professor, Dept. Computer Science & Engineering, School of Computing and Information Technology, VELTECHDr.RR & Dr. SR Technical University., Chennai, Avadi.

B. Environmental Applications

Environmental applications include tracking the movements and patterns of insects, birds or small animals.

C. Health Care Applications

Wireless sensor networks can be used to monitor and track elders and patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care expenditures in the current health care systems. For example sensors can be deployed in a patient's home to monitor the behaviors of the patient. It can alert doctors when the patient falls and requires immediate medical attention.

D. Environmental Conditions Monitoring

WSN applications in this area include monitoring the environmental conditions affecting crops or livestock, monitoring temperature, humidity and lighting in office buildings, and so on. These monitoring modules could even be combined with actuator modules which can control, for example , the amount of fertilizer in the soil, or the amount of cooling or heating in a building, based on distributed sensor measurements.

E. Home Intelligence

Wireless sensor networks can be used to provide more convenient and intelligent living environments for human beings. For example, wireless sensors can be used to remotely read utility meters in a home like water, gas, electricity and then send the readings to a remote centre through wireless communication.

F. Industrial Process Control

In industry, WSNs can be used to monitor manufacturing process or the condition of manufacturing equipment. For example, chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. These sensors are used to alert in case of any failures occurred.

G. Agriculture

Using wireless sensor networks within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control center for billing. Irrigation automation enables more efficient water use and reduces waste.

H. Structural Monitoring

Wireless sensors can be used to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc... enabling Engineering practices to monitor assets remotely without the need for costly site visits, as well as having the advantage of daily data, whereas traditionally this data was collected weekly or monthly, using physical site visits, involving either road or rail closure in some cases. It is also far more accurate than any visual inspection that would be carried out.

III. ATTACKS ON WIRELESS SENSOR NETWORKS

The following are the types of attacks on wireless sensor networks:-

- Common Attacks
- Denial of service(DOS) Attack
- Node compromise
- Impersonation Attack
- Protocol- specific Attack

A. Common Attack

The first common attack is eavesdropping i.e.., an adversary can easily retrieve valuable data from the transmitted packets that are sent. The second common attack is Message modification i.e.., the adversary can intercept the packets and modify them. The third common attack is message replay ie.., the adversary can retransmit the contents of the packets at a later time.

B. DOS Attack

A DOS attack[4] on WSN may take several forms. The first one is node collaboration, in which a set of nodes act maliciously and prevent broadcast messages from reaching certain sections of the sensor networks. The second one is jamming attack, in which an attacker jams the communication channel and avoids any member of the network in the affected area to send or receive any packet. The third one is exhaustion of power, in which an attacker repeatedly requests packets from sensors to deplete their battery life.

C. Node compromise Attack

A sensor node is said to be compromised when an attacker gains control or access to the sensor node itself after it has been deployed. Various complex attacks can be easily launched from compromised nodes , since the subverted node is a full- fledged member of the sensor network.

D. Impersonation Attack

The most common attack that can be launched using a compromised node is the impersonation attack, in which a malicious node impersonates a legitimate node and uses its identity to mount an active attack such as Sybil[5] or node replication. In a Sybil attack, a single node takes on multiple identities to deceive other nodes. On the other hand, the node replication attack is the duplication of sensor nodes.

E. Protocol- specific Attack

The attacks against routing protocols in WSN are: Spoofed routing information- corruption of the internal control information such as the routing tables, Selective forwarding- selective forwarding of the packets that traverse a malicious node depending on some criteria, Wormhole attack- Creation of a wormhole[6] that captures the information at one location and replays them in another location either unchanged or tampered, Hello flood attack- creation of false control packets during the deployment

of the network.

IV. SECURITY MECHANISMS FOR COUNTERING ATTACKS ON WIRELESS SENSOR NETWORKS

The following are the security mechanisms to counter the attacks on WSNs:

1. To counter common attacks like eavesdropping, message modification, message replay attacks, strong encryption techniques and time stamps are to be used.
2. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.
3. To counter Sybil attack proper authentication is a key defense. A trusted key server or base station may be used to authenticate nodes to each other and bootstrap a shared session key for encrypted communications. This requires that every node share a secret key with the key server. If a single network key is used, compromise of a any node in the WSN would defeat all authentication.
4. To counter HELLO flood attack, verifying the bi-directionality of the local links before using them is effective if the attacker possesses the same reception capabilities as the sensor devices.
5. To counter selective forwarding attack, Using multiple disjoint routing paths and diversity coding are used.
6. For countering worm hole attack, geographic forwarding is a tamper- resistant routing protocol.Each message is forwarded individually, choosing the next- hop node to be the neighbor closest to the ultimate destination. Such a scheme would not favor wormhole attack in the network, though it may coincidentally use it.

V. CONCLUSION

Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Many applications of WSNs include military, helath, environmental, water, industries, home, agriculture and so on. Besides these applications, security is the main issue in WSNs. There are many attacks on WSNs including wormhole attack, sybil attack, selective forwarding, impersonation attack. In this paper we present an overview of the applications of WSNs and different attacks and their countermeasures.

REFERENCES

1. J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, System Architecture Directions for Networked Sensors, ASPLOS, November 2000.
2. Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
3. Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., “Security for Sensor Networks”, CADIP Research Symposium, 2002, available at, http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf
4. A.D. Wood and J.A. Stankovic, (2002) “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, 2002, pp. 54– 62.
5. J. R. Douceur,(2002) “The Sybil Attack,” in 1st International Workshop on Peer-to-Peer Systems (IPTPS "02).
6. Zaw Tun and Aung Htein Maw,(2008),” Worm hole Attack Detection in Wireless Sensor networks”, proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication