www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 2 Feb. 2017, Page No. 20289-20292
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i2.24

Security protocols for Wireless Sensor Networks

P. Udaya Sri[1], S. Sravani[2], G. Priyanka[3]

[1]Dept. Of CSE,
SVU College Of Engineering, Tirupati, India.
udayasripaidala@gmail.com

[2]Dept. Of CSE,
SVU College Of Engineering, Tirupati, India.
ssravani1012@gmail.com

[3]Dept. Of CSE,
SVU College Of Engineering, Tirupati, India.
gudivadapriyanka@gmail.com

Abstract: **Wireless sensor networks(WSNs) are consisting of multifunction sensor nodes that are small in size and communicate wirelessly over short distances. Sensor nodes incorporate properties for sensing the environment, data processing and communication with other sensors. The unique properties of WSNs increase flexibility and reduce user involvement in operational tasks such as in battlefields. WSNs present unique and different challenges compared to traditional networks. In particular, wireless sensor nodes are battery operated, often having limited energy and bandwidth available for communications. Continuous growth in the use of WSNs in sensitive applications, it becomes a requirement to provide security in WSNs. Achieving security in resource constrained WSNs is a challenging research task.**

In this paper, we outline what is WSN, need for security in WSN, security issues, possible attacks in WSNs, security requirements in WSN and finally security protocols used in WSN and how they are achieved security requirements.

Keywords : data confidentiality, data authentication, data integrity, data freshness, SNEP, µTESLA

1. Introduction

Wireless sensor networks are composed of multiple detection stations called sensor nodes and a base station. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interfaces. It can be used as a connection to disseminate control information into the network or extract data from it. A base station is also referred to as a sink. Sinks are often many orders of magnitude more powerful than sensor nodes. Every sensor node in network is small, light weight and portable and is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a base station and transmits data to that base station. The power for each sensor node is derived from a battery. They are used for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

Security is sometimes viewed as a standalone component of a system’s architecture, where a separate module provides security[3]. This separation is, however, usually a flawed approach to network security. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack.

2. SECURITY ISSUES

Small sensor devices are inexpensive, low-power devices. They have limited computational and communicational resources. The energy source on the devices is a small battery. Communication over radio is the most energy-consuming function performed by these devices, so the communications overhead needs to be minimized. The limited energy supplies create limits for security. Hence security needs to limit consumption of processor power. However, limited power supply limits the life time of keys. These constraints make it impossible to use secure algorithms designed for powerful workstations[6][8].For example, the working memory of a sensor node is insufficient even to hold the variables that are required in cryptographic occur, or dropped at highly congested nodes in the network. Further, Wireless sensor networks have another vulnerable algorithms.

Another security issue in WSN is Unreliable Communication. Due to the wireless medium that is inherently broadcast in nature, packets may get damaged due to channel errors and conflict will to security attacks because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

3. POSSIBLE ATTACKS

Wireless networks are usually more vulnerable to various security threats as they are located in different geographical locations to monitor critical conditions.An attacker in WSN can be categorized based on the following characteristics:goals,performer and layer wise.

Goal oriented attacks are classified into two types:Passive attacks and Active attacks[10]. Passive attacks include traffic analysis, monitoring communications, decrypting weakly encrypted traffic, and capturing authentication information.Denial of service attack(DoS), modification of data, black hole, replay, sinkhole, spoofing, flooding, jamming, overwhelm, wormhole, fabrication, Hello flood, node subversion, lack of cooperation, modification, node subversion, man-in-middle attack, selective forwarding and false node comes under Active attacks.

Performer oriented attacks are classified into outside attacks and inside attacks [10]. The outsider attacks are attacks from nodes which do not belong to a WSN. An outsider attacker has no access to most cryptographic materials in sensor network. The insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. Inside attackers can launch various types of attacks, such as modification, misrouting, eavesdropping or packet drop.

WSNs are organized in layered form[11]. This layered architecture makes WSNs vulnerable to various kinds of attacks. For example,Physical layer attacks on WSNs range from node capturing to the jamming of the radio channel.All other layers are also vulnerable to attacks as physical layer.

Here,we describe some of the above mentioned possible attacks on WSNs.

- *Denial of Service*

Denial of Service is produced by the unintentional failure of nodes or malicious action. In the denial-of-Service (DoS) attack, the hacker's objective is to render target machines inaccessible by legitimate users.Dos attacks can happen in multiple WSN protocols layers. At physical layer, the DoS attack could be jamming and tempering, at link layer, collision, exhaustion, unfairness etc; Payment for network resources, pushback, strong authentication and identification of traffic techniques are used to prevent DoS attacks in WSNs.

- *Attacks on information transit*

This is the most common attach in WSNs.Information in transit is vulnerable to eavesdropping, modification, injection.This attack can be prevented using well established confidentiality, authentication, integrity and replay protection protocols.

