RESEARCH ARTICLE OPEN ACCESS

A Survey on Threats and Security schemes in Wireless Sensor Networks

P.P.Joby[1], Dr.P.Sengottuvelan[2]
1. Research Scholar, Anna University, Chennai
2. Associate Professor, Bannari Amman Institute of Technology, Sathyamangalam

ABSTRACT
It is difficult to achieve and become particularly acute in wireless sensor networks due to the limitation in network capability, computational power and memory which do not allow for implementation of complex security mechanism because security being vital to the acceptance and use of wireless sensor networks for many applications. In this paper we have explored general security threats in wireless sensor networks and analyzed them. This paper is an attempt to survey and analyze the threats to the wireless sensor networks and focus on the type of attacks and achieve secure communication in wireless sensor networks.

Keywords: Wireless sensor Networks, WSN, Security, Threats, Authentication, Confidentiality.

I. INTRODUCTION

A wireless sensor network is a self-organizing network, through a large number of low-cost, resource-constrained sensor node devices to work together to achieve a specific task. It is the perception and acquisition of information technology, a revolution in the 21st century, one of the most important technologies. It is in climate monitoring, the temperature of the surrounding environment, light, humidity detection, atmospheric pollution monitoring, monitoring the structural integrity of buildings, the abnormal family environment, airport or stadium chemical, biological threat detection and prediction and so on, WSN will be an economic alternative, with a wide range of applications. Sensor network is the cause for the deployment in complex large-scale network environment, real-time data acquisition and processing of hope. WSN is usually deployed in the same time, no maintenance, non-controlled environment, in addition to facing the wireless network with the general disclosure of information, information tampering, replay attacks, denial of service and other threats, WSN sensor nodes is also likely to be faced physical manipulation of the attacker, and stored in the sensor nodes to obtain all the information to control the threat of part of the network. A good security design is based on the threats to its network features, etc. based on a profound analysis, sensor network is no exception. This article will feature in-depth analysis of wireless sensor networks security threats, and their corresponding security measures.

II. CHARACTERISTICS OF SENSOR NETWORKS

WSN is a large-scale distributed network, often deployed in unattended maintenance, poor conditions of the environment, in most cases single-use sensor nodes to determine the sensor node is low cost, extremely limited resources of wireless communication devices which is characterized in the following areas:

2.1 Limited energy: energy is to limit the ability of sensor nodes, the life conditions of the most important constraints are some sensor nodes are AAA or AA by Standard battery-powered, and cannot be recharged.

2.2 Limited computing power: sensor nodes CPU is typically for 8bit, 4 MHz - 8 MHz of processing power.

2.3 Limited storage capacity: sensor nodes generally include three types of memory RAM, program memory and working memory. RAM is used to store temporary data when working, usually no more than 2kbytes,program memory for storing the operating system, applications, and security functions, sensor memory is used to store information.

2.4 Limited communication range: the time of signal transmission for energy consumption, sensor nodes in the transmission of RF power module is generally between 10mW to 100 MW, the transmission range is also limited to 100 meters to within 1 km.

2.5 Tamper resistance: is the low cost sensor node. It is a loose, open network equipment, once an attacker can easily gain access to sensor nodes and modify the sensor nodes that are stored in the key information and code and so on.

III. Security Requirements in WSN

A Wireless Sensor Network is a special type of network. It shares some common features with a typical computer network, but it also parades many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from threats and misbehavior of nodes. Some important security requirements are discussed.

3.1 Confidentiality

Confidentiality requirement is needed to ensure that sensitive information is well protected and not revealed to unauthorized third parties. The confidentiality objective is required in sensor environment to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication. By eavesdropping, the adversary could overhear critical information such as sensing data and routing information. Based on the sensitivity of the data stolen, an adversary may cause severe damage since he can use the sensing data for many illegal purposes i.e. sabotage blackmail.

3.2 Authentication

Authentication techniques verify the identity of the participants in a communication, differentiating the way legitimate users from intruders. In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data is supplied into the network, then the behavior of the network could not be predicted and most of the times outcome will not be as expected. Authentication objective is essential to be achieved when clustering of nodes is performed. clustering involves grouping nodes based on some attribute such as their location, sensing data etc and that each cluster usually has a cluster head that is the node that joins its cluster with the rest of the sensor network. In these cases, where clustering is required, there are two authentication situations which should be investigated, first it is critical to ensure that the nodes contained in each cluster will exchange data only with the authorized nodes contained and which are trusted by the specified cluster. Otherwise, if nodes within a cluster receive data from nodes that are not trusted within the current community of nodes and further process it, then the expected data from that cluster will be based on false data and may cause damage. The second authentication situation involves the communication between the cluster heads of each cluster; communication must be established only with cluster heads that can prove their identity. No malicious node should be able to masquerade as a cluster head and communicate with a legitimate cluster head, sending it false data or either compromising exchanged data.

