International Journal of Engineering, Science and Metallurgy

(General article)

Security Threats in Wireless Sensor Networks: A Comprehensive Overview

Mukesh Chawla[a*], Kamlesh Dutta[a], Navneet Verma[b]

[a]Department of CSE, NIT Hamirpur,[b]Department of CSE , MMU, Mullana

Accepted 9 July 2012, Available online 1Sept 2012

Abstract

Wireless sensor networks are an emerging technology for low-cost, unattended monitoring of a wide range of environments. Their importance has been enforced by the recent delivery of the IEEE 802.15.4 standard for the physical and MAC layers. Resource limitations in the Wireless Sensor networks prevent us to directly apply the security mechanism of normal computer networks, a completely different set of security protocols exist for the sensor networks. This paper identifies the vulnerabilities associated with the operational paradigms currently employed by Wireless Sensor Network. A Survey of current WSN security research is presented. A framework for implementing Security in WSNs, which identifies the security measures necessary to mitigate the identified vulnerabilities, is defined.

Keywords: Sensor, Security, Attack, Wireless, WSN,Research Area, Countermeasures

1. Introduction

Wireless Sensor Network is a heterogeneous system, made of tiny inexpensive sensors, actuators and general purpose computing elements. Sensors are scattered over a specific geographical area, which are capable of sensing changes in parameters such as temperature, pressure, humidity and noise level [1] of surrounding environment. They communicates with other devices over a specific area using transceiver and send sensed information to a central location, so that central processing can be performed on it to achieve desired functionality such as environment monitoring, providing security at home or in public place. The most efficient model for WSN is cluster based hierarchical model. WSN is like ad-hoc network, so it is also called "ad-hoc wireless sensor network". Potential applications includes monitoring factory environment such as instrumentation, pollution level, fire alerts, free way traffic, climate monitoring and control[2],medical monitoring and emergency response [3], monitoring remote or inhospitable habitats [4, 5], target tracking in battlefields [6] .The desired features of WSN are security, reliability, robustness, self-healing and scalability. So this kind of network has four properties combined together [7]:

1. Sensors: Nodes can sense/capture information from the network
2. Ad hoc: network is established on need base
3. Mobile: Nodes are not located on fixed locations
4. Wireless: nodes can communicate wirelessly

2. Obstacles to wsn security

The following section list the limitations in sensor networks which make the design more complicated.

A. Node limitations

A typical sensor node processor is of 4-8 MHz, having 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency. Heterogeneous nature of sensor nodes is an additional limitation which prevents one security solution.

B. Network limitations

Beside node limitations, sensor networks bring all the limitations of a mobile ad hoc network where they lack physical infrastructure, and they rely on insecure wireless media.

C. Physical limitations

Sensor networks deployment nature in public and hostile environments in many applications makes them highly vulnerable to capture and vandalism. Physically security of sensor nodes with tamper proof material increases the node cost.

D. Memory limitations

*Corresponding author's email: Mukeshk.chawla@gmail.com

In wireless sensor network, nodes have limited memory capability, having 4KB of RAM, 128KB flash.

E. Computational limitations

Due to limited power supply to the sensor nodes, complex computational algorithms that are used on normal computers may not be directly applicable to the WSN.

3. Characterstics of WSN

Sensor networks are emerging technologies currently being deployed in seismic monitoring, wild life studies, manufacturing and performance monitoring. A typical sensor network contains large number of densely deployed, tiny, low cost nodes that use wireless peer-to-peer network. These sensor nodes are densely deployed in a predetermined geographical area to self-organize into ad-hoc wireless networks to gather and aggregate data [19]. They use multi-hop and cluster based routing algorithms and resources algorithms based on dynamic network topology [20]. The characteristics of WSN are wireless medium, ability to withstand harsh environmental conditions, ability to cope with node failures, communication failures, heterogeneity of nodes, large scale of deployment, unattended operation, low power consumption, low cost and low data rate. Other characteristics of WSN are as follows:

A. Large scale of Deployment

Sensor nodes may be placed at specific locations or be placed randomly. After the initial deployment, sensors may be added or replaced, which affects node location, density, and the overall topology.