- *Node capture attacks*

In this attack,an adversary gains full control over a sensor node through direct physical access.The adversary can then easily get cryptographic primitives and obtain unlimited access to the information stored on the node'smemory chip,with the potential to cause substantial damage to the entire system.Many researchers have proposed different key management schemes for secure communication between sensor nodes. These schemes try to prevent node capture attacks.

- *Routing attacks*

There are a number of attacks that target the routing protocol of WSNs, all of which are necessarily insider attacks.Every node acts as a router in a WSN. Routing and data forwarding are an important task for sensor nodes. Routing protocols have to be energy and memory efficient, but at the same time they have to be robust against attacks and node failures. Selective forwarding, Sinkhole attack, Sybil attack, Wormhole attack, Flooding are comes under routing attacks.

In selective forwarding attack, malicious nodes simply drop certain messages instead of forwarding every message. Malicious nodes can refuse to route certain messages and drop them. If they forward all packets through malicious node then it is black hole attack. If selectively forward the packets,then it is selective forwarding. In sinkhole attacks,malicious node is placed where it can attract most of the traffic,possibly closer to base station. In Sybil attack, a single node presents multiple identities to all other nodes in the WSN. This may mislead other nodes, and hence routes believed to be disjoint w.r.t node can have the same adversary node. In wormhole attacks, an adversary positioned closer to the base station can completely disrupt the traffic by tunneling messages over a low latency link. Sometime, the malicious node can cause immense traffic of useless messages on the network. This is known as the flooding.

4. SECURITY REQUIREMENTS IN WSN

Security requirements in WSN to ensure trustworthy and secure connections and communications are a combination of the specifications for computer network and wireless communication security.

4.1.*Data Confidentiality*

WSN uses multi hop routing.Data is communicated between the sender and the recipient, sometimes being routed through many nodes. This data may also be kept in memory for further processing. This data can be sensitive enough to be known only by the sender and the recipient. Sometimes, the adversary can access this information by eavesdropping between wireless links, gaining admission to the storage or by other attacks. Data confidentiality means that the data can only be accessed, and thus utilized, by only those entities that are authorized for this purpose.

Encryption is one of the most commonly used procedures to provide confidentiality of data.Secure communication channels between different nodes and between nodes and base station can make sure data confidentiality in WSNs.

4.2.*Data Integrity*

Data integrity ensures the receiver that the received data is not altered in transmit by an adversary. Data integrity can be provided by Message Authentication Code (MAC). For this purpose, both sender and receiver share a secret key.When a message with a correct MAC arrives,the receiver knows that it must have been originated by the sender.

4.3.*Data authentication*

Data authentication allows a receiver to verify that the data really was sent by the claimed sender. It is particularly important in case of decision making chunks of information. Nodes receiving the packets must make sure that the originator of packets is an accredited source. Nodes taking part in the communication must be capable of recognizing and rejecting the information from illegitimate nodes. Multi-party communications or broadcasting makes use of asymmetric authentication schemes to provide data or message authentication.

4.4.*Data freshness*

In WSNs,we must ensure that each message is fresh.Sensors send data periodically to the base station. Confidentiality and Authentication may not be useful when any old message is replayed by any attacker.Data freshness implies that the received messages are recent and previous messages are not replayed.There are two types of freshness.Weak freshness,which provides partial message ordering, but carries no delay information,and Strong freshness,which provides total order on a request-response pair, and allows for delay estimation.

4.5.*Data Availability*

Insertion of security can cause earlier depletion of energy and storage resources, causing unavailability of data. Similarly, if security of any one node is compromised or any Denial of Service (DoS) attack is launched, data becomes inaccessible. Availability of data becomes an important security requirement.

5. SECURITY PROTOCOLS IN WSN

Security requirements are achieved by using two security building blocks.Secure Network Encryption Protocol(SNEP) and micro version of the Timed,Efficient,Streaming,Loss-tolerant Authentication protocol(µTESLA).SNEP provides data confidentiality,data authentication,integrity, and freshness. µTESLA provides authentication for data broadcast.

5.1.*SNEP*

SNEP has low communication overhead since it only adds bytes per message.SNEP,like many cryptographic protocols,uses a counter,but transmitting the counter value is avoided by keeping state at both end points.SNEP achieves semantic security,a strong security property that prevents eaves-droppers from inferring the message content from the encrypted message using randomization.A basic technique for achieving this randomization is before encrypting message with a chaining encryption function,the sender precedes the message with a random bit string.A simple form of confidentiality can be achieved through encryption.To achieve two-party authentication and data integrity a message authentication code(MAC) is used.The combination of these mechanisms forms protocol SNEP.

The encrypted data has following format:$E=\{D\}_{(Ke,C)}$,where D is data,the encryption key is K_e,and counter is C.The MAC is $M=MAC(K_{mac},C|E)$ .The complete message that A sends to B is:

A to B:$\{D\}_{(Ke,C)}$, $MAC(K_{mac},C|\{D\}_{(Ke,C)})$

But this method provides weak freshness.To achieve strong freshness by including random number.