3.3 Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn’t mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

3.4 Availability

This requirement ensures that the services of a WSN should be available always even in the presence of an internal or external attacks.. Different approaches have been proposed by researchers to achieve this goal. While some mechanisms make use of additional communication among nodes, others propose use of a central access control system to ensure successful delivery of every message to its recipient.

3.5 Data Freshness

Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when the WSN nodes use shared keys for message communication, where a potential adversary can launch a replay attack. A nonce or time-specific counter may be added to each packet to check the freshness of the packet.

3.6 Self-organization

A wireless sensor network is a typically an adhoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security.

3.6 Secure Localization

A sensor network will rely on its ability to locate accurately and automatically each sensor in the network. A sensor network designed to locate faults will need accurate locations information in order to pinpoint the location of a fault. An attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc.

IV. SECURITY VULNERABILITIES IN WSNS

Wireless Sensor Networks are vulnerable to various types of attacks. These attacks are mainly of three types (i) Attacks on network availability, (ii) Attacks on secrecy and authentication, (iii) Stealthy attack against service integrity.

4.1 THREATS IN WIRELESS SENSOR NETWORKS

Threats against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms.

Threats

Wireless networks are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. These attacks are normally due to one or more vulnerability at the various layers in the network .Sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. The security of the WSNs is compromised due to the attacks. An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or an attempt to compromise integrity, availability, or confidentiality of a system. The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw. Attacks on the computer system or network can be broadly classified as interruption, interception, modification and fabrication. Interruption is an attack on the availability of the network, for example physical capturing of the nodes, message corruption, insertion of malicious code etc. Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it. Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with counterfeit data. Fabrication is an attack on authentication. In fabrication an adversary injects false data and compromises the trustworthiness of the information relayed. Certain critical attacks are explained in detail.

4.1.1 Denial of Service (DoS): This attack is possible on every layer of the system. Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. This attack is a pervasive threat to most networks. Sensor networks being very energy-sensitive and resource-limitation, they are very vulnerable to DoS attacks. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness may occur at network layer, neglect and greed, homing, misdirection, black holes

and at transport layer this attack could be performed by malicious flooding and de-synchronization. Potential defenses against denial-of service attacks are as varied as the attacks themselves. Techniques such as spread-spectrum communication or frequency hopping can counteract jamming attacks. Proper authentication can prevent injected messages from being accepted by the network. However, the protocols involved must be efficient so that they themselves do not become targets for an energy exhaustion attack. For example, using signatures based on asymmetric cryptography can provide message authentication. However, the creation and verification of asymmetric signatures are highly computationally intensive, and attackers can induce a large number of these operations and mount

an effective energy-exhaustion attack.

4.1.2 Sybil Attack: This attack is defined as a malicious device illegitimately taking on multiple identities. In Sybil attack, an adversary can appear to be in multiple places at the same time. In other words, a single node presents multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of legitimate nodes. Sybil attack is a harmful threat to sensor networks. It poses a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors efficiently to route geographically addressed packets. The Sybil attack can disrupt normal functioning of the sensor network, such as multipath routing, used to explore the multiple disjoint paths between source-destination pairs. It can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, dispersive and multipath Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. It can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection.

4.1.3. Sinkhole Attack: In sinkhole attacks, a malicious node acts as a black hole to attract all the traffic in the sensor network through a compromised node creating a symbolic sinkhole with the adversary at the center. A compromised node is placed at the centre, which looks attractive to surrounding nodes and lures nearly all the traffic destined for a base station from the sensor nodes. Thus, creating a metaphorical sinkhole with the adversary at the center, from where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station. The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. Sinkholes are difficult to defend in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify.

4.1.4 Wormhole: Wormhole attack is a critical attack in which the attacker records the packets at one location in the network and tunnels those to another location. In the wormhole attack, an adversary eavesdrop the packet and can tunnel messages received in one part of the network over a low latency link and retransmit them in a different part. This generates a false scenario that the original sender is in the neighborhood of the remote location. The tunneling procedure forms wormholes in a sensor network. The tunneling or retransmitting of bits could be done selectively. The simplest case of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbors, leading to quick exhaustion of their energy resources. Wormholes are effective even if routing information is authenticated or encrypted. This attack can be launched by insiders and outsiders. This can create a sinkhole since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. When this attack is coupled with selective forwarding and the Sybil attack it is very difficult to detect. More generally, wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. The goal of this attack is to undermine cryptography protection and to confuse the sensor's network protocols. Wormhole attack is a significant threat to wireless sensor networks, because this type of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information.

