Wireless Sensor Network (WSN): Security Issues, Challenges and Solutions

JHUJHAR SINGH

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

Abstract

Wireless Sensor Network technology is combined with processing power & wireless communication which makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology incurs various types of security threats. Security issues of sensor network are different from that of conventional network. The intent of this paper is to explore the security related issues, challenges and propose some solutions to secure the wireless sensor network (WSN) against security threats. Further, as security being vital to the acceptance and use of sensor network for many applications; I have made an in depth threat analysis & propose some security mechanism in wireless sensor network.

Keywords: Issues, Challenges, Security, Wireless Sensor Network (WSN)

Introduction

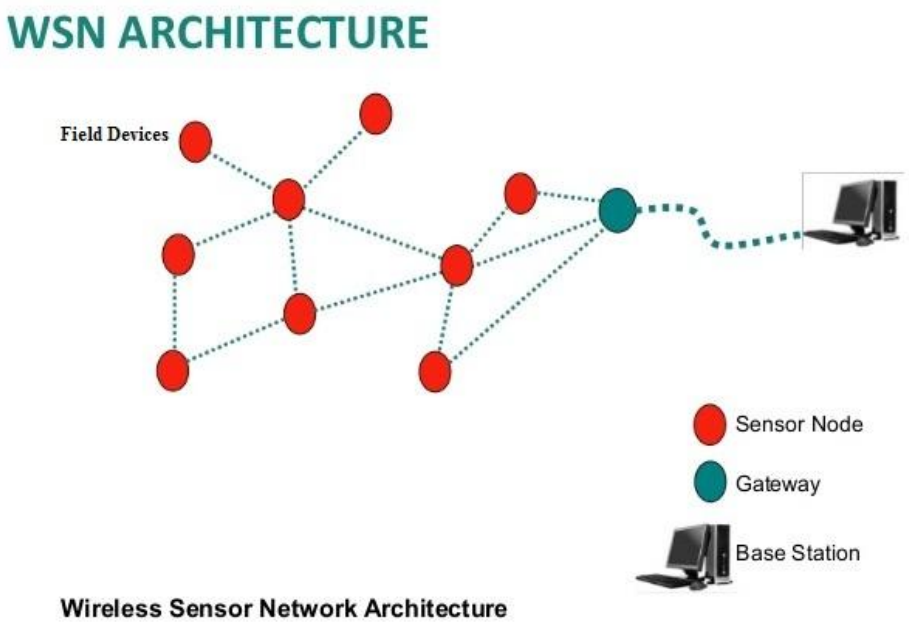
A Wireless Sensor Network can be defined as a group of independent nodes, which are communicate wirelessly. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sense some changes of communication with other devices for some specific purpose like target tracking, surveillance etc. Today sensor can monitor temperature, pressure, humidity, soil makeup, vehicle movement, noise level and other properties. Sensor networks are highly distributed networks of small lightweight wireless nodes deployed in large numbers to monitor the system. Build up sensors have been made possible by the recent advance in micro-electro-mechanical system (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit. A wireless sensor network is scattered in a region where it is meant to collect data through its sensor nodes. The applications of sensor networks are endless. This paper provides an overview of security issues, challenges and solutions in wireless sensor networks

To design a complete secure wireless sensor network, security must be integrated in to every node of the system. Any component of a network implemented without any security could easily become a point of attacks. Security in wireless sensor networks can be defined as a method of protecting prospective applications against all known types of attacks. Attacks including Denial-of-Service, Traffic Analysis, Multiple identity/manipulation of routing information, cloning, hello flood, Sybil, Wormhole, Sinkhole etc. are all areas for concern within wireless sensor network security architecture design. It is extremely important to ensure that all known attacks are defended against when designing security system for a wireless sensor network.

Architecture of Wireless Sensor Network (WSN)

In a typical WSN we see following network components:

- Network Manager - The responsibility of the network manager is to configure the network.
- Security Manager - The overall responsibility of the security manager is to generate, store and manage keys.
- Interfacing with the sensor and an energy source, usually a battery or an embedded from of energy harvesting.
- Gateway Access Point – A gateway enable communication between host application and field devices.



Wireless Sensor Network Architecture

Wireless sensor network security analysis

In order to protect sensed data and communication exchange between sensor nodes, it is important to guarantee the secrecy of message. In the sensor network all this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However encryption protects against outside attacks.

Attacks on Sensor Network

Wireless Sensor Networks are vulnerable to security attacks due to the broadcast nature of the transmission media. Therefore sensor networks are particularly vulnerable to several key types of attacks.The most popular attacks are:-

Basically attacks are broadly classified in two categories i.e. active attacks and passive attacks.

A. Active attacks:

The unauthorized attacks monitors, listen to and modifies the data streams in the communication channel as known as active attacks. The following active attacks are:

a) Routing Attacks in Sensor Networks: The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the message
   - Sybill Attack: A single node presents multiple identities to other nodes in the network.
   - Sinkhole Attack: Attracting traffic to a specific node.
   - Wormholes Attack: An attacker records packets at one location in the network, tunnels them to another location & transmit in to the network.
   - HELLO Flood Attack: This attack use HELLO packets as a weapon to convince the sensor in wsn (attacker routing protocol's HELLO packets from one node to another).
   - Selected Forwarding: A malicious node can selectively drop only certain packets.

b) Denial of Service Attack: The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevent legitimate network users from accessing services or resources to which they are entitled. At physical layer the DoS attacks could be jamming and tempering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanism to prevent the DoS attacks includes payment for network resources, pushback, strong authentication and identification of traffic.

c) Physical Attack: Physical attacks destroy sensors permanently, so the losses are irreversible. For instance attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors or replace them with malicious sensors under the control of the attacker.

d) Message Corruption: Any modification of the content of a message by an attacker compromises its integrity.

e) False Node: A false node involves the addition of nodes by an adversary and causes the injection of malicious data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious can injected in the network could spread to all nodes, potentially destroying the whole network.

f) Node Replication Attack: An attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance, packet can be corrupted or even misrouted.

g) Node Subversion: Capture of a node may reveal its information including disclosure of cryptographic keys & thus compromise the whole sensor network.

h) Node Malfunction: A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it a data aggregating node such as a cluster leader.

i) Node Outage: Node outage is the situation that occur when a node stop its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outage by proving an alternate route.

