# Security Issues in Wireless Sensor Networks (WSN)

**JHUJHAR SINGH ,Assistant Professor**
**Dept. of Computer Science, Guru Nanak Khalsa College,**
**Karnal 132001 (Haryana)**

**ABSTRACT:**

The sensor networks technology as one of the main technology in the future has posed various challenges to researchers. Wireless Sensor Networks (WSN) is composed of large number of tiny sensors nodes, running separately. As every network, sensor networks are exposed to security threats which, if not properly addressed, can exclude them to be deployed in the envisaged scenarios. These types of networks processing sensitive data are facing the risk of data manipulation. Our focus should not only be on how to secure sensor networks, but also on how this can be done through generic and independent solutions.

Keywords: Resilience to Denial of Service Attacks, Node Compromises, Routing Security, Secure Aggregation and Dissemination

## I. INTRODUCTION

During the past few years there has been an explosive growth in the research devoted to the field of wireless sensor networks (WSN), covering a broad range of areas, from understanding theoretical issues to technological advances that made the realization of such networks possible. These networks use hundreds to thousands of inexpensive wireless sensor nodes (motes) over an area for the purpose of monitoring certain phenomena and capture geographically distinct measurements. The pervasive interconnection of such devices has given birth to a broad class of exciting new applications in several areas of our lives, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. However, as every network, sensor networks are exposed to security threats which, if not properly addressed, can exclude them to be deployed in the envisaged scenarios. Their wireless and distributed nature and the serious constraints in node battery power prevent previously known security approaches to be deployed and have created a large number of vulnerabilities that attackers can exploit. Unfortunately, while sensor networks were in their infancy, the main research focus was on making sensor networks feasible and useful, and less emphasis was placed on security. A number of new protocols have been designed for Tiny OS [Hil00], which is an operating system specially designed for wireless sensor networks. Most of these protocols are built assuming a trusted environment and are very vulnerable against security attacks. Therefore, our focus should not only be on how to secure sensor networks, but also on how this can be done through generic and independent solutions[1,9,10,12].

## II. OBSTACLES IN SENSOR NETWORKS SECURITY

Security architecture for sensor networks must integrate a number of security measures and techniques in order to protect the network and satisfy the desirable requirements we have outlined. In what follows we describe a comprehensive set of these components (and the techniques involved) that are currently under research in sensor networks. Some of these research issues are similar to those faced in traditional networks, only with some additional constraints; others are unique to sensor networks. Although wireless sensor networks have an ad-hoc nature, there are several limitations that make security mechanisms proposed for ad-hoc networks not applicable in this setting. In particular, security in sensor networks is complicated by more constrained resources and the need for large-scale deployments. A wireless sensor network has many constraints compared to other networks; because

of these constraints it is more difficult to directly deploy the traditional security approaches in WSNs. Therefore, to develop useful security mechanisms while borrowing the ideas from the existing security techniques, it is impressive to understand these constraints first as in[2,5].

***Limited Resources***

All security techniques require a specific amount of resources for the implementation, including code space, data memory, and energy to power the sensor devices. However, these resources are very limited in a wireless sensor device. The two major limitations are storage space and battery power:

1) Limited Storage Space and Memory: A tiny sensor device has a small amount of memory and storage space for the code. Indeed, to construct effective security techniques, it is necessary to limit the size of the security algorithm code. For example, Zigbex sensor type HBE has an 8-bit, 7.372 MHz ATmega128L RISC MCU with only 4Kb SRAM, 128 Kb flash memories, and 512 Kb flash storage.

2) Power Limitation: Another strongest constraint to wireless sensor capabilities is power energy. Once sensor nodes are deployed in a sensor network the energy must be conserved for prolonging the life of the individual sensor node and the entire sensor network.

***Unreliable Communication***

The secure network depends on a protocol, which eventually, depends on communication within the entire network.

1) Unreliable Transfer: Because of the inherent unreliable wireless routing in sensor network, packets may get damaged due to channel errors or dropped at highly congested nodes in the network.

2) Conflicts: Due to the broadcast nature of the wireless sensor network, packets may collide in the middle of transfer and conflict will occur.

3) Latency: Latency is due to the multi-hop routing, congestion, and node processing delay in the sensor network. In the presence of latency it is too difficult to achieve synchronization among sensor nodes.

## III. SECURITY REQUIREMENTS FOR WSNs

In this section, we present a brief overview for a security goals in sensor networks .Requirements of WSNs are encompassing both the typical network requirements and the unique requirements suited solely to WSNs.

***A. Data Confidentiality***

It is the ability to hide message from a passive attacker and is the most important issue in network security. The network with any security focusing must address this problem. In sensor networks, the confidentiality relates to the following:

1) A sensor network should not leak sensor readings to its neighbors.

2) Sensor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in a wireless sensor network.

3) Sensor identities and public keys should also be encrypted to some extent to protect against traffic analysis attack.

***B. Data Integrity and Authentication***

Integrity refers to the ability to confirm that message has not been tampered or changed while it was on the network. An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. Indeed, data authentication allows a receiver to verify that the data is really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism.

***C. Data Freshness***

By supposing that both forenamed goals are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no messages has been replayed. This requirement is especially important when there are shared-key strategies employed in the design and need to be changed over time.

***D. Availability***

It is to verify if a node has the ability to utilize the resources and the network is available for the message to move on.

***E. Self-Organization***

WSN is typically an ad hoc network, which requires every sensor node to be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature also brings a great challenge to wireless sensor network security.

***F. Time Synchronization***

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two sensors.

A more collaborative sensor network may require group synchronization for tracking application.

***G. Secure Localization***

The use of a sensor network will depend on its ability to accurately and automatically locate each node in the network. A sensor network designed to locate faults, this need accurate location information in order to pinpoint the location of a fault [3, 5, 9].

## IV. ATTACKS ON SENSOR NETWORKS

### *A. Resilience to Denial of service attacks (DoS)*

Adversaries can limit the value of a wireless sensor network through DoS attacks making it imperative to defend against them. DoS attacks can occur at multiple protocol layers [Woo02], from radio jamming in physical layer to flooding in transport layer, all with the same goal: to prevent the network from performing its expected function. Adversaries can involve malicious transmissions into the network to interfere with sensor network protocols and induce battery exhaustion or physically destroy central network nodes.

### *B. Resilience to Node Compromises*

Recent advances in sensor networks research have shown that even without physical access, an attacker can still manage to modify the code running on the nodes, by exploiting memory-related vulnerabilities, e.g., buffer over flow [Goo07b; Goo07a]. This has been demonstrated for Tiny OS 2.x on a T mote Sky wireless sensor node, which uses the Texas Instruments MSP430 microcontroller. The way to inject code into the node is to craft a packet which when copied over the stack – overwrites the return address with the address of the global copy of itself [4,6,9].

### *C.Routing Security*

Packet routing is one of the most essential services in sensor networks, as it is used to exchange messages with sensor nodes that are outside of a particular radio range. Researchers have proposed several approaches for efficient routing, but rarely do they consider security as a central design parameter [Par06]. Usually a trusted environment is assumed, where all sensor nodes cooperate and no attacker is present. Securing such protocols is very important, since even a single compromised node could completely paralyze communication in the network.

### *D. Location Aware Security*

Many applications of sensor networks require location information, not only for routing purposes, but also for determining the origin of the sensed information or preventing threats against services [Liu03; Laz03]. Many localization techniques have been proposed, but little research has been done in securing the localization scheme [Sas03; Laz05; ˇC06; Du06]. Security in this case is twofold: Each node must determine its own location in a secure way (secure localization) and each node must verify the location claim of another node (location verification) [11, 12].

### *E. Secure Aggregation and Dissemination*

Since sensor nodes have limited energy which may be exhausted, sensor networks are densely deployed to deal with connectivity and coverage problems. This causes neighbouring nodes to have overlapping sensing regions and generate correlated measurements whenever an event occurs in this overlap. Moreover, sensor nodes are usually deployed randomly, which reinforces the effect of overlapping regions. Each node observes its sensing region independent of its neighbours and sends its measurements to the base station. In particular, the following requirements must be supported by the key management scheme, in order to facilitate data aggregation and dissemination process:

1. Data aggregation is possible only if intermediate nodes have access to encrypted data so that they can extract measurement values and apply to them aggregation functions. Therefore, nodes that send data packets toward the base station must encrypt them with keys available to the aggregator nodes.

2. Data dissemination implies broadcasting of a message from the aggregator to its group members. If an aggregator shares a different key (or set of keys) with each of the sensor within its group, then it will have to make multiple transmissions, encrypted each time with a different key, in order to broadcast a message to all of the nodes. But transmissions must be kept as low as possible because of their high energy consumption rate [12].

### *F. Link-layer Security*

What makes link-layer security important is that end-to-end security mechanisms are not possible in sensor networks, so more transparent mechanisms provided by the link layer are needed. Protocols used in conventional networks for end-to-end security, such as SSH [Ylo96], SSL [ssl01], or IP Sec [Ken98], even though they are feasible in constrained embedded devices [Gup05], they are considered inappropriate since they do not allow in-network processing and data aggregation which play an important role in energy efficient data retrieval. These operations require the intermediate nodes to access and possibly modify the contents of packets, which would not be possible if an end-to-end

security scheme was used. In sensor networks it is also important to allow intermediate nodes to check message integrity and authenticity, or else the network would be prone to several denial of service attacks.

### *G. Secure Network Programming*

The process of programming sensor nodes typically involves the development of the application in a PC and the loading of the program image to the node through the parallel or the serial port. The same process is repeated for all the nodes of the sensor network before deployment. However, after deployment, there is often the need to change the behavior of the nodes in order to adapt to new application requirements or new environmental conditions. This would require the effort of re-programming each individual node with the updated code and relocate it back to the deployment site. Network programming saves this effort by propagating the new code over the wireless link to the entire network, as soon as that code is loaded to only one node. Then, nodes reprogram themselves and start operating with the updated code. As network programming simplifies things for legitimate users, it also simplifies things for attackers that want to disrupt the normal operation of the network or operate them for their own advantage[13,14].

## V. CONCLUSIONS

This paper outlined different security issues in wireless sensor network in general and made an extensive study of different threats associated with existing data gathering protocols. As these protocols are not designed taking security issues into account, most of them are prone to different types of attacks. Even some of the protocols are seems to be vulnerable to most of the attacks. Similarly some attacks like HELLO flood, Acknowledgement spoofing and sniffing can be used by the adversaries to affect most of the protocols.

## REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Communications Magazine,* vol. 40, no. 8, pp.102-114, August 2002.
[2] 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.
[3] Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, and Tanveer A. Zia, “Threat Models and Security Issues in Wireless Sensor Networks”, *International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October 2013*
[4] I.F. Akyildiz, E.P. Stuntebeck, “Wireless underground sensor networks: research challenges”, *Ad-Hoc Networks* 4 (2006) 669–686

[5] Kriti Jain, Upasana Bahuguna, "Survey on Wireless Sensor Network", *IJSTM,* Vol. 3 Issue 2, pp. 83-90, Sept 2012
[6] Jaydip Sen, *Security and Privacy Challenges in Cognitive Wireless Sensor Networks*, Dec 2012
[7] Shio Kumar Singh, M P Singh, D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", *International Journal of Computer Trends and Technology-*, May to June Issue 2011, ISSN: 2231-2803
[8] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", *IJCIT,* vol. 2, issue 1, pp. 62-67, 2011
[9] Snehlata Yadav, Kamlesh Gupta, Sanjay Silakari, "Security issues in wireless sensor networks", *Journal of Information Systems and Communication,* vol. 1, issue 2, 2010, pp-01-06
[10] Pooja , Manisha, Dr. Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks", *International Journal of P2P Network Trends and Technology,* vol. 3, issue 1, pp. 7-13, 2013
[11] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi, Sareh Beheshti, **"**A Survey on Wireless Sensor Networks Security", SETIT 2007, *4th International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications,* March 25-29, 2007 – TUNISIA
[12] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In *Proc. of the 1st IEEE Int. Workshop on Sensor Network Protocols and Applications (SNPA'03)*, pp. 113-127, May 2003
[13] X. Wang, W. Gu, K. Schosek, S. Chellappan, D. Xuan, "Sensor network configuration under physical attacks", *International Journal of Ad Hoc and Ubiquitous Computing*, Vol 4, Issue 3/4, pp. 174-182, April 2009
[14] A.D. Wood, J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, Vol. 35, Issue 10, pp. 54-62, October 2002