Impact of Wireless Communications Sensor Based Secure Networks: Case Study

V K Panday[1] and Dr. G. K. Upadhyay[2]

[1]Research Scholar CMJ University, Shillong.
[2]Director Landmark Technical Campus Moradabad

Abstract: In this paper we will discuss the typical wireless sensor network consists of thousands of sensor nodes, deployed either randomly or according to some predefined statistical distribution, over a geographic region of interest. A sensor node by itself has severe resource constraints, such as low battery power, limited signal processing, limited computation and communication capabilities, and a small amount of memory; hence it can sense only a limited portion of the environment. However, when a group of sensor nodes collaborate with each other, they can accomplish a much bigger task efficiently. Wireless sensor networks are made up of a large number of inexpensive devices that are networked via low power wireless communications topologies. Here we implement the application of sensor networks include environmental monitoring system, natural disaster prediction and relief, homeland security, healthcare, manufacturing, transportation, and home appliances and entertainment.
[V K Panday and G. K. Upadhyay. **Impact of Wireless Communications Sensor Based Secure Networks: Case Study.** *N Y Sci J* 2012;5(11):152-154]. (ISSN: 1554-0200). http://www.sciencepub.net/newyork. 22

Keywords: Security, routers, wireless networks, wireless devices, sensor assets, ICT.

1. Introduction

Wireless sensor networks are application specific; they are designed and deployed for special purposes. Thus the network design must take into account the specific intended applications. Wireless sensor networks ensure a wide range of applications [**1**]; it is starting for security surveillance in military and battlefields, monitoring previously unobserved environmental phenomena, smart homes and offices, improved healthcare, industrial diagnosis, and many more. For instance, a sensor network can be deployed in a remote island for monitoring wildlife habitat and animal behavior **[2]**, or near the crater of a volcano to measure temperature, pressure, and seismic activities. Wireless sensor networks very useful network protocols which can provide the security services. Which wireless sensor network is used in many applications, the success of the network is highly dependent on the sensors' positions, referred to as the deployment of the network. Deciding the positions of the sensors is the main subject of sensor network deployment, and in turn it depends on the desired coverage of the area of interest. Sensor is the most useful and powerful device which can implement on the wireless networks. With regard to the dynamic deployment problem, initially sensors are located in the area in random positions and the sensors change their positions by using the knowledge of others positions, if they are mobile. These movements attempt to increase the coverage rate of the sensors. However, if the sensors are static, they do not have the ability to change their positions. [3]

2. Wireless Sensor Networks Deployment Problem

In wireless sensor approach we have some limitation and we can say that some problems are there. Firstly, problems in the sensor network also affect the monitoring mechanism, thus reducing the desired benefit. Secondly, scarce sensor network resources are used for inspection. In Sympathy [4], for example, up to 30% of the network bandwidth is used for monitoring traffic. Thirdly, the monitoring infrastructure is tightly interwoven with the application. Hence, adding/removing instrumentation may change the application behavior in subtle ways, causing probe effects. Also, it is non-trivial to adopt the instrumentation mechanism to different applications. [5]

2.1. Wireless Sensor Security reasons

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is midcult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first [6].

2.2. Current scenario on Wireless Sensor Networks

Current research in sensor based research areas of wireless communications networks, micro-electromechanical systems and low power design is progressively leading to the development of cost effective, energy efficient, multifunctional sensor nodes. Here we can implement the remote sensing functions and many more typical ideas of using the sensor networks. Sensing, communication, processing

and battery units are the primary components of a sensor node. Individual sensors have the capacity to detect events occurring in their area of deployment.

3. Sensor Based Communications networks

Today era many wireless sensor networks collect sensitive information and do not provide the any other person. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. Further, wireless communications make it easy for an adversary to eavesdrop on sensor transmissions. For example, one of the most challenging security threats is a *denial-of-service* attack, whose goal is to disrupt the correct operation of a sensor network.[7]

4. Wireless sensor Based Security analysis

In this world we can imagine we are the atomic world. And in this tome Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. [10]

4.1. Deployment Problems of wireless sensor networks

In this paper we contain a classification of the problems typically found during deployment according to our own experience. Here, a problem is essentially defined as a behavior of a set of nodes that is not compliant with the specification. We classify problems according to the number of nodes involved into four classes: node problems that involve only a single node, link problems that involve two neighboring nodes and the wireless link between them, path problems that involve three or more nodes and a multi-hop path formed by them, and global problems that are properties of the network as a whole. [5]

5. Wireless sensor networks Application

There are many applications of wireless sensor networks. But few applications are as follows:

5.1. Military Application

Today era is very beautiful because most of the elemental knowledge of sensor networks is basic on the defense application at the beginning, especially two important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology form the Defense Advanced Research Project Agency (DARPA), sensor networks are applied very successfully in the military sensing. [7] Now wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems.

6. Wireless Sensor Based Architecture

In this network we can create the typical architecture on the following based as follows: [10]

- Gateway or Access points – A Gateway enables communication between Host application and field devices.
- Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
- Security manager – The Security Manager is responsible for the generation, storage, and management of keys. [10]

6.1. Wireless Communication security Environment Application

Nowadays sensor networks are also widely applied in habitat monitoring, agriculture research, fire detection and traffic control. [8] Because there is no interruption to the environment, sensor networks in environmental area is not that strict as in battlefield.

Conclusion

In this paper we can discuss the wireless sensor based applications, and in many of these applications the environment can be hostile where human intervention is not possible and hence, the sensor nodes will be deployed randomly or sprinkled from air and will remain unattended for months or years without any battery replacement and security analysis. Therefore, energy consumption or, in general, resource management is of critical importance to these networks. By being able to estimate the energy consumption of the sensor nodes, applications and routing protocols are able to make informed decisions that increase the lifetime of the sensor network of security aspects.

References

[1]. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E., A Survey on Sensor Networks," in *IEEE Communications Magazine*, Aug. 2002.

[2]. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, Wireless sensor networks for habitat monitoring, Proc. 1st ACM Int. Workshop on Wireless Sensor

Networks and Applications (WSNA'02), Atlanta, GA, Sept. 2002, pp. 88–97.
[3]. Gaige Wang, Lihong Guo, Hong Duan, Luo Liu, Heqi Wang, Dynamic Deployment of Wireless Sensor Networks by Biogeography Based Optimization Algorithm, *J. Sens. Actuator Netw.* 2012,
[4]. N. Ramanathan, K. Chang, R. Kapur, L. Girod, E. Kohler, and D. Estrin. Sympathy for the Sensor Network Debugger. In SenSys 2005
[5]. Matthias Ringwald, Kay Romer, Deployment of Sensor Networks: Problems and Passive Inspection.
[6]. D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.
[7]. Chee-Yee Chong; Kumar, S.P., "Sensor networks: Evolution, opportunities, and challenges,"Proc IEEE, August 2003.
[8]. Akyildiz, I.F., W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks",IEEE Communications Magazine, August, 102-114(2002).
[9]. H. Chan and A. Perrig. Security and privacy in sensor networks. IEEE Com- puter Magazine, pages 103–105, 2003 2003.
[10]. Hemanta Kumar Kalita and Avijit Kar, wireless sensor network security analysis, International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

10/26/2012