B. Passive Attacks:

The monitoring and listening of communication channel by unauthorized attacks are known as passive attacks. The most popular types of attacks are:

a) The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor network could probably collected through direct site surveillance. Hence, adversaries need not be physical present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks against sensor privacy are:

- Monitor and Eavesdropping: This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contain potentially more detailed information than

accessible through the location server, the eavesdropping can act effectively against the privacy protection.

- Traffic Analysis: Even when the messages transferred are encrypted, it still leaves a high possibilities 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 compromise the node 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.

Security Mechanism in WSN

The security mechanisms are actually used to detect, prevent and recover from the security attacks. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high-level and low-level.

a) Low-level security mechanism primitive for security sensor network include:
   - Key Establishment and trust setup: one important of sensor network security is programmable and controlled group communication. The primary requirement of setting up the sensor network is the establishment of cryptographic keys. Key-establishment technique to scale the network with hundreds of nodes.
   - Secrecy and Authentication: Most of the sensor network applications require protection against eavesdropping, injection and modification of packets. Cryptography is the standard defense. The earlier sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network cryptographic approaches.
   - Secure routing or data forwarding is a critical service for enabling communication in sensor networks. Unfortunately, current routing protocol suffers from many security vulnerabilities.
   - Privacy: Like other traditional network, the sensor networks have also force privacy concerns. Initially the sensor networks are deploying for legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is particularly important.

b) High-level security mechanism for securing sensor networks includes secure group management, intrusion detection and secures data aggregation.
   - Secure Group Management: Each and every node in a wireless sensor network is limited in its computing and communication capabilities. However, interesting in-

network data aggregation and analysis can be performed by groups of nodes. Secure protocol fro group management is required, securely admitting new group members and supporting secure group communication.

- Intrusion Detection: WSNs are susceptible to many forms of intrusion. Wireless sensor network require a solution that is fully distributed and memory requirements. The use of secure groups may be a promising approach for decentralized intrusion detection.
- Secure Data Aggregation: One advantage of wsn is the fine-grain sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amount of traffic back to the base station.

Challenges of sensor networks

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. A wsn is a special network which has many constraint compared to a traditional computer network.

a) Wireless Medium: The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones.

b) Ad-Hoc Deployment: The ad-hoc nature of sensor network means no structure can be statically defined. The network topology is always subject to change due to node failure, addition or mobility. Nodes may be deployed by airdrop, so nothing os known of the topology prior to deployment.

c) Hostile Environment: The next challenging factor is the hostile environment in which sensor nodes function notes the possibility of destruction or capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical access to the device.

Summary of various security schemes for wireless sensor networks

Security Schemes	Attacks Deterred	Network Architecture	Major Features
JAM	Hello Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based	Hello Attack (Jamming)	Hybrid (mainly wireless partly wired) sensor network	Uses wormholes to avoid jamming
Statistical En-Route Filtering	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution etc.	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting sybil entity
Bidirectional Verification, Multi-path multi-base station routing	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security	Information or Data Spoofing	Traditional wireless sensor network	Efficient resource management, Protects the network even if par: of the network is compromised
TIK	Wormhole Attack, Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Predistribution [28]	Data and information spoofing, Attacks in information in Transit, Data and Information Spoofing	Traditional wireless sensor network, Distributed Sensor Network, Large-scale wireless sensor network with dynamic	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes, Suitable for large wireless sensor networks which allows addition and deletion of sensors, Resilient to sensor node capture
REWARD	Blackhole attacks	Traditional wireless sensor network	Uses geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect blackhole attacks
TinySec	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP &//TESLA	Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

Conclusion

Wireless sensor networks are increasingly being used in military, environment, health and commercial applications. Sensor networks inherently different from traditional wired network as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarized the attacks and their classifications in wireless sensor networks. And also an attempt has been made to explore the security mechanism widely used to handle those attacks. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. The challenges of wireless sensor network are also briefly discussed.

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

[15] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004

[16] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003

[17] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[18]John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhaiy, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5,10-15, year 2006

[19]Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006

[20]Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009

[21]Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002 http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf

[22]Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 - 40, year 2006

[23]Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2,page(s): 52-62, year 2009

[24]Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6,

June 2004, pp. 30-33.

[25]D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile ad hoc and Sensor Networks," *IEEE Commun. Surveys Tutorials,* vol. 7, pp. 2-28, year 2005.

[26]S. Schmidt, H. Krahn, S. Fischer, and D. Watjen, "A Security Architecture for Mobile Wireless Sensor Networks," in *Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS),* 2004.

[27] G. Padmavathi, D. Shanmugapriya, "*A Survey of Attacks, Security Mechanisms and Challenges in WSNs*", IJCSIS, Vol.4, No. 1 &2, 2009.

[28] Eschenaur, L. and Gligor, V.D., "*A Key-Management Scheme for distributed sensor network*", Proc. ACM CCS'02,18-22 November 2002, pp. 41-47.