B. Mobility of nodes

Mobility is a desired property of the system to move nodes to interesting physical locations. Mobility may apply to all nodes within a network or only to a subset of nodes. It has a large impact on the degree of network dynamics and hence influences the design of networking protocols and distributed algorithms.

C. Infrastructure

The various communication models can be used to construct a wireless sensor network. Two common communication models are infrastructure based networks and ad hoc networks. In infrastructure based networks, Sensor nodes can only communicate directly with base stations. The number of base stations depends on the communication range and the area covered by the sensor nodes. In ad hoc networks, nodes can communicate directly with each other without an infrastructure.

D. Dynamic Network Topology

One important property of a WSN is its diameter, that is, the maximum number of hops between any two nodes in the network. In its simplest form, a WSN forms a fully connected topology, in which every sensor node being able to communicate directly with every other node. An infrastructure based network with a single base station forms a star network with a diameter of two. A multi-hop network may form an arbitrary graph. The topology affects many network characteristics such as latency, robustness, and capacity.

E. Connectivity

The physical locations of individual sensor nodes define the connectivity of a network. If there is always a direct connection between any two nodes, the network is said to be connected. If nodes are isolated most of the time and enter the communication range of other nodes only occasionally, we say that communication is sporadic. Connectivity influences the design of communication protocols.

F. Lifetime

Depending on the application, the required lifetime of a sensor network may range from a few hours to several years. The lifetime has a high impact on the required degree of energy efficiency and robustness of the nodes and required the minimum energy expenditure.

G. Data Aggregation

Data aggregation is the task of data summarization while data are traveling through the sensor network. An excessive number of sensor nodes can easily congest the network, flooding it with information. The solution to this problem is to aggregate data within the WSN then transmits an aggregate of the data to the controller. There are three major ways of performing data aggregation: First, diffusion algorithms assume that data are transmitted from one node to the next, thus propagating through the network to the destination. Second, streaming queries are based on SQL extensions for continuous querying. Third, event graphs work on streams of events and compose simple events into composite events based on event algebra.

I. Self-Configuration

When there is a large number of nodes and scattered in a large geographical area, then it is essential that the network be able to self-organize. Moreover, nodes may fail from limitation of energy, from physical destruction or any other means and new nodes may need to join the

network. Nodes will have to self-configure to establish a topology that provides communication under stringent energy constraints. The network must be able to continuously and periodically

4. Principles of security

A. Confidentiality

Confidentiality is the ability to conceal messages from a passive attacker, so that any message communicated via the sensor network remains confidential. It means keeping information secret from unauthorized access. A sensor network should not leak the sensed data to its neighboring network. In many applications, communicating nodes shares the secret data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that is known only to sender and intended receiver, Hence achieving confidentiality. Symmetric key encryption method is most popularly used method in WSN, because public-key cryptography is too expensive to be used in the resource constrained sensor networks. Establishing and maintaining confidentiality is extremely important when keys are being distributed to establish a secure communication channel among sensor nodes [10].

B. Authentication

Authentication establishes proof of identities. It assures the recipient that the message is from the source that it claim to be from. Authentication prevents unauthorized parties from participating in network and recipient should be able to detect that these messages from adversary and reject them. In two party communications, authentication can be achieved through symmetric key encryption. Sender and Receiver share the secret key to encrypt the data and to compute MAC. When a message is received, the receiver re computes the MAC, if both MAC are matched; the receiver knows that it must have been sent by the sender. It can be achieved through synchronous and asynchronous mechanism where sending and receiving nodes share the secret key to compute the MAC.

In broadcast communication, the creators of SPINS [8] contend that if one sender wants to send data to mutually entrusted receivers, symmetric MAC is insecure since any one of the receivers know the MAC key, and hence could impersonate the sender and forge messages to other receivers. In SPINS asymmetric key encryption method and one way function is used for authentication. LEAP [9] uses a globally shared symmetric key for broadcast messages to the whole group. However, since the key is shared among all the nodes in the network, an efficient rekeying mechanism is defined for changing the key after a compromised node is revoked. This means that LEAP has also defined an efficient mechanism to verify whether a node has been compromised.

