Security Protocols for Wireless Sensor Networks

Monika Bhalla
Amity School of Engineering and Technology
Amity University, Noida(U.P.)
mbhalla2@amity.edu

Nitin Pandey
Amity Institute of Information Technology
Amity University, Noida(U.P.)
npandey@amity.edu

Brijesh Kumar
Lingaya's GVKS Institute of Management and Technology,Faridabad,
director@lgimt.org

Abstract. As Sensor networks are being used in remote environment monitoring, healthcare, machine automation, security of these networks is becoming a central concern. Till now main concern was to make sensor networks useful and deployable and little emphasis was placed on security. This paper analyses security issues and vulnerabilities in wireless sensor networks. The paper gives an overview of various security protocols used for wireless sensor networks and finally a comparison is done for the various security protocols available.

***Keywords*—— Sensor networks, Attacks , Security Protocols , Sensor nodes, security issues**

1. Introduction to WSN

Wireless Sensor Networks are a collection of thousands of sensor nodes that are self-organized and are capable of wireless communication. But these nodes are constrained in terms of size, energy, memory, processing power .These nodes sense environmental data, perform limited processing and communicate over short distances. As the applications of wireless sensor networks are continuously growing also the need for security mechanisms is increasing day by day. Wireless Sensor Networks may interact with sensitive data or usually these networks operate in hostile, unattended environments, it is necessary to address these security concerns. Security challenges of sensor networks are different from traditional networks due to many constraints of these networks.

1.1 CONSTRAINTS IN WIRELESS SENSOR NETWORKS

Resource Constraints: Sensor nodes have limited resources like small memory, limited computational capability, limited battery power and since these nodes are deployed in unattended environments so battery can't be replaced or recharged easily.

Local Addressing Schemes: Because nodes are large in numbers so it is impossible to implement a global addressing scheme.

Message size is small: In wireless sensor networks messages are small in size compared with existing networks.

Security Constraints: Sensor networks operate in hostile environment rather than traditional networks that are properly structured and are easy to secure.

Redundant data collection: Each sensor node collects data based on its location so there is high probability to collect redundant data.

1.2 SECURITY REQUIREMENTS

The main security requirements that each WSN has to fulfil are as follows:

Availability: WSN services should always be available in spite of all the resource depletion attacks that may occur on the system. So our network should be resistant to such attacks.

Confidentiality: Secrecy of message transmitted between nodes should be maintained properly. For that important segments of message should be encrypted. In some cases even the two end points

978-1-4673-7910-6/15/$31.00 ©2015 IEEE

are also hidden. In some dynamic systems where nodes keep on joining and leaving the network, *forward* and *backward secrecy* needs to be maintained. *Forward Secrecy* means that nodes leaving the network may not be able to access future transmissions on the network after leaving the network and *Backward Secrecy* means that new nodes may not be able to access past transmissions before their joining the network. These phenomenon are needed to maintain confidentiality of data in wireless sensor networks.

Integrity: Attackers should not be able to change the data in Wireless sensor networks. If somehow attacker succeeds in doing so then network should be able to detect those alterations.

Authenticity: Before transmitting any message the identity of sender must always be verified so that no intruder may be able to forge wrong data into the network.

Non-Repudiation: Neither the sender nor the receiver should be able to deny that the message is sent by him. For that message can be digitally signed by both the sender and the receiver.

2. ATTACKS ON WIRELESS SENSOR NETWORKS

Since wireless sensor networks operate in unsafe environment these are vulnerable to several types of attacks

2.1 *Denial-of-Service Attack*

In Denial-of-Service attack the main aim of attacker is to make the system inaccessible to legitimate users. DoS attacks can occur in multiple protocol layers of WSN. At Physical Layer it could be in the form of jamming and tempering attack, At the data link layer the attack could be Collision, exhaustion and unfairness, At the network Layer DoS attack could be Black Hole, Hello Flood attack, at the transport Layer this attack can be performed by flooding attack.

