International Journal of Information Technology and Management

Vol. V, Issue No. I, August-2013, ISSN 2249-4510

WIRELESS SENSOR NETWORKS - SECURITY ISSUES AND ITS CHALLENGES

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. V, Issue No. I, August-2013, ISSN 2249-4510

Wireless Sensor Networks - Security Issues and Its Challenges

Jhujhar Singh

Assistant Professor, Department of Computer Science, Guru Nanak Khalsa College, Karnal

Abstract – In this paper we present about wireless sensor networks - security issues and its challenges. The sensing technology combined with dispensation authority and wireless communication makes it lucrative for being oppressed in abundance in future.

Keywords: Wireless Sensor Networks, WSN, networking, security

----------♦----------

INTRODUCTION

Wireless Sensor Networks (WSN) are up-and-coming as both an important new tier in the IT bionetwork and a rich domain of active research involving hardware and system plan, networking, distributed algorithms, programming models, data management, security and social factors [Culler, D. E and Hong, W.], [Dai, S, Jing, X, and Li, L]. WSN is particularly susceptible against external and internal attacks due to its exacting characteristics. It is necessary to provide WSN with basic security mechanisms and protocols that can guarantee a negligible protection to the services and the in order flow. This means the hardware layer needs to be protected against node cooperation, the communication channels should meet certain security goals (like privacy, honesty and authentication), and the protocols and services of the network must be robust next to any possible interference.

A Wireless Sensor Network (WSN) can be definite as a group of sovereign nodes, communicating wirelessly over limited frequency and bandwidth [Akyildiz, I. F, and Su, W., Sankarasubramaniam, Y. and Cayirci, E]. Distributed sensing allows for closer placement to the phenomena to be achieved, when the exact location of a particular event is unknown, than is possible using a single sensor [Bharathidasan, A., Anand, V., Ponduru, S.].

SECURITY INTIMIDATION AND CONCERNS IN WSN

Wireless Sensor Networks are susceptible to security attacks due to the transmit nature of the transmission medium. Basically attacks are broadly confidential in two categories i.e. active attacks and passive attacks. This paper points out both of these attacks in details.

PASSIVE ASSAULT

To keep an eye on the statement channel by illegal assaulters are known as passive attack. Some of the more ordinary attacks against sensor privacy are:

- **Monitor and Eavesdropping:**

This is the most common attack to privacy. By inquisitive to the data, the adversary could easily find out the communication contents.

- **Traffic Analysis:**

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

- **Camouflage Adversaries:**

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

ACTIVE ATTACKS

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

- **Routing Attacks in Sensor Networks:**

The attacks which act on the network layer are called routing attacks. The following are the attacks that occur while routing the communication.

- **Attacks on Information in transit:**

In a sense or network, sensors monitor the changes of precise parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless statement is susceptible to eavesdropping, any attacker can monitor the traffic flow and get into action to break off, intercept, modify or fabricate packets thus, give wrong information to the base stations or sinks.

- **Selective Forwarding:**

A malicious node can selectively drop only certain packets. Particularly effective if combined with an attack that gathers much traffic via the node. In sensor networks it is unspecified that nodes devotedly forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.

- **Black hole/Sinkhole Attack:**

In this attack, a malicious node acts as a black hole to pull towards you all the traffic in the sensor network. In fact, this attack can affect even the nodes those are considerably far from the base stations.

CONCLUSION:

In this paper we found that security in wireless sensor network is one of the most important research issues. In today's time, many of projected security schemes are based on specific network models. We found that there is be deficient in of collective effort to take a common model to ensure the security mechanism.

REFERENCES:

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002) 'A Survey on Sensor Networks', IEEE Communications Magazine, 40(8), 102-114.

[2] Bharathidasan, A., Anand, V., Ponduru, S. (2001), Sensor Networks: An Overview, Department of Computer Science, University of California, Davis 2001. Technical Report.

[3] David Boyle, Thomas Newe "Securing Wireless Sensor Networks: Security Architectures" journal of networks, vol. 3, no. 1, january 2008.

[4] Vikash Kumar, Anshu Jain and P N Barwal "Wireless Sensor Networks: Security Issues, Challenges and Solutions" International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 859-868.

[5] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[6] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.

[7] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges" ICACT2006, ISBN 89-5519-129-4