Hello flood Attack: This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. This assumption may be false. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker. A laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbor, so that all the nodes will respond to the HELLO message and waste their energy. In a HELLO flood attack, every node thinks that the attacker is within one-hop radio communication range. If the attacker subsequently advertises low-cost routes, nodes will attempt to forward their messages to the attacker. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to this attack. HELLO floods can also be thought of as one-way, broadcast wormholes.

V. SECURITY SCHEMES

At the basic level, the security schemes are to prevent the above attacks that can be based on (a) symmetric key encryption schemes, (b) message authentication codes and the public key cryptography. These in turn individually raise concerns like key setup and establishment, feasibility of applying cryptographic techniques in hardware, use of sophisticated measures like spread-spectrum to tackle jamming, feasibility of the public key cryptography in resource starved sensor nodes.

Security protocols for sensor networks (SPIN) was proposed by Adrian Perrig in which security building blocks optimized for resource constrained environments and wireless communication. SPINs has two secure building blocks: (a) sensor network encryption protocol (SNEP) and (b) μTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments. SNEP uses encryption to achieve confidentiality and message authentication code (MAC) to achieve two-party authentication and data integrity. Since sending data over the RF channel requires more energy, all cryptographic primitives such as encryption, MAC, hash, random number generator, are constructed out of a single block cipher for code reuse. This, along with the symmetric cryptographic primitives used reduces the overhead on the resource constrained sensor network. SNEP provides number of advantages such as low communication overhead, semantic security which prevents eavesdroppers from inferring the message content from the encrypted message, data authentication, replay protection, and message freshness. TinySec is link layer security architecture for wireless network, which was designed by Karlof. It provides similar services as of SNEP, including authentication, message integrity, confidentiality and replay protection. It is a lightweight, generic security package that can be integrated into sensor network applications. A major difference between TinySec and SNEP is that there are no counters used in TinySec.TinySec provides the basic security properties of message authentication and integrity using MAC, message confidentiality through encryption, semantic security through an Initialization Vector and replay protection. Localized encryption and authentication protocol (LEAP) is a key management protocol for sensor networks. It is designed to support in-network processing and secure communications in sensor networks. LEAP provides the basic security services such as confidentiality and authentication.

VI. CONCLUSION

Sensor networks are set to become a truly pervasive technology that will affect our daily lives in important ways. We cannot deploy such a critical technology, however, without first addressing the security and privacy research challenges to ensure that it does not turn against those whom it is meant to benefit.

Biographical notes:

Mr.P.P.Joby received B.E.,degree in the Branch of Computer Science and Engineering from Periyar University, Salem in 2002 and M.TECH., degree in Advanced Computing from SASTRA University. Thanjavur in 2005. He is currently pursuing his Ph.D. in Anna University, Chennai. Presently, he is working as an Associate Professor in the Department of Information Technology, PPG Institute of Technology, Coimbatore. His Ph.D. dissertation is focused on “Wireless Sensor Network Security”**Dr.P.Sengottuvelan** received M.Sc., Degree in Computer Technology from Periyar University, Salem in 2001 and Master of Philosophy in Computer Science from Bharathiyar University, Coimbatore in 2003 and M.E. degree in Computer Science & Engineering from Anna University, Chennai in 2004. He also received his Ph.D. degree in Computer Science & Engineering from Vinayaka Missions University, Salem in 2010. Since 2004, he has been a Faculty in the Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam. His current research focuses on Concurrent Engineering, Multi Agent System Networks; Constraint Management Agents He is a member of IACSIT, ACEEE, IAENG and a Life Member of FUWA and ISTE..

REFERENCES

[1] Haowen Chan and Adrian Perrig, Carnegie Mellon University”*Security and Privacy in Sensor Networks*”

[2] Shio Kumar Singh,M P Singh , and 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

[3] 3. JaydipSen Innovation Lab, Tata Consultancy Services Ltd. India” *Routing Security Issues in Wireless Sensor Networks: Attacks and Defenses*”

[4] Sen, J. ; Chandra, M.G. ; Balamuralidhar, P. ; Harihara, S.G. & Reddy, H. (2007a). *A distributed protocol for detection of packet dropping attack in mobile ad hoc networks*. Proceedings of the IEEE International Conference on Telecommunications

[5] (ICT’07), Penang, Malaysia.