A to B:N_A,R_A where N_A is random number and R_A is request message from node A.

B to A:$\{R_B\}_{(Ke,C)}$,$MAC(K_{mac,}N_A|C|\{R_B\}_{(Ke,C)})$

5.2. *µTESLA*

µTESLA protocol provide efficient authenticated broadcast.It requires that the base station and nodes are loosely time synchronized.To send an authenticated packet,the base station simply computes MAC on the packet with a key that is secret at that point of time.When a node gets a packet ,it can verify that the corresponding MAC key has not yet been disclosed by the base station.The node stores the packet in buffer,and at the time of key disclosure,the base station broadcasts the verification key to all receivers.Each MAC key is one in a key chain,generated by a public one-way function F.To generate the one-way key chain,the sender chooses the last K_n of the chain randomly,and repeatedly applies F to compute all other keys.$K_i=F(K_{i+1})$.

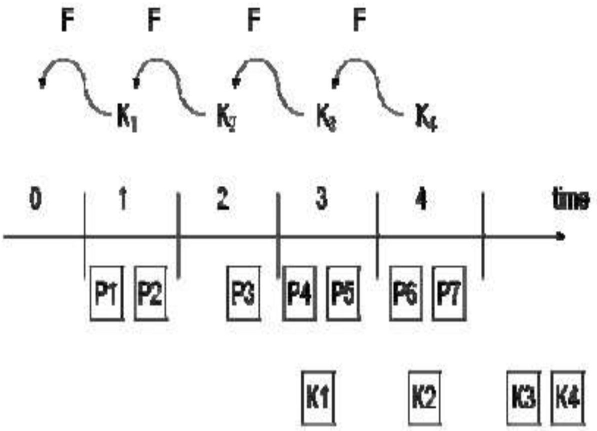

Fig 1:oneway function for µTESLA

µTESLA has multiple phases:sender set-up,sending authenticated packets,bootstrapping new receivers,and authenticating packets.During sender set-up,the sender first generates a sequence of secret keys.During broadcasting authenticated packets,the time is divided into interval and sender associates each key of the one-way chain with one interval time.In time interval t,the sender uses key of the current interval,K_t to compute MAC.The sender will then reveal the key K_t after a delay of δ intervals after the end of the time interval t.During bootstrapping,each receiver needs to have one authentic key of one-way chain.Both loose time synchronization,as well as the authenticated key chain commitment,can establish a mechanism that provides strong freshness and point-to-point authentication.During authenticating broadcast packets,the receiver needs to know the key disclosure schedule.

6. CONCLUSION

The wireless sensor networks continue to grow and become widely used in many mission-critical applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, as well as unreliable communication and unattended operation.In this article,we discussedabout WSNs, security issues involved in designing WSNs, attacks that are prone to WSNs, and security requirements for designing security protocols. SNEP and µTESLA are two protocols used to provide security in WSNs.

REFERENCES

1. Eschenauer, L. and Gligor, V. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communication Security (Washington, D.C., Nov.). ACM Press, New York, 2002, 41–47.
2. Karlof, C. and Wagner, D. Secure routing in wireless sensor networks:Attacks and countermeasures. In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (Anchorage, AK,May 11, 2003).
3. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. SPINS:Security protocols for sensor networks. J. Wireless Nets. 8, 5 (Sept. 2002),521–534.
4. I.F.Akyildiz et al., “A Survey on Sensor Networks”, IEEE Commun.Mag.,Vol. 40, No. 8, pp.102-114, Aug. 2002.
5. Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication of the ACM, Vol. 47, No. 6, pp. 30-33, Jun. 2004.

DOI: 10.18535/ijecs/v6i2.24

6. E.Shi and A.Perrig, "Designing Secure Sensor Networks", Wireless Commun. Mag., Vol. 11, No. 6, pp.38-43, Dec 2004.
7. H. Chan and A. Perrig, "Security and Privacy in Sensor Networks,"Computer, vol. 36,no. 10, Oct. 2003, pp. 103–05.
8. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy, page 197. IEEE Computer Society, 2003.
9. M. Gruteser, G. Schelle, A. Jain, R. Han, D. Grunwald:Privacy-Aware Location Sensor Networks,9th Conference on Hot Topics in Operating Systems2003 (2003) pp. 28–28.
10. RituSharma,Yogeshchaba and Yudhvirsingh "Analysis of Security Protocols in Wireless Sensor Network"Int. J. Advanced Networking and Applications Volume: 02, Issue: 03, Pages: 707-713 (2010).
11. Undercoffer, J., Avancha, S., Joshi A., and Pinkston J., "Security for Sensor Networks", CADIP Research Symposium, 2002, availableat, http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf 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 1,27-30May,2005,