2.2 *Attacks on Information during transmission*

The most dangerous attack in WSN are on information that is being transmitted between nodes because that information is susceptible to eavesdropping, injection, modification. Traffic analysis attack can also be performed because attacker may be able to get to know about the layout of the network and can damage the busiest portions of the network to perform greatest damage.

2.3 *Replicating a Node Attack*

The attacker may insert a new node into the sensor network which can be a clone to an pre-existing node. This new cloned node can transmit useful information to the attacker. This node replication attack is most dangerous when the cloned node is some base station. So base stations needs to be deployed in secure locations.

2.4 *Routing Attack*

The attacks that affect the routing protocol of wireless sensor network are as follows:

a. *Selective Forwarding*

In Selective Forwarding attack the malicious node may drop certain packets and transmit the rest. If it drops all the packets then it is a Black Hole attack. But if it forwards selective packets then is selective forwarding attack. The effectiveness of the attack depends on how close is the malicious node to the base station because then maximum traffic will go through it.

b. *Sinkhole Attacks*

Sinkhole Attack is to attract maximum traffic through malicious node which is placed somewhere near the base station. If the sensor network has one main base station then this attack can be very dangerous.

c. *Sybil attack*

In Sybil attack one node presents multiple identities in the network that may mislead nodes in the network. Sybil attacks can be used against topology maintenance and routing algorithms

d. *Wormhole Attack*

In Wormhole attack just like Sinkhole attack the attacker sitting closer to base station may tunnel the traffic to a low-latency link thus disrupting the traffic.

e. *Flooding*

The attacker may flood the network with useless messages to cause congestion on the network. It is a type of DoS attack which may lead to exhaustion of legitimate nodes.

3. SECURITY PROTOCOLS FOR WIRELESS SENSOR NETWORKS

Traditional security solutions cannot be applied to wireless sensor network because these are resource constrained networks. So a lot of research is going on to develop security protocols for these resource constrained networks. Most security protocols that exist today require a lot of computation for which large memory is required which is a major constraint of this network. In this section we present some of the most popular security solutions available for wireless sensor networks.

3.1 *SPINS* (Security Protocols for Wireless Sensor Networks) Adrian Perrig et al.[3] proposed a protocol called SPINS which is a suite of security protocols for sensor networks. SPINS consists of two main protocols- SNEP AND µTESLA . SNEP focuses on data confidentiality, two-party authentication of data and data freshness whereas µTESLA provides authenticated broadcast for severely resource constrained networks.

3.1.1 *SNEP(Sensor Network Encryption Protocol)*

Sensor Network Encryption Protocol uses shared counters. In SNEP, plain text block is encrypted with a counter using CTR encryption algorithm. The counter is not included in the message. The sender and the receiver update the shared counter after they have sent/received a cipher block. Each message has a MAC computed with CBC-MAC algorithm in the encrypted data. The MAC is computed once for each package. When receiver gets the message it computes the MAC for the message and compare it with the received MAC. If these two MAC matches the message is accepted otherwise rejected. SNEP has following advantages:

1. SNEP uses a shared counter so it need not to be transmitted with the message.
2. It adds only 8 bytes to a message.
3. It offers following kind of security to the data in transit.

Semantic Security: Since Sender/Receiver share the counter and increment it after each transfer of data , the same message may be encrypted differently every time. This is called Semantic security and the counter value is long enough not to be repeated during lifetime of a node.

Data Authentication: Since MAC is generated and sent with the message and the message is accepted only if generated MAC matches with the received MAC, the receiver is assured that message is authentic.

Replay Protection: Counter value in the MAC prevents an attacker from replaying old messages.

Weak Freshness: If the authentic message is received and accepted then the message can be ordered resulting in weak freshness.

Low communication overhead: The counter is shared between sender and receiver and is not sent with the message.

3.1.2 *µTESLA:* Authenticated broadcast requires asymmetric mechanism that has high computation, communication and storage overhead , so they cannot be used in a resource constrained sensor network. µTESLA overcomes this problem by introducing asymmetry through delayed disclosure of symmetric keys. In µTESLA protocol a node stores the packet in the buffer till the key is disclosed. The time when the key is disclosed , the base-station broadcasts verification key to all the receivers, which the node can use to authenticate the packet stored in its buffer. Each MAC key is a sequence of keys generated by one way function F. The sender chooses last key K_n and repeatedly applies F to compute the keys

$$K_i = F(K_{i+1})$$

3.2 *TINYSEC :* Karlof et al.[5] designed a protocol called TINYSEC. It provides all the services provided by SNEP like authentication , message integrity , confidentiality and replay protection . Major difference is that no counters are used in TINYSEC.

Two variants of TINYSEC are available i.e. TINYSEC-AE(authentication Encryption) and TINYSEC-Auth(Authentication Only)

Message Header of TINYSEC-AE

Message		Header

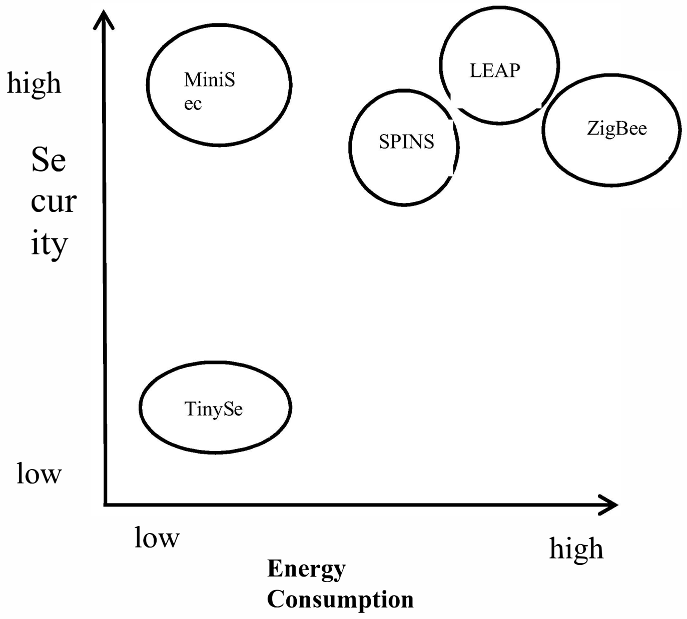
Message Header of TINYSEC-Auth

Message	Header	MAC

In both the cases data is authenticated with MAC maintaining Data Integrity.

3.3 *MiniSec:* MiniSec[4] is a secure network layer protocol that have lower energy consumption than TinySec but level of security matches with that of Zigbee. It uses offset Codebook Mode(OCB) as its block cipher mode of operation. Two passes are required for secrecy and authentication.
OCB mode for faster MAC + ciphertext.

Fig 1 shows the comparison of these security protocols in terms of their energy consumption and security provided by them



3.4 Zigbee: Zigbee [6] defines the Higher Layer communication protocols based on the IEEE 802.15.4 standards. Zigbee network consists of three types of network devices - the Zigbee Coordinator, Zigbee Router and Zigbee End Device.

Zigbee coordinator: It starts network communication , stores information in the network and bridges the various networks.

Zigbee Router: It helps in linking various devices with each other and provide muti hop communication.

Zigbee End Devices: It is composed of Sensors, Actuators and Controllers that collects data and communicates with other Zigbee components.

3.5 *LEAP(Localized Encryption And authentication Protocol):* Sencun Zhu et al.[7] proposed Localized Encryption Authentication Protocol that is a key management protocol for Sensor Networks designed to support secure communications in these networks. It provides authentication and confidentiality. In addition to it LEAP has following features:

- LEAP provides four types of keys for each sensor node- an individual key shared with the base station, a pairwise key shared with other Sensor Node, a Clustered key shared with multiple neighbouring nodes, and a group key shared by all nodes in the network.
- LEAP includes use of one-way key chains for local broadcast authentication.
- Key sharing mechanism of LEAP supports in- network processing.

  Thus LEAP can prevent or make it complex to attack nodes on the sensor network.

  Following table (Table 1) shows the comparison of these security protocols on the basis of some features like encryption , freshness etc.

Table 1: Table shows comparison between Protocols based on five features i.e. Overhead , Encryption , Freshness , Key Agreement , MAC used

	SPINS	TinySec	MiniSec	LEAP	ZigBee
Overhead(Bytes)	8	4	4+3	Variable	4,8 or 16
Encryption	yes	yes	Yes	Yes	Yes
Freshness	Yes	No	Yes	No	Yes
Key Agreement	Symmetric Delayed	Any	Any	Pre-Deployed	Trust-Center
MAC Used	Yes	Yes	Yes	Yes	Yes

4. CONCLUSION AND FUTURE SCOPE

All the security protocols mentioned should be analysed using simulation and some more features like speed-of- operation, Power Consumption and Efficiency should be evaluated .The future goal of this research is to Develop a new authentication protocol or approach that should incorporate all the best features of existing security mechanisms and should be optimized for implementation in wireless sensor networks.

REFERENCES

[1] John Paul Walters , Zhengqiang Liang , Weisong Shi , and Vipin Chaudhary "Wireless Sensor Network Security: A Survey " Auerbach Publications, CRC Press 2006.

[2] Mahsa Teymourzadeh , Roshanak Vahed , Soulmaz Alibeygi , Narges Dastanpor , "Security in Wireless Sensor Networks : Issues and Challenges" International Journal of Computer Networks and Communication Security, Vol. 1 , December, 2013

[3] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler and J.D. Tygar,"SPINS: Security protocols for sensor networks", In Seventh Annual ACM International Conference on Mobile Computing and Networks(MobiCom 2001),July 2001.

M. Luk,?G.Mezzour, A. Perrig. And V. GLigor,"MiniSec: A Secure Sensor Network Communication Architecture", in IEEE International conference on Information Processing in Sensor Networks Cambridge,Massachusetts, USA, 2007

[4] C. Karlof, N. Sastry, D. Wagner , "TinySec: a link layer security architecture for wireless sensor networks",in 2nd International conference on embedded networked sensor systems, Baltimore, MD,USA,2004 , 162-175.

[5] ZigBee Specification v1.0: ZigBee Specification(2005), San Ramon , CA,USA:ZigBeeAlliance.http://www.zigbee.org/en/spec_download/download_request.asp

[6] S. Zhu , S. Setia, and S.Jajodia,"LEAP:efficient security mechanism for large scale distributed sensor networks",In CCS ' 03: Proceedings of 10th ACM Conference on Computer and Communication Security, New York, USA,2003,62-72.

[7] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayirci, "A survey on Sensor Networks," IEEE Communications Magazine, vol. 40, Issue: 8, pp. 102-114, August 2002

[8] Gaurav Sharma , Suman Bala , Anil K. Verma,"Security Frameworks for Wireless Sensor Networks-Review", 2nd International Conference on Communication, Computing & Security [ICCCS] -2012

[9] Alzaid, H., Alfaraj, M. "MASA: End-to-End Data Security in Sensor Networks Using a Mix of Asymmetric and Symmetric Approaches", 2nd IEEE International Conference on New Technologies, Mobility and Security,2008

[10] B. Arazi, L. Elhanany, O. Arazi, H. Qi, "Revisiting public-key cryptography for wireless sensor networks", IEEE Computer, 38 (11), pp. 103–105, 2005

[11] D. Boyle, T. Newe, "Security Protocols for use with Wireless Sensor Networks: A Survey of Security Architectures", Proceedings of the 3rd International Conference on Wireless and Mobile Communications, Guadeloupe, French Caribbean, pp. 54, 04-09 March 2007.

[12] A.Perrig, R.Canetti, J.D.Tygar, and D.Song, " The TESLA Broadcast Authentication Protocol," In CrytoBytes, Summer/Fall, pp:2-13 ,2002

[13] Hu Xiangdong, Feng Rui, "Message Broadcast Authentication in uTESLA Based on Double Filtering Mechanism," International Conference on Internet Technology and Applications (iTAP), pp.1,4, 16-18 Aug. 2011