IJCSC International Journal of Computer Science and Communication Vol. 2, No. 2, July-December 2011, pp. 355-358

SECURITY ISSUES IN WIRELESS SENSOR NETWORK

Manju Gupta[1] and C. Ram Gupta[2]

[1]Research Scholar, Department of Electrical Singhania University, Rajasthan, India.
[2]Professor, Deptt. of ECE, Dronacharya College of Engg. & Tech, Gurgaon, India.
E-mail: nimtkkr@gmail.com

ABSTRACT

Wireless sensor and actor networks (WSANs) refer to a group of sensors and actors linked by wireless medium to perform distributed sensing and actuation tasks. Nowadays it is rapidly growing in popularity and becoming a part of our use. It is giving the vision of anywhere and anytime with pervasive access and computing a reality [3]. It has spanned over a broad range of civilian and military applications relating to monitoring and control, including health care, habitat monitoring, building surveillance, battlefield reconnaissance and perimeter defense [9].

But WSANs are exposed to numerous security threats that adversely act the success of import applications. It faces acute security concerns, including eavesdropping, forgery of sensor data, denial of service attacks, and the physical compromise of sensor nodes deployed into enemy territory [4]. Its unreliable communication channel and unattended operation make the security defenses harder. Hence security is a significant concern for many sensor network applications [7]. These problems inspire new research & represent, to properly address the sensor network security from the start.

Keyword: Ad-Hoc, BSS, Multi-Hop, Sink and WEP.

1. INTRODUCTION

In network, sensors gather information about the physical world, while actors take decisions and then perform appropriate actions upon the environment, which allows a user to effectively sense and act at a distance. The physical architecture of the WSAN is given in Figure 1.

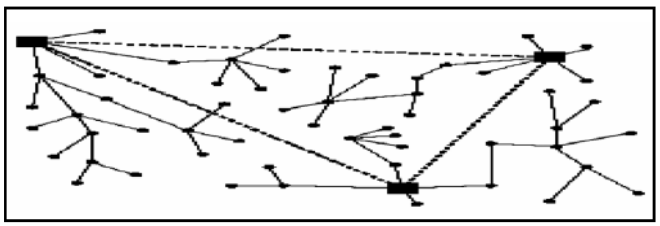

Figure1

It is a collection of sensor nodes that works collaboratively in multi-hop wireless communication architecture [8]. See Figure-2. It refers to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. These networks consist of hundreds or thousands of self-organizing, low-power, low-cost wireless nodes deployed in mass to monitor and affect the environment [5].

WANS networks are rapidly growing in popularity and becoming a part of our use. It is giving the vision of anywhere and anytime with pervasive access and computing a reality [3]. System major benefit is it performs in-network processing to reduce large streams of raw data into useful aggregated information. Its

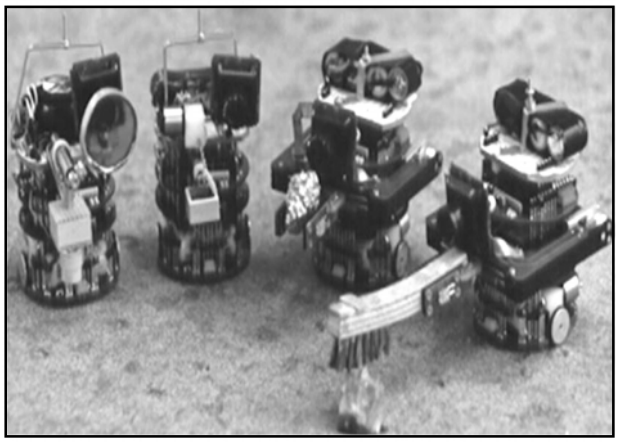

Figure 2

Figure 3

Figure 4

emerged applications include habitat monitoring, robotic toys, battlefield monitoring, location aware in home and offices, biomedical sensing, and of storms, oceans, and weather events monitoring [4]. See Figures 3 & 4.

WSANs unfortunately, are exposed to numerous security threats that adversely act to its success. Its channel and unattended operation make the security defenses harder. System faces acute security concerns, including eavesdropping, forgery of sensor data, denial of service attacks, and the physical compromise of sensor nodes deployed into enemy territory [4].

