WIRELESS SENSOR NETWORKS – ARCHITECTURE, SECURITY REQUIREMENTS, SECURITY THREATS AND ITS COUNTERMEASURES

Ranjit Panigrahi[1], Kalpana Sharma[2], M.K. Ghose

[1]Department of Computer Sc. & Engineering, SMIT, Majhitar, Sikkim, India
ranjit.panigrahi@gmail.com
[2]Department of Computer Sc. & Engineering, SMIT, Majhitar, Sikkim, India
kalpanaiitkgp@yahoo.com
[3]Department of Computer Sc. & Engineering, SMIT, Majhitar, Sikkim, India
mkghose@smu.edu.in

ABSTRACT

Wireless Sensor Network (WSN) has a huge range of applications such as battlefield, surveillance, emergency rescue operation and smart home technology etc. Apart from its inherent constraints such as limited memory and energy resources, when deployed in hostile environmental conditions, the sensor nodes are vulnerable to physical capture and other security constraints. These constraints put security as a major challenge for the researchers in the field of computer networking. This paper reflects various issues and challenges related to security of WSN, its security architecture. The paper also provides a discussion on various security mechanisms deployed in WSN environment to overcome its security threats.

KEYWORDS

Sensor network, security, Denial of Service (DoS), Intrusion Detection System (IDS), Authentication.

1. INTRODUCTION

In today's realistic world Wireless Sensor Networks (WSN) [1] has become the most popular communication medium because of its low cost architecture. It is one of the emerging wireless networks among the various classes of communication net-works such as Cellular Networks, Adhoc Networks and Mesh Networks. An Adhoc network cannot be considered as a sensor network because an Adhoc Network uses multi hop radio relaying and is lack of sensors [2].

A Wireless Sensor Network is defined differently by different authors. According to Akkaya and Younis [3] WSN is a network that consists of small nodes with sensing, computation and communication capabilities. Akylidiz et al.[1] defines WSN as a network consisting of large number of nodes that are deployed in such a way that they can sense the phenomena. Similarly according to Gowrishankar et al.[4] WSN is a special class of adhoc wireless network that are used to provide a wireless communication infrastructure that allows us to instrument, observe and respond to the phenomena in the natural environment and in our physical and cyber infrastructure.

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 107–115, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3611

In short a WSN is a special kind of adhoc wireless network equipped with the sensors to sense the environment.

Designing a wireless sensor network involves variety of challenges such as hard-ware issues and Operating System, characteristics related to wireless radio communication, medium access schemes, deployment, localization, synchronization, calibration, synchronization, data aggregation and dissemination, Quality of Service and security. Many researchers carried out many research works on these issues; however security is the most challenging area in WSN which is yet to be explored extensively.

Since the sensors are usually deployed in open environment they are non trust worthy and hence prone to various security threats. The common security threats include information disclosure, message injection, sleep deprivation attack etc [5]. An attacker may capture and compromise a node and thus be able to control some part or even the whole network exclusively [5]. For example, in a sleep deprivation attack the intruder makes a node or a set of nodes to remain busy; so that they waste their energy while carrying out the task for the intruders [6]. This attack imposes a huge amount of energy consumption upon the sensor nodes and as a result the node battery becomes exhausted and thus the concerned node stops working. The condition becomes worst if WSN is deployed in a hostile environment. In addition to this there may be a possibility of Denial of Service attacks in WSN. Therefore it is required to employ a tight security mechanism to overcome these security threats. Many security mechanisms are presented by many authors. Broadly they are either Key Management techniques or Intrusion Detection techniques.
The rest of the paper has been organized as follows: section 2 deals with architecture and environment of WSN, section 3 reflects the various security requirements related to WSN, section 4 focuses on security threats and the related issues followed by section 5 which deals with the various security mechanisms and finally the paper is concluded at section 6.

2. ARCHITECTURE OF WIRELESS SENSOR NETWORK

A WSN is a collection of sensor nodes which are deployed in a sensor fields which collect and route data back to the Base Station. A sensor node can be divided into four basic parts, viz. the sensing unit, a processing unit, a transceiver unit, and a power unit [7][8]. Localization is the heart of the routing principle in WSN. The position finding system helps the sensor node to discover its position in the environment. The power unit gives the constant power supply to the sensor nodes which is the prime target area of the intruders.

