# Security in Wireless Sensor Network

Pritesh Patel, Nikhil Lende
PG Student
Computer Engineering Department, MAEER'S MIT Pune

***Abstract*—Wireless Sensor Networks (WSN) is an emerging technology and day by day it is attracting the attention of researchers with its challenging characteristics and diversified application domain. The more researchers try to develop further cost and energy efficient computing devices and algorithms for WSN, the more challenging it becomes to fit the security of WSN into that constrained environment. However, security is crucial to the success of applying WSN. So, familiarity with the security aspects of WSN is essential before designing WSN system. In this paper, we survey the state of art in securing wireless sensor networks. We review several protocols that provide security in sensor networks. . Also, this study documents the well known attacks at the Network layer of WSN.**

***Index Terms— Wireless Sensor Network, Network Security, Adhoc-network, Attack***

## I. INTRODUCTION

With the advances in wireless communication and computing devices, Wireless Sensor Network has come into the spotlight. By utilizing these advances, WSN provides low cost solution to a variety of real world challenges. A Wireless Sensor Network is a combination of wireless networking and embedded system technology that monitors physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Initially, Wireless Sensor Networks were mainly used for military surveillance.[1] However, now its applicability is extended to civilian and commercial application areas, including environmental and medical monitoring, manufacturing machinery performance monitoring, home automation, traffic control etc.

The basic building block of a sensor network is an individual sensor node. A typical node might, for example, monitor temperature, light, sound, or odor, the final choice is application dependent. A sensor node is characterized by its small size, meager computing power, low communication bandwidth, and a limited energy supply. Given these limitations, sensor nodes are typically deployed redundantly in large number (possibly on the order of thousands) within a target environment. Currently, sensor nodes exist only on a macro-scale, that is, they are visible to the naked human eye. Limitations on size do effect how and where sensor networks can be deployed. Researches envision a micro-scale and even a nano scale sensor nodes that could be deployed, say,
within the human body or some other confined space. This means that the number of micro- and/or nano-scale sensor nodes deployed within some environment could approach (on the order) the number of hosts in today's Internet.[2][3][4] However, currently such networks are only now being theoretically investigated. The protocols and methods presented in this paper are primarily applicable to macro scale sensor networks.

The design limitations, communication and deployment patterns of WSN pose several security problems to it and make it vulnerable to different type attacks. Exploiting those security holes adversaries can perform different types of attacks in order to disrupt the network, hamper or misguide the communication flow of the network, or to intercept, fabricate or modify the confidential data. To combat against those attacks coming from different levels of WSN security vulnerabilities, firstly, it is very important to know about the security requirements of WSN. Moreover, analysis of security requirements gives right directions to develop or implement the proper safeguards against the security violations [5][6].

## II. SECURITY PROBLEMS

Usually, sensor nodes are densely deployed and they interact with their surrounding environment very closely. They are operated unattended and also without the absence of any remote monitoring system. That is, the nodes are exposed to the hostile environment as well as to the attackers and at a risk of physically being tampered. So, there is always the possibility of capturing nodes physically by the attackers to attack the WSN. Also, there are lots of security problems in Wireless Sensor Network that can be logically exploited by the adversaries to attack the networks. According to [7][8][9] the security problems in WSN as follows.

Sensor nodes themselves are points of attack for the Wireless Sensor Networks. Adversaries can compromise or subvert sensor nodes to gain full control of them and utilize them for disrupting the network. If sensor nodes are compromised, the attackers are able to know all the confidential information stored on them and may launch a variety of malicious actions against the network through these compromised nodes. For example, the compromised nodes may discard important data or report with wrong or modified data to mislead any decision which is taken based on this data. The subverted nodes may reveal the cryptographic key information and thus allow the attackers to compromise the whole network. False malicious nodes can be added to exhaust other sensor nodes, attract them to send data only to it preventing the passage of true data.

Besides the sensor nodes, attackers can target the routing information which is used to maintain the communication between sensor nodes and the base station.



ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

The routing mechanisms used for WSN requires complete trust between all the participating nodes. The proper transport of data in the network depends on the integrity of the routing information given by other nodes. False routing information transmitted by a host may partition the network by misguiding the traffic to a small group of nodes and thus causes difficulty in communication.

Again, the unreliable wireless medium used as communication medium in WSN causes many security problems.[10] The adversary just needs to be within the radio range of the nodes. Being there, he can easily intercept the transmission without causing any interruption in the network communication. Thus, an adversary can collect sensitive information if the transmission is not encrypted. Also, an attacker can easily inject malicious messages in the WSN.

## III. SECURITY REQUIREMENTS

Wireless Sensor Network is vulnerable to various attacks like any other conventional network, but its limited resource characteristics and unique application features requires some extra security requirements including the typical network requirements. [10] [11] [12] discuss on several security properties that should be achieved when designing a secure WSN.

### 1. DATA CONFIDENTIALITY

Data confidentiality is one of the vital security requirements for WSN because of its application purpose (for example, military and key distribution applications). Sensor nodes communicate sensitive data, so it is necessary to ensure that any intruder or other neighboring network could not get confidential information intercepting the transmissions. One standard security method of providing data confidentiality is to encrypt data and use of shared key so that only intended receivers can get the sensitive data.

### 2. AUTHENTICITY AND INTEGRITY

Only providing data confidentiality is not enough to ensure the data security in WSN. As an adversary can change messages on communication or inject malicious message, authentication of data as well as sender are also crucial security requirements. Source authentication provides the truthfulness of originality of the sender. Whereas, data authentication ensures the receiver that the data has not been modified during the transmission.

### 3. AVAILABILITY

We cannot ignore the importance of availability of nodes when they are needed. For example, when WSN is used for monitoring purpose in manufacturing system, unavailability of nodes may fail to detect possible accidents. Availability ensures that sensor nodes are active in the network to fulfill the functionality of the network. It should be ensured that security mechanisms imposed for data confidentiality and authentication are allowing the authorized nodes to participate in the processing of data or communication when their services are needed.

As sensor nodes have limited battery power, unnecessary computations may exhaust them before their normal lifetime and make them unavailable. Sometimes, deployed security protocols or mechanisms in WSN are exploited by the adversaries to exhaust the sensor nodes by its resources and makes them unavailable for the network. So, security policies should be implied so that sensor nodes do not do extra computation or do not try to allocate extra resources for security purpose.

## IV. REQUIREMENT FOR SECURE SENSOR NETWORK PROTOCOL

The above mentioned security requirements are the basic security needs for WSN. However, sensor nodes are always at a risk of physically being captured. Only fulfilling those basic requirements cannot totally solve the security problems created by node compromise. Tamper resistance hardware can protect the data stored on sensor node. But using such hard ware exceeds the cost limit of WSN by increasing cost of individual sensor node. So, a better solution is to design secure sensor network protocols that are resilient to node comprise or node failure. Secure protocols can also be developed to achieve the basic security requirements.

Security protocols for WSN should have the capability of providing the following requirements besides the basic security requirements to ensure proper security functionality in WSN.

### A. DATA FRESHNESS

Data Freshness implies that the data is recent. This is an important security requirement to ensure that no message has been replayed meaning that the messages are in an ordering and they cannot be reused. This prevents the adversaries from confusing the network by replaying the captured messages exchanged between sensor nodes. To achieve freshness, security protocols must be designed in such a way that they can identify duplicate packets and discard them preventing replay attack.

### B. ROBUSTNESS AGAINST ATTACKS

Security protocols should have robustness against attacks. If an attack is performed they should have the ability to minimize the impact. They also should have the ability to detect failed sensor nodes and work with the remaining nodes and updated topology.