2. WSAN ARCHITECTURE AND WORKING

A sensor network is a collection of sheer number of sensor nodes that collaboratively work in multi-hop wireless communications architecture. It is advanced form of independent BSS [2]. Sensor networks are often organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource constrained sensor nodes.

Sensor networks have one or more points of centralized control called base stations also referred to as sinks. See Figure 5. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. Base stations are many orders of magnitude more powerful than sensor nodes. These have enough battery power to surpass the lifetime of all sensor nodes, sufficient memory to store cryptographic keys, stronger processors, and means for communicating with outside networks. In order to provide effective sensing and acting, a distributed local coordination mechanism is used among sensors and actors.

Sensors gather information about the physical world, while actors take decisions and then perform appropriate actions upon the environment, which allows a user to effectively sense and act at a distance. The sensor nodes using RF bandwidth, which is extremely dear, establish a routing forest, with a base station at the root of every

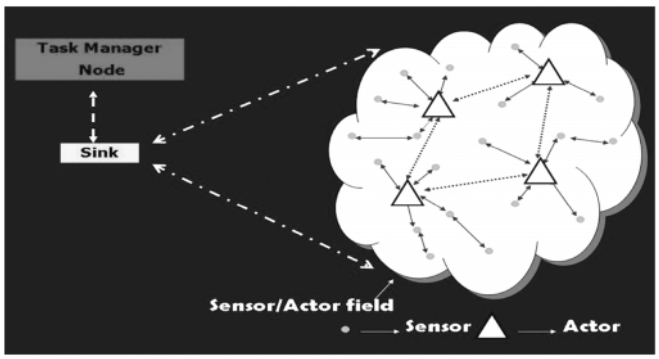

Figure 5 (WSAN Architecture)

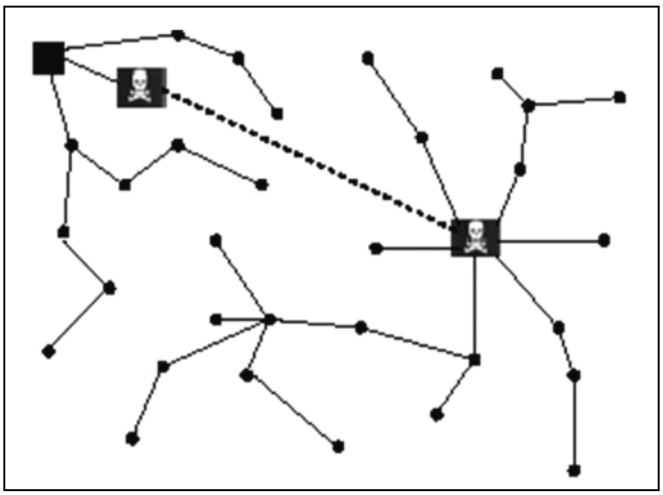

Figure 6

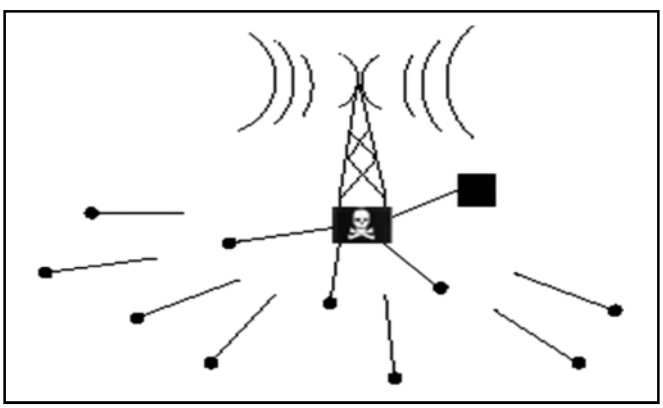

Figure 7

tree. Each bit transmitted consumes about as much power as executing 800–1000 instructions. The communication patterns within the network fall into the following categories:

- Node to base station communication, e.g. sensor readings, specific alerts.
- Base station to node communication, e.g. specific requests, key updations.
- Base station to all nodes, e.g. network entire routing, beacons, queries or reprogramming.

- Communication amongst a defined cluster of nodes (a node and all its neighbors).

3. WSAN SECURITY ISSUES

Security is key issues especially in tactical wireless sensor networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. The 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol, used to protect link-layer communications from eavesdropping and other attacks. But several serious security flaws have discovered in this protocol that lead to a number of practical attacks that demonstrate that WEP fails to achieve its security goals [6].

Wireless communications are difficult to protect; they are by nature a broadcast medium. In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject, and alter transmitted data. See Figures 6 & 7. In addition, adversaries are not restricted to using sensor network hardware. They can interact with the network from a distance by using expensive radio transceivers and powerful workstations. Sensor networks are vulnerable to resource consumption attacks. Adversaries can repeatedly send packets to drain the nodes' batteries and waste network bandwidth. Since sensor networks will be deployed in a variety of physically insecure environments, adversary can steal nodes, recover their cryptographic material, and pose as authorized nodes in the network. All these lead to a very demanding environment to provide security.

4. WSAN SECURITY CHALLENGES

Protecting wireless sensor networks in all is critical. Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack [1]. And third, sensor networks interact closely with their physical environments and with people, posing new security problems. Existing security mechanisms are inadequate, and new ideas are needed. A WSAN presents significant challenges in designing security schemes. Five of the most pronounced challenges are described below.

1. **Wireless Medium**: Wireless medium is inherently less secure, its broadcast nature makes eaves-dropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. It allows an attacker to easily intercept valid packets and easily inject malicious ones.
2. **Ad-Hoc Deployment**: Network topology keeps changing due to node failure, addition & mobility. So nothing is known of the topology prior to deployment. Security schemes require robust designs to cope and operate in dynamic and ever-changing environment.
3. **Hostile Environment**: The highly hostile environment represents a serious challenge. Attackers can capture a node, physically disassemble it, and extract from it valuable information.
4. **Resource Limitation**: Energy is the most precious resource for sensor networks. Communication is expensive in terms of power. Security mechanisms must be energy efficient.
5. **Big Scale Network**: The high scale of sensor networks poses a significant challenge for security mechanisms. Providing security for it is equally challenging. Security mechanisms must be scalable to very large networks maintaining high computation and communication efficiency.

5. SECURITY THREATS, TYPES OF ATTACKS AND COUNTERMEASURES

1. **Passive Information Gathering**: Intruder with a powerful receiver and well-designed antenna can easily pick off the data stream. It allows attacker to locate and destroy the nodes. *To minimize the threats of passive information gathering, strong encryption techniques can be used.*
2. **Subversion of a Node**: A particular sensor might be captured, and its stored information might be obtained. *Defines an efficient way to disable the node and flash its stored information.*
3. **False Node & Malicious Data** (*sleep deprivation torture*): Intruder can add a node to the system to feed false data or prevents the passage of true data. *Strong authentication techniques can prevent an adversary from impersonating as a valid node in the sensor network.*
4. **Sybil Attack**: In a Sybil attack, a node presents multiple identities for other nodes in the network. They pose a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. *Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.*
5. **Wormhole Attacks**: In wormhole attack, an adversary tunnels messages received in one part of the network replays them in a different part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole.

REFERENCES

[1] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks", Year 2004, Paper 1217, *Communications of The ACM,* June 2004, **47**, No. 6.

[2] Binod Kumar, Dr. Kanak Saxena, "Ad-hoc Network: Security Overview and Design", *Techno Saga*, National Seminar, SIRT, Bhopal, Aug. 2007.

[3] "Guest Editorial Security in Wireless Ad Hoc Networks", *IEEE Journal on Selected Areas in Communications*, **24**, No. 2, February 2006.

[4] Jing Deng, Richard Han, and Shivakant Mishra, "Enhancing Base Station Security in Wireless Sensor Networks", *Technical Report CU-CS-951-03*, April 2003.

[5] Mayank Saraogi, "Security in Wireless Sensor Networks", *Department of Computer Science University of Tennessee*, Knoxville Saraogi AT.

[6] Nikita Borisov, Ian Goldberg, David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, p.180-189, July 2001, Rome, Italy.

[7] Serdar Sancak1, Erdal Cayirci2, Vedat Coskun3, Sensor Wars: Detecting and Defending Against Spam Attacks in Wireless Sensor Networks.