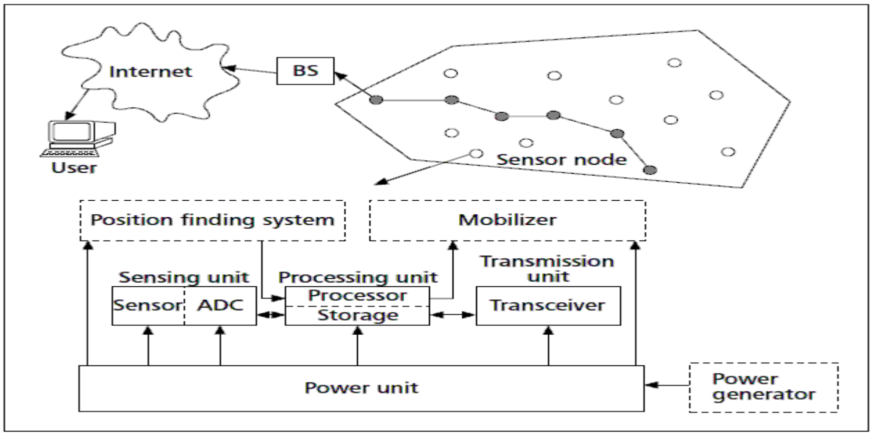

Figure 1. The components of a sensor node (Source: [7]).

3. SECURITY REQUIREMENTS

The main aim of security aspects of WSN is to protect WSN resources and information. This can be achieved by fulfilling the following security requirements.

3.1. Resource Confidentiality

Confidentiality is the major concern for achieving security in WSN [8][33]. Resource confidentiality works on the principle that, "the resource destined for the destination only". In other words a WSN node should not leak information about the sensed signal at any cost. While transmitting data the sensor node must create a secure channel for the destination.

3.2. Resource Integrity

Confidentiality doesn't mean integrity of data [8]. Although the intruder may not be able to steal data but it may modify the data in certain cases. As a result the sensor network receives the modified information. Therefore Data integrity ensures that the received data by a node should not be altered.

3.3. Resource Freshness

In this requirement a node must ensure that it received the fresh data. Data freshness suggests that the data is recent, and it ensures that no old messages have been resent [8][33].

3.4. Resource Availability

The sensors and the sensor network itself is a scarce resource. The availability of these resources is vital [8][33]. The availability of a sensor and sensor network is a tedious, because in a WSN additional computation consumes more energy. So for a secure WSN these resources must be available.

3.5. Self Organization

Like adhoc wireless network a WSN need to be self organizing in nature in different situations[33]. For example in case of a node failure the other stable node must able to identify the best path to the destination by bypassing the failed node.

3.6. Time Synchronization

Time synchronization is a vital scenario in WSN [33]. During transmission the sensor may off or on in order to preserve energy. In such a scenario it is very tedious to be synchronized. So the sensor node must ensure that time synchronization is achieved in such a distributed environment.

3.7. Node Authentication

During data transmission it is prime goal that the data which is intended for the destination must be delivered to the destination only. In other words, data authentication allows a receiver to verify that the data really is sent by the claimed sender [8][33]. This can be achieved by introducing a message authentication code (MAC) of all communicated data [33].

3.8. Node Authorization

Node authorization is another aspect for providing security in a WSN environment [8]. In this process the receiver on receives the data of genuine senders.

4. SECURITY THREATS AND ITS RELATED ISSUES

The WSN is more vulnerable to various security threats as compared to its counterpart wired network [9][10][11][12]. It is because the WSN access the open shared channel. The security threats related to wireless adhoc networks are similar to wireless sensor networks [10][11]. These security threats along with various security schemes are reflected in various research papers [10][11][12]. It should be noted that the security schemes and protocols used for adhoc wireless network can't applied directly to the WSN, because of the architectural complexity of the sensor nodes [13]. One of the most challenging security threats in WSN is the Denial of Service (DoS). This paper mainly focuses of DoS attacks. The various DoS attacks and its related measures are summarized in Table 1.

Table 1. Various attacks and its security measures. (Source [8])

Attacks and its behaviors	**Security measures**
Jamming - The attacker's radio frequency interferes with the radio frequencies of stable nodes. [8][14]	Enhancing variations of spread-spectrum communication such as frequency hopping and code spreading [15]. Implementing Code spreading [8].
Tampering - An attacker can extract sensitive information such as cryptographic keys or other data on the node.	Tamper-proofing the node's physical package.[8][15]
Collision - Intentionally creating collisions in specific packets such as ACK control messages. [8][15]	Implementing error-correcting code [8]
Exhaustion - Creating repeated collisions by an attacker to cause exhaustion of resources [8].	Applying rate limits to the MAC admission control so that the network can ignore excessive requests. Employing time-division multiplexing where each node is allotted a time slot in which it can transmit [8].
Spoofing altered and Replayed routing information - For disrupting traffic in the network an attacker may spoof, alter, or replay routing information.[16]	Appending a message authentication code at the end of the message. In this way the receivers can verify whether the messages have been spoofed or altered.[8][17] Counters or timestamps can be included in the messages for defending against replayed information.[8][17]
Selective forwarding. - An attacker node during data transmission foreword specific packets and drop others. For example, Black hole attack where the attacker drops all the packets that it receives	Using multiple paths to send data [16][8]. Selecting the malicious node and chose a path that does not follow the malicious node.