[6] Wang, Y. ; Attebury, G. & Ramamurthy, B. (2006). *A survey of security issues in wireless sensor networks*. IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2- 23.

[7] D. C. Jinwala Dhiren R. Patel K. S. Das Gupta” *A survey of the security issues in wireless sensor networks*”

[8] N Ahmed, Salil S Kanhere, Sanjay Jha, *The Holes Problem in Wireless Sensor Networks: A Survey*, Mobile Computing and Communications Review, Volume 9, No 2, April 2005.

[9] M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, “*A Survey on Wireless Sensor Networks Security*”, SETIT 2007.

[10] S.S. Kulkarni, M.G. Gouda, and A. Arora, “*Secret instantiation in adhoc networks*,” Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, May 2005, pp. 1–15.

[11] A.D. Wood, J.A. Stankovic, and S.H. Son, "*JAM: A Jammed- Area Mapping Service for Sensor Networks*", 24th IEEE Real-Time Systems Symposium, (RTSS), 2003, pp. 286-297.

[12] W. Stallings, "*Cryptography and Network Security Principles and Practice*", Cryptography Book, 2nd Edition, Prentice-Hall, 2000, 0- 13-869017-0.

[13] Chris Karlof, Naveen Sastry, and David Wagner, "*TinySec: A Link Layer security Architecture for Wireless Sensor Networks*", *ACM SenSys 2004,* Nov. 3-5, 2004, pp. 162-175.

[14] Adrian perrig, John stankovic, *and D*avid wagner" *Security in Sensor Networks*" communications of the acm june 2004/vol. 47, no. 6.

[15] Hu, Y.-C., Perrig, A., and Johnson, D. *Packet leashes: A defense against wormhole attacks in wireless ad hoc networks*. In Proceedings of IEEE Infocom 2003 (San Francisco, Apr. 1–3, 2003).

[16] Wood, A. and Stankovic, J. *Denial of service in sensor networks*. IEEE Comput. (Oct. 2002), 54–62.

[17] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong" *Security in Wireless Sensor Networks: Issues and Challenges*" Feb. 20-22, 2006 ICACT2006 ISBN 89-5519-129-4.

[18] Culler, D. E and Hong, W., "*Wireless Sensor Networks"* Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[19] 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.

[20] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E.," *Wireless Sensor Networks: A Survey*", Computer Networks, 38, 2002, pp. 393-422.

[21] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "*SPINS: Security Protocols for Sensor Networks*", Wireless Networks, vol. 8, no.5, 2002, pp. 521-534.

[22] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "*Security in Mobile Ad Hoc Networks: Challenges and Solutions*", IEEE Wireless Communications, Volume 11, Issue 1, February 2004, pp. 38 – 47.

[23] 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, September 2003, pp. 293-315.

[24] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary., "*Wireless Sensor Network Security:A Survey Security in Distributed*, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp.c 2006 Auerbach Publications, CRC Press

[25] J. Deng, R. Han, and S. Mishra. *Security, privacy, and fault tolerance in wireless sensor networks*. Artech House, August 2005.

[26] Tolga Onel, Ertan Onur, Cem Ersoy and Hakan Delic" *wireless sensor networks for security: issues and challenges*"

[27] D. P. Mishra and m. K. Kowar" *A survey on security issues and challenges in Wireless sensor networks International J.of Multidispl.* Research & Advcs. in Engg. (IJMRAE),ISSN 0975-7074, Vol. 2, No. III (October 2010), pp. 29-40 http://www.xbow.com/wireless home.aspx, 2006.

[28] L. Hu and D. Evans. *Using directional antennas to prevent wormhole attacks.* In In 11th Annual Network and Distributed System Security Symposium, February 2004.

[29] B. Schneier. Applied Cryptography. Second Edition, John Wiley & Sons, 1996.

[30] Feng Zhao, Leonidas. J.Guibas, "*Wireless Sensor Networks"* Morgan Kaufamann Publishers, 2000.

[31] Kazem Sohraby, Daniel Minoli, Taieb Znati, "*Wireless Sensor Networks Technology, Protocols and applications*", Wiley edition,2007.

[32] C. Siva Ram Murthy and B.S. Manoj "*Ad Hoc Wireless Networks: Architectures and Protocols*", Prentice Hall PTR, 2004.

[33] C.K. Toh, Ad Hoc Mobile Wireless Networks: "*Protocols and Systems*", Prentice Hall PTR, 2001.

[34] Hemanta Kumar Kalita and Avijit Kar" *Wireless Sensor Network Security Analysis*" International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

[35] X. Du, H. Chen, "*Security in Wireless Sensor Networks*", IEEE Wireless Communications,2008.