### C. RESILIENCE

In practice, detection of compromised nodes and revocation of their cryptographic keys are not always possible. So, a security protocol should always consider WSN with compromised nodes. If a number of nodes are compromised, secure protocols should function in such a way that the performance of WSN degrades gracefully.

### D. BROADCAST AUTHENTICATION

The base station broadcasts command and data to sensor nodes. An attacker can modify or forge the commands and sensor nodes perform incorrect operations accepting those commands. So, secure protocols should provide broadcast authentication functionality for the sensor nodes.



ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

E. SCALABILITY

The number of sensor nodes in WSN can be of several orders of magnitudes and the nodes are densely deployed. Again, the network topology of WSN is dynamic in nature that is new nodes can be added extending the network size. So, scalability is an important issue and security protocols as well as key management should cope with the increasing network size. A security mechanism is not an efficient one if it performs well in a small size network but does not work well for large size network.

## V. ATTACKS IN WIRELESS SENSOR NETWORK

### 1. PHYSICAL ATTACK

This attack is also known as node capture. In this type of attack, attackers gain full control over some sensor nodes through direct physical access [3]. As the cost of sensor nodes must be kept as cheap as possible for WSN, sensor nodes with tamper proofing features are impractical. This is why sensor nodes are susceptible to be physically being accessed. Physical attacks have significant impacts on routing and access control mechanisms of WSN. For example, getting key information stored on sensor node's memory gives attacker the opportunity of unrestricted access to WSN.

### 2. ATTACKS AT NETWORK LAYER.

Network layer is responsible for routing messages from one to another node which are neighbors or may be multi hops away for example, node to base station or node to cluster leader. The network layer for WSN is usually designed considering the power efficiency and data centric characteristics of WSN. There are several attacks exploiting routing mechanisms in WSN. Some familiar attacks are listed here.

A. SELECTIVE FORWARDING

Selective forwarding is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to minimize the suspicion to the neighbor nodes. The impact becomes worse when these malicious nodes are at closer to the base station [14]. Then many sensor nodes route messages through these malicious nodes. As a consequence of this attack, a WSN may give wrong observation about the environment which affects badly the purpose of mission critical applications such as, military surveillance and forest fire monitoring. This attack can be extended to forward messages to wrong nodes and thus misdirecting the traffic.

Two different countermeasures have been proposed against selective forwarding attack. One defense is to send data using multi path routing [8]. Another one is detection of compromised nodes which are misbehaving in terms of selective forwarding and route the data seeking an alternative path. [15][16] proposes CHEMAS (CHEckpoint-based Multi-hop Acknowledgement Scheme), a lightweight security scheme for detecting selective forwarding attacks. This scheme randomly selects a number of intermediate nodes as checkpoints which are responsible for generating acknowledgement. According to this scheme, along a forwarding path, if a checkpoint node does not receive enough acknowledgements from the downstream checkpoint nodes it can detect abnormal packet loss and identify suspect nodes.

B. SINKHOLE ATTACK

In sinkhole attack, a compromised node attracts a large number of traffic of surrounding neighbors by spoofing or replaying an advertisement of high quality route to the base station [17]. The attacker can do any malicious activity with the packets passing through the compromised node.

C. WORMHOLE ATTACK

Wormhole is a critical attack, where the attacker receives packets at one point in the network, tunnels them through a less latency link than the network links to another point in the network and replay packets there locally [13]. This convinces the neighbor nodes of these two end points that these two distant points at either end of the tunnel are very close to each other. If one end point of the tunnel is at near to the base station, the wormhole tunnel can attract significant amount of data traffic to disrupt the routing and operational functionality of WSN. In this case, the attack is similar to sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station.

D. HELLO FLOOD ATTACK

In Hello flood attack, the attacker broadcasts hello message with a very powerful radio transmission to the network to convince all nodes to choose the attacker to route their messages. The affected nodes waste their energy by sending messages to the node which is out of their radio range.