C. Data Integrity

Data integrity ensures that a message has not been changed while on the network. It ensures the reliability of data. Data Authentication also can provide Data Integrity. There is still a possibility that the data's integrity has been compromised by alterations. It can be compromised if

 A malicious node present in the network injects bogus data.Turbulent conditions due to wireless channel cause damage or loss of data.

Data freshness

Data freshness ensures that data is up to date and adversary has not replayed old message.(used by SPIN[8])A monotonically increasing counter is used with each message. Recipient must maintains a table of last value of received message and should reject the message with old counter value.WSN is a RAM constrained sensor network, where memory allocation for neighbor table becomes problematic for even modestly sized networks due to small memory size. Assumes that nodes of WSN allocates only a small fraction of their RAM for this neighbor table, an adversary by sending broadcast messages from different senders can fill up the table. At this point, the recipient has one of two options:

 Ignore any messages from senders not in its neighbor table,
 Purge entries from the table.

E. Availability

Availability ensures that resources or network should be available to authorized parties at all times for the communication[10].However, unavailability of resources such as failure of base stations,nodes,acutator and computing elements will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network [10].

F. Access Control

Access control determines "Who should be able to access what". it is the ability to limit and control the access to network via communications links. Each user trying to gain access to network must first be identified and authenticated so that only authorized user can gain access to network. in[10],Access control is broadly related to two areas:

Role management

Role management concentrates on user side and determines which user can do what, whereas Role management focuses on the resources and determines which resource is accessible and under what circumstances.

G. Non-Repudiation

Non-Repudiation ensures that no one can deny the transmitted message. It means when a message is received, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

5. Types of attacks

There are two types of attacks [1].

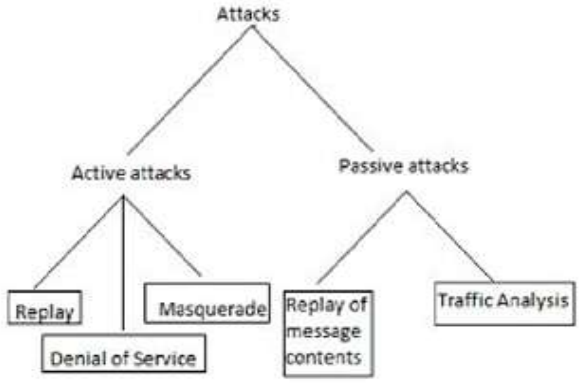

Figure 1: Attack model

 Active Attacks

An active attempts to alter the contents and affects the system operation. e.g. masquerade, ,replay, ,message modification and DoS[11].

 Passive Attacks

A passive attack accesses the information and uses it, but does not alter the contents and affects the system operation. E.g. release of message contents, traffic analysis [11].

6. Key research areas in WSN

We identified the two key research areas Routing & Transport" and "In-network Processing" for developing secure and reliable WSNs.

Routing & Transport

- Key pre-distribution
- Pair wise/group wise authentication
- Access Control
- Routing

In-network Processing

- Data aggregation
- Distributed data storage
- Data plausibility

Table1Threats and Countermeasures

Threats	Countermeasures
Wormhole[22]	Physical monitoring of Field devices and
	regular monitoring of network using
	Source Routing. Monitoring system may
	use Packet Leach techniques.
Selective forwarding[22]	Regular network monitoring using Source
	Routing
DoS[25]	Protection of network specific data like
	Network ID etc. Physical protection and
	inspection of network
Sybil[21]	Resetting of devices and changing of
	session keys
false routing information	authenticated broadcast [22]
Traffic Analysis[26]	Sending of dummy packet in quite hours

7. Security threats and Countermeasures in routing and Transport

We describe various security threats and corresponding countermeasures in case of routing and transport in table 1.

8. Security threats andCountermeasures for in – network Processsing

We describe various security threats and corresponding countermeasures in case of routing and transport in table 2.

Table 2Threats and Countermeasures

Security Threats	Countermeasures
eavesdropping	link layer encryption [22, 23]
modification	link layer authentication [22, 23]
Node replication	Asymmetric key encryption[24]
DoS	prohibit network broadcast from
	sensor nodes[25]
Node Compromise	Public key cryptography [25]
Sybil Attack[21]	Resetting of devices and changing
	of session keys

9. Conclusion

In this paper, we have addressed the issue securing a wireless sensor network against a variety of threats that can lead to the failure of the base station, threats to routing and transport and In network processing. Although most of the threats have been addressed by Researchers much deeply, but a need exists to combine all these separate efforts to develop a unique light weight and Powerful protocol to address the issues cumulatively.. We described security and reliability challenges for WSNs. We analyze the key research areas with the goal of developing a modular toolbox to support an integrated security and reliability architecture for medium and large-scale WSNs.

References

1. Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using *Wireless Ad Hoc and Sensor Networks*", to appear in IEEE ICNEWS 2006.
2. Haowen Chan, and Adrian Perrig, *"Security and Privacy in Sensor Networks"* Carnegie Mellon University pp. 99-101.
3. Matt Welsh, Dan Myung, Mark Gaynor, and Steve Moulton.Resuscitation monitoring with a *wireless sensor network.* In Supplement to Circulation: Journal of the American Heart Association, October 2003.
4. Alan Mainwaring, Joseph Polastre,Robert Szewczyk, and David Culler. Wireless sensor networks for habitat monitoring. In First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
5. Robert Szewczyk, Joseph Polastre, Alan Mainwaring, and David Culler. Lessons from a *sensor network expedition.* In First European Workshop on Wireless Sensor Networks(EWSN'04), January 2004.
6. G.L. Duckworth, D.C. Gilbert, and J.E. Barger. Acoustic counter-sniper system. In SPIE International12 symposium on Enabling Technologies for Law Enforcement and Security,1996.
7. Y. W. Law, S. Dulman, S. Etalle, P. Havinga, "*Assessing security-critical energy efficient sensor networks"*University of Twente, EA Enshede,Netherlands.[2] Adria
8. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. SPINS: *Security Protocols for Sensor Networks*. In The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001), 2001.
9. Alan Mainwaring, Joseph Polastre, Robert Szewczyk, and David Culler.Wireless sensor networks for habitat monitoring. In First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
10. Atul Kahate.*Cryptography and Network Security*, 2E by McGrew-Hill.
11. William Stalling *Cryptography and Network Security*, 4E , Pearson education, Inc. and dorling Kindersley publishing Inc. for network security.
12. Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.
13. Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.
14. Douceur, J. "The Sybil Attack", 1st International Workshop on *Peer-to-Peer Systems* (2002).
15. 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.
16. S. Madden, R. Szewczyk, M. Franklin, and D. Culler. Supporting Aggregate Queries over *Ad-Hoc Wireless Sensor Networks*. In 4th IEEE Workshop on Mobile Computing Systems And Applications, June 2002
17. Karlof, C. and Wagner, D., "*Secure routing in wireless sensor networks*: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September2003, pp. 293-315.
18. Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes*: a defense against wormhole attacks in wireless Networks"*, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies.IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.
19. N. Hu, Randy R. K. Smith and P. G. Bradford, Security for Fixed Sensor Networks, Proceedings of the 42nd Annual Southeast regional conference, ACM Press, 2004, NY, USA20.
20. R. Anderson, H. Chan, and A. Perrig, Key infection: smart trust for smart dust, 12th IEEE International Conference on Network Protocols. Oct 5-8 2004, Berlin, Germany.

21. Girao, D. Westhoff, E. Mykletun, T. Araki, "TinyPEDS: Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks,"currently under review.
22. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. 1st IEEE Int'l. Wksp. Sensor Network Protocols and Applications (SNPA'03),May 2003
23. A.Perrig *et al., "SPINS: Security Protocols for Sensor Networks," ACM Wireless Networks, vol. 8, no. 5, Sept. 2002, pp.* 521–34.
24. Deng, R. Han, and S. Mishra, "A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks," *Proc. 2nd IEEE Int'l. Wksp. Info. Processing in Sensor Networks (IPSN'03), Palo Alto, CA, Apr. 2003*
25. Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.
26. S. Sharma, "Energy-efficient Secure Routing in Wireless Sensor Networks", Dept of Computer Science and Engineering, National Institute of Technology , Rourkela, Orissa, 769 008,India, 2009