Sinkhole - The malicious node behave that it is the best node and having the best path to the destination [8][9]. Sybil - The attacker node has multiple identities in the network [8][9]. Wormholes - The attackers receive packets at one location of the network and tunnel them to the other location of the network [9]. Hello flood attacks - Using a high power transmitter the attacker broadcast hello packets to the surrounding nodes which are practically far apart from the flooder [9]. Acknowledgement spoofing - Grab the acknowledgement and provide false information to those neighboring nodes [8].	Egress filtering, authentication, monitoring Redundancy, probing, Authentication, monitoring, redundancy Authentication, probing Authentication, packet leashes by using geographic and temporal information Authentication, verify the bidirectional link Authentication [8].
Flooding - An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. [8] Desynchronization - An attacker may repeatedly spoof messages to an end host, causing missed frames as a result the nodes lost its synchronization [8].	Client puzzles Authentication [8].

5. COUNTERMEASURES TO THE VARIOUS SECURITY THREATS

The common security measures to deal with the security threats are by implementing cryptography in WSN. This can be achieved either through public key or private key cryptography [8][33]. In public key cryptography two mathematically related keys are maintained, one of which is made public while the other is kept private [8][33]. In this process data is encrypted with the public key and decrypted only with the private key. The problem with asymmetric cryptography, in a wireless sensor network, is that it is typically too computationally intensive for the individual nodes in a sensor network [8]. Thus, this technique is not popular in WSN family. Alternatively the use of Symmetric key cryptography in WSN reduces computational complexity. Apart from key management techniques WSN also use Intrusion Detection as another method to keep WSN family secure from the intruders.

Therefore, the WSN Security is entirely based on the following two concepts

5.1. Key Management

The main goal of Key management technique is to establish a valid key pair among the sensor nodes so that they can exchange data more securely [8][18][33]. There were many key management techniques but most of these are impractical in a large network such as pair wise key distribution scheme because it require larger amount of overhead [8].

Although many key management protocols are proposed but these protocols suffer from the drawbacks stated below.

- Most of the key management schemes assume that the Base Station is trust worthy [8] but which is not always true.

- Most of the key management schemes are based on private key cryptography but the public key management schemes may be extended to support public key cryptography.

5.2. Intrusion Detection System [IDS]

An intrusion can be defined as a set of actions that can lead to an unauthorized access or alteration of a certain system [32]. The main aim of intrusion detection system is the identification of intrusions and intruders thus alerting it to the user. It monitors a host or network for malicious activity [6][32]. Various authors propose various schemes pertaining to intrusion detection in order avoid possible intruders in terms of filtering injected false information only [6][32]. So these protocols need to be re defined in order to achieve scalability issues. Table 2 focuses on various security schemes and the major features that it proposes.

Table 2. Summary of various security schemes for WSN (Source [9])

Security Schemes and Attacks Deterred	**Network Architecture**	**Major Features**
JAM [19]. DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based [20]. DoS Attack (Jamming)	Hybrid sensor network	Uses wormholes to avoid jamming
Statistical En-Route Filtering [21]. Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution etc. [22]. Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting Sybil entity
Bidirectional Verification, Multipath multi-base station routing [23]. Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security [24]. Information or Data Spoofing	Traditional wireless sensor network	Efficient resource management, Protects the network even if part of the network is compromised
TIK [25]. Wormhole Attack, Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Predistribution [26], [27], [28]. Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
REWARD [29]. Black hole attacks	Traditional wireless sensor network	Uses geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect Black hole attacks

TinySec [30]. Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & µTESLA [31]. Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

6. CONCLUSIONS

The rapid application of WSN in today's world leads to various attacks and security threats [33]. Therefore, it becomes necessary to deploy strong security mechanisms to prevent possible intruders. This paper reflects the overview of security in WSN. Covering the architecture, security requirements, security threats and attacks possible, and various mechanisms used to overcome these security issues in WSN in brief. The main solution to WSN security viz., the Key Management scheme and Intrusion Detection System (IDS) are highlighted. Summary of various security schemes are also provided.

REFERENCES

[1] Akylidiz, I. , Su,W., Subramaniam, S., and E.Cayrici, "A survey on sensor networks", IEEE Communications Magazine, Volume: 40 Issue: 8, August 2002, pp.102-114.

[2] Cao, J., "Mobile ad-hoc and sensor networks" MSN (2, 2006, Hong Kong) – 2006

[3] Akkaya, K. and Younis, M., "A survey of Routing Protocols in Wireless, Sensor Networks", Elsevier Ad Hoc Network Journal, 2005, pp 325-349.

[4] Gowrishankar, S., Basavaraju, T.G., Manjaiah, D.H. and Sarkar, S.K., "Issues in wireless sensor networks", July 2008.

[5] Schmidt,S., Krahn,H., Fischer,S., and Watjen,D.. A Security Architecture for Mobile Wireless Sensor Networks: LNCC 3313, Spronger-Verlag Berlin Heidelberg, pp. 166-177, 2005

[6] Bhattasali,T., Chaki,R., "A Survey Of Recent Intrusion Detection Systems For Wireless Sensor Network"

[7] Akyildiz, I.F., et al., "A Survey on Sensor Networks," IEEE Communications Magazine, vol. 40, no. 8, Aug. 2002, pp. 102–114.

[8] Wang, Y., Attebury,G., Ramamurthy,B., "A Survey of Security Issues In Wireless Sensor Networks", CSE Journal Article Paper 84 Jan 2006.

[9] Pathan, A-S. K, Lee, H., Hong, C. S., "Security in Wireless Sensor Networks: Issues and Challenges", ICACT2006, Feb 2006.

[10] Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30.

[11] Strulo, B., Farr, J., and Smith, A., "Securing Mobile Ad hoc Networks — A Motivational Approach", BT Technology Journal, Volume 21, Issue 3, 2003, pp. 81 – 89.

[12] 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.

[13] Pathan, A-S. K., Alam, M., Monowar, M., and Rabbi, F., "An Efficient Routing Protocol for Mobile Ad Hoc Networks with Neighbor Awareness and Multicasting", Proc. IEEE E-Tech, Karachi, 31 July, 2004, pp. 97-100.

[14] Shi, E., and Perrig,A., "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004 pp. 38–43.

[15] Wood, A.D., and Stankovic, J.A., "Denial of service in sensor networks", IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.

[16] Karlof, C. and Wagner, D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications, May 2003, pp. 113–27.

[17] Perrig, A., et al., “SPINS: Security Protocols for Sensor Networks,” Wireless Networks, vol. 8, no. 5, Sept. 2002, pp. 521–34.

[18] Eschenauer, L., and Gligor,V., A Key-Management Scheme for Distributed Sensor Networks. In Proc. of ACM CCS’02, November 2002.

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

[20] Cagalj, M., Capkun, S., and Hubaux, J-P., “Wormhole-based Anti-Jamming Techniques in Sensor Networks” from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf.

[21] Ye, F., Luo, H., Lu, S, and Zhang, L, “Statistical en-route filtering of injected false data in sensor networks”, IEEE Journal on Selected Areas in Communications, Volume 23, Issue 4, April 2005, pp. 839 – 850.

[22] 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.

[23] Hamid, M. A., Rashid, M-O., and Hong, C. S., “Routing Security in Sensor Network: Hello Flood Attack and Defense”, to appear in IEEE ICNEWS 2006, 2-4 January, Dhaka.

[24] Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., and Srivastava, M.B., “On communication security in wireless ad-hoc sensor networks”, 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002, 10-12 June 2002, pp. 139 – 144.

[25] 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.

[26] Du, W., Deng, J., Han, Y. S., and Varshney, P. K., “A pairwise key pre-distribution scheme for wireless sensor networks”, Proc. of the 10th ACM conference on Computer and communications security, 2003, pp. 42-51.

[27] Oniz, C. C, Tasci, S. E, Savas, E., Ercetin, O., and Levi, A, “SeFER: Secure, Flexible and Efficient Routing Protocol for Distributed Sensor Networks”, from http://people.sabanciuniv.edu/~levi/SeFER_EWSN.pdf

[28] Chan, H, Perrig, A., and Song, D., "Random key predistribution schemes for sensor networks", In IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213.

[29] Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.

[30] Karlof, C., Sastry, N., and Wagner, D., “TinySec: a link layer security architecture for wireless sensor networks”, Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004, pp. 162 – 175.

[31] 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.

[32] Roman, R., Zhou, J., Lopez, J., “Applying Intrusion Detection Systems to Wireless Sensor Networks”. July 2006.

[33] Singh, R., Singh, D.K., Kumar, L., “A review on security issues in wireless sensor network”. Journal of Information Systems and Communication, ISSN: 0976-8742 & E-ISSN: 0976-8750, Vol. 1, Issue 1, 2010, PP-01-07

AUTHORS

Mr. Ranjit Panigrahi received his Master degree in Computer Science and Engineering at Sikkim Manipal University in 2013**.** He is currently deputed as Assistant Professor in Department of Computer Sc. & Engineering in