E. SYBIL ATTACK

In Sybil attack, a malicious or subverted node forges the identities of more than one node or fabricates identity. This attack has significant effect in geographic routing protocols [17]. In the location based routing protocols, nodes need to exchange location information with their neighbors to route the geographically addressed packets efficiently. Sybil attack disrupts this protocol functionality simultaneously being at more than one place.

## VI. CONCLUSION

With super small sensor nodes, super low power consumption and alluring low cost, Wireless Sensor Network is attracting uncountable application domains to sense and collect data. But, these attractive features made Wireless Sensor Network challenging to integrate security mechanism into it. This paper gives an idea of a major subset of security problems that Wireless Sensor Network faces because of its exceptional design characteristics, communication and deployment pattern.

At the same time, this paper includes brief discussion on the important security aspects that are required to design a secure Wire Sensor Network. Some Well known attacks and their proposed counter measures are also discussed in this paper in order to give an idea about how the adversaries can actually attack the WSN exploiting its vulnerabilities and what kind of security awareness should be taken into account when incorporating security mechanisms



ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

in WSN. Finally, this paper explores some works on three crucial security aspects of WSN which are key management, link layer security and secure routing. There are also many security aspects of WSN such as secure data aggregation, intrusion detection, secure localization, etc. which are not covered in this paper.

There are many security solutions or mechanisms that have been proposed for Wireless Sensor Network; some of which are concerned about specific security attacks whereas some are concerned about specific security aspect. There is no standard security mechanism that can provide overall security for WSN. Providing such mechanism is not possible also as WSNs are implemented in various application domains with different level of security requirements. Designing a secure WSN needs proper mapping of security solutions or mechanisms with different security aspects. This also imposes a research challenge for WSN security.

.

## REFERENCES

[1] F. Anjum and P. Mouchtaris "SECURITY FOR WIRE- LESS AD HOC NETWORKS" Wiley, 2007
[2] Mayank S "Security in Wireless Sensor Networks," In ACM SenSys, 2004
[3] Al-Sakib K P, H-W Lee, C S Hong, "Security in Wireless Sensor Networks: Issues and Challenges" Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Volume: 2) 6 pp. – 1048, 20-22 Feb. 2006
[4] Akyildiz IF, Su W, S Y, Cayirci E. "A survey on sensor networks," IEEE Communications Magazine 2002; 40 (8): 102–114
[5] Y. W. Law and P. Havinga "How to secure a wireless sensor network," pages 89–95, Dec. 2005
[6] C. W. L. Weimin, Y. Zongkai and T. Ymmen "Research on the security in wireless sensor network," TAsian Journal of Information Technology, 2009
[7] Z. Tanveer and Z. Albert "Security issues in wireless sensor networks," In ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication, page 40, Washington, DC, USA, 2006. IEEE Computer Society
[8] B. Xiao, B. Yu, and C. Gao Chemas: "Identify suspect nodes in selective forwarding attacks" Journal of Parallel and Distributed Computing, 67(11):1218 – 1230, 2007.
[9] S. Zhu, S. Setia, and S. Jajodia "Leap: efficient security mechanisms for large-scale distributed sensor networks" In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, pages 62–72, New York, NY, USA, 2003. ACM Press
[10] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar "Spins: Security protocols for sensor networks," In Wireless Networks pages 189–199, 2001
[11] E. Shi and A. P. "Designing secure sensor networks" In Wireless Communications, IEEE , volume 11, December 2004
[12] S. Datema, "A Case Study of Wireless Sensor Network Attacks" Master's thesis, Delft University of Technology, September 2005.
[13] D. R. Raymond and S. F. Midkiff "Denial-of-service in wireless sensor networks: Attacks and defenses" In IEEE Pervasive computing, volume 7, pages 74–81, 2008.
[14] I. Khalil, S. Bagchi, and N. B. Shroff "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks" Computer Network, 51(13):3750–3772, 2007
[15] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless communications, Volume 11, Issue 1, February 2004, pp. 38 – 47
[16] Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30. .
[17] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268


ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET