ISSN:0975-9646

Security on Wireless Sensor Networks: A Survey

P.Brindha[1], Dr.A.Senthilkumar[2]

[1]Assistant Professor, Department of Computer Science, MGR College, Hosur, TN, India
[2]Assistant Professor, Department of Computer Science, Aringar Anna Government Arts College, Namakkal TN, India

Abstract-Wireless Sensor Networks(WSN) are a most powerful, challenging and promising technology for the research due to their vital scope in the field coupled with their low processing power and associated low energy. Wireless sensor networks are ally used in environmental control, surveillance tasks, monitoring, tracking and controlling etc. Mainly wireless sensor networks need the secure communication because they are being used in open field which involves broadcasting technology. Here, in this paper we discuss the security of the wireless sensor networks. Staring with a overview of the sensor networks, a review is made on how to provide the security on the wireless sensor networks.

Keywords- Wireless sensor networks, security, attacks, security protocol.

INTRODUCTION

Wireless sensor networks are the collection of nodes. Each node in the network has its own sensor, processor, transmitter and receiver. The sensors which are used are low cost devices to perform a specific sensing process. Since the sensors are low cost, they were deployed densely throughout the area where it has to monitor specific event. The wireless sensor networks operate in public and uncontrolled area, for this reason the security is a major challenge in sensor applications. The traditional security mechanisms are authentication, symmetric key encryption & decryption and Public Key Infrastructure (PKI) cryptography. The main motive is to deploy the above mentioned encryption techniques or their equivalent techniques in a sensor network which is characterized with specified memory, power supply and processing capability [1]. Today Intrusion Detection Systems (IDS) are broadly used as a security solution in a wired network in the both the form of software/ hardware to detect unwanted services going on the system and identify the distrustful patterns to indicate whether the network/system is under attack or not. For WSN quite a few schemes were proposed but they all have limited features like only address to attacks on a particular layer. There are many researchers who proposed some theoretical framework that is not suitable at deployment time [16, 17, 19, and 24].

Xbow (developer of Mica mote) & Ambient System (developer of μnode) were first two companies who produced sensor nodes for commercial use [15]. Recently Sun Microsystems have also developed a WSN platform that runs java code "on-the-metal" on their motes known as Sun SPOTs [22].

COMMUNICATION PROTOCOLS

Wireless sensor networks employ the layered architecture similar to wired network architecture. The characteristics and functions of their each layer are given in brief below.

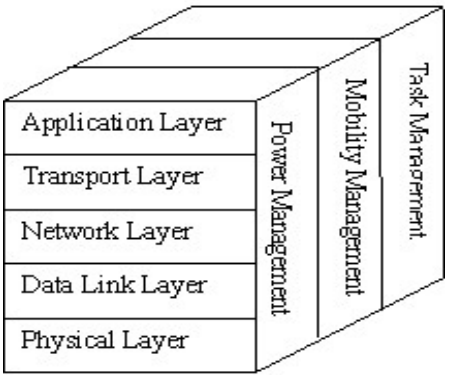

Figure1- Layered Architecture of WSN

1. Physical Layer

The aim of physical layer is to amplify the reliability by reducing path loss effect and shadowing. This layer is in charge for established connection, data rate, modulation, data encryption, signal detection, frequency generation and signal detection.

2. Data Link Layer

The aim of Data link layer is to assure interoperability. It concern on connectivity and communication between its nodes. This layer is also responsible for error detection, multiplexing, Prevention of Collision of packets, repeated transmission etc. Some researchers have worked on the possible use of public key cryptography [3, 9], secure code distribution [10] to form secure key during network installation and maintenance.

3. Network Layer

The aim of Network layer is to produce the efficient routing. It finds the best path amongst all the nodes in the network. This layer is responsible for steering the data from node to node, node to sink, node to base station, node to cluster head and vice versa. The LEACH and PEGASIS are the protocols are widely used techniques to save the energy consumption (power of sensor) so that it improves the lifetime of sensors. LEACH offers cluster based transmission while PEGASIS is chain protocol [5, 6, and 15]. For routing, WSN uses data-centric protocols and ID based protocols. All nodes in the network can acts as a router so that it can create secure routing protocol which uses broadcast communication scheme. Encryption and decryption techniques are employed for secure routing [8, 13, and 14].

4. Transport Layer

The aim of Transport Layer is to provide communication for internal nodes to external networks i.e. sensor network which is connected to the internet. This is most challenging issue in wireless sensor networks.

5. Application Layer

The aim of Application Layer is to present the final output by guarantying a smooth information flow to lower layers. This layer is accounts data collection, management and processing of the data through the application software to attain reliable results. SPINS (Security Protocols in sensor Networks) Localized Encryption and Authentication Protocol (LEAP)[12] is a key management protocol for sensor networks. It works with multiple keying mechanisms (Group Key, Cluster Key, and Pair wise Shared Key). Layer wise possible attacks and existing protocols described above are summarized in table 1 below.

WSN Layer	Types of attacks	Existing protocols
Physical Layer	Denial of service attack	
Data Link Layer	Denial of service attack	Link Layer security protocol (TinySec, PEGASIS, LEACH)
Network Layer	Denial of service attack, Wormholes, Sinkholes, Sybil attacks.	Routing protocols (ID based, data- centric)
Transport Layer	Denial of service attack	
Application Layer	Malicious Node	Aggregation scheme

Table 1 - summary of WSN layers, possible attacks on them and the existing protocols.

ATTACKS ON WSN AND THEIR MITIGATION

The security breaches occur primarily in the form of following [25, and 26].

- *Interruption* - breakdown of communication links
- *Interception* - unauthorized access of WSN
- *Modification* - Change of data by unauthorized access
- *Fabrication* - Addition of false data by unauthorized accesses

Also wirelesses Sensor Networks are vulnerable to various types of attacks. These attacks are mainly of three types:

- *Attacks on secrecy and authentication*: A standard cryptographic techniques used to protect the confidentiality and can authenticity the communication channels from anonymous attacks such as packet replay attacks, eavesdropping and modification or spoofing of packets.
- *Attacks on network availability*: Attacks on accessibility of WSN which are often referred to as denial-of-service (DoS) attacks.
- *Stealthy attack against service integrity*: The objective of the attacker is to make the network accept a fake data value.

1. Denial of Service

This type of attack results into making false resources to their users. As an example node "A" sends request to node "B" for communication and node "B" sends acknowledge to node "A" but "A" keeps on sending request to "B" constantly. As a result "B" is unable to communicate with the rest of the nodes and it results as the unavailable node to all of them. Denial of service attack might also be execute at physical layer level by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and grievance in use of networks. In network layer, it induces path failure by the way of neglecting and the greediness of packets. Flooding and de-synchronization leads to DoS in transport layer. Most of denial of service attacks can be prevented by identification mechanisms and powerful authentication.

2. Attacks of Information in Transit

Each node in WSN reports the changes to a cluster head or base station barely for data on above some threshold. Information in transit may be altered, vanished, spoofed or duplicated. In this type of attack, attacker has a wide communication range and a high processing power. It might be prevented by data aggregation and authentication techniques.

3. Sybil Attack

In this attack the attacker gets illegally multiple identities on one node. By this, the attacker frequently affects the routing mechanism. Sybil attacks are in generally prevented by validation techniques.

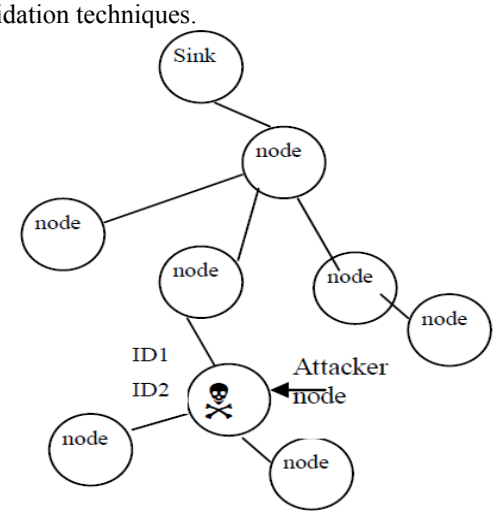

Figure 2 - Sybil Attack

4. Blackhole/ Sinkhole Attack

In this type of attack, attacker himself plays in a network with high capability resources i.e., with high processing power and high band width which results in the creation of

shortest path. Thus, all data passes through attacker's node.

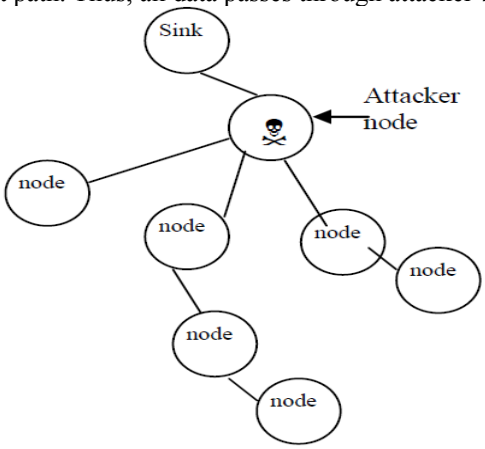

Figure 3 - Blackhole/S sinkhole Attack

5. 'Hello flood' Attack

This is a simplest attack in wireless sensor networks in which attacker broadcasts HELLO packets with high transmission control to sender or receiver. The receiver which receives the messages assumes that the sender node is nearest to them and sends packets by this node. This attack results in congestion in the network. It is a specific type of DoS. To prevent Hello Flood attacks blocking technique can be used.

6. Wormhole Attack

In this type of attack, the attacker directly plays on the routing protocol. Tunneling mechanism is used to establish for confusing the routing protocol. Figure 4 shows mechanism of wormhole attack let "Y" wants to send data by way of broadcasting before sending the data to find path. Though the attacker "☠" introduces himself as a node "X" and sends acknowledgement to "Y". "Y" sends data to "X" that is received by "☠" and "☠" sends that data to "X" by tunneling, hiding its own identity. In this case "X" and "Y" are not in a single hop but they think they are in a one hop range. The attacker "☠" thus may destroy security by interruption, interception, modification and fabrication.

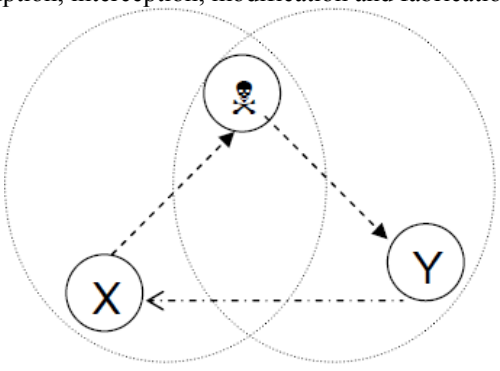

Figure 4 - Wormhole Attack

CONCLUSION AND FUTURE WORK

The overview of wireless sensor networks, their security issues and generic solutions are briefly given. Some applications of wireless sensor network are in need of a secure communication. Here, this paper portrays the introduction of WSN, a few applications, layered architecture, types of attack its feature and its revoking techniques. The existing security models for wireless sensor networks are based on some specific network models are also reviewed. As the hardware technologies are growing rapidly will automatically eliminating the hardware constraint like low processing speed, low memory and battery life time of the sensors may soon be overcome or reduced to facilitate the powerful security measures which are being adopted in this field.

REFERENCES

[1] Jan Steffan, Ludger Fiege, Mariano Cilia Alejandro Buchman,"Scoping in Wireless Sensor Networks", 2nd workshop on middleware for pervasive and Ad-Hoc Computing Toronto, Canada,2004 ACM 1-58113-951-9.

[2] Chris karlof, Naveen Sastry, David Wanger, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd international conference on Embedded networked sensor systems, November 3-5, 2004, pages 162-172,Baltimore, Maryland, USA. ISBN:1-58113-879-2.

[3] Gunnar Gaubat, Jens-Peter Kaps, BerkSunar, "Public Key Cryptography in Sensor networks- Revisited", Book Series Lecture Notes in Computer Science Pages 2-18, 11 january 2005.

[4] Naveen Sastry, David Wagner, "Security Consideration for IEEE802.15.4 Networks", WiSE"04, October 1, 2004 Philadelphia, Pennsylvania,USA.

[5] Cauligi S. Raghavendra,"PEGASIS: Power- Efficient Gathering in Sensor Information System", 2002 IEEE Aerospace Conference Proceedings - Volume 3, Big Sky, MT;UNITED STATES; 9-16 Mar. 2002. pp. 3-1125 to 3-1130. 2002 2002.

[6] Siva D. Muruganathan, Daniel C.F. MA, Rolly I. Bhasin, Abraham O. Fapojuwo,"A Centralized Energy- Efficient Routing Protocol for Wireless Sensor Networks", IEEE Communications Magazine. Vol. 43, no. 3, pp. S8-13. Mar. 2005.

[7] David Wagner, university of California "Resilient Aggregation in Sensor Networks",2nd ACM workshop on Security of adhoc and sensor networks, Pages 78-87, October 25 2004 Washington DC, USA.

[8] Xiao Chen, Jawad Drissi, "An Efficient Key Management Scheme in Hierarchical Sensor Networks", IEEE MASS 2005 Workshop-WSN05.

[9] Kirk H.M. Wong, Yuan Zheng, JiannongCao, Shengwei Wang," A Dynamic User Authentication Scheme for Wireless Sensor Networks", IEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing (SUTC"06), 2006.

[10] Jing Deng, Richard Han, Shivakant Mishra,"Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks", 5th international conference on Information processing in sensor networks, Pages 292-300, April 19-21, 2006.

[11] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen, "SPINS: Security Protocols for Sensor Networks", Department of Electrical Engineering and Computer Sciences, University of California, Berkley, 2002.

[12] Sencun Zhu, Sanjeev Setia, Sushil Jajodia,"LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", Aug. 2004, publish inACM.

[13] Al-Sakib Khan Pathan, hyung-Woo Lee,Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb 20-22, 2006 ICACT2006.

[14] Woo Kwon Koo, Hwaseong Lee, Yong Hokim, Dong Hoon Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks", International Conference on Information Security and Assurance,2008.

[15] Christian Herman and Waltenegus Dargie,"Senceive: A Middleware for a Wireless Sensor Network",22nd international Conference on Advanced Information Networking and Applications, 2008.

[16] Bo Sun, Lawrence Osborne, Yang Xiao, Sghaier Guizani, "Intrusion Detection Techniques In Mobile Ad hoc and Wireless Sensor Networks", IEEE Wireless Communications October2007.

[17] Zhenwei Yu, Jeffrey J.P. Tsai "A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks", 2008 IEEE.

[18] Tutorial of NS2 http://www.isi.edu/nsnam/ns/tutorial/

[19] Online tutorials http://en.wikipedia.org/wiki

[20] Tutorial of OMNeT++http://personal.stevens.edu/~hli5/TutorialofOMNET.htm
[21] Philip Levis, "TinyOS Programming ", june 28 ,2006
[22] Http://mobilab.wustl.edu/projects
[23] Min Chen, Taekyoung Kwon, Yong Yuan and Victor C.M. Leung, "Mobile Agent Based Wireless Sensor Networks", Journal of computers, vol. 1, No. 1, APRIL2006.
[24] Yun Zhou," LLK: A Link-Layer Key Establishment Scheme for Wireless Sensor Networks", IEEE Communication Society / WCNC2005.
[25] Mohammad Ilyas and Imad Mahgoub, "Handbook of Sensor Networks: Compact Wireless and Wired Sensing System", CRC Press, London New York Washington, D.C.
[26] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti,"A survey on Wireless Sensor Networks Security", 4th International Conference: sciences of Electronic, Technologies of Information and Telecommunications, March 25-29, 2007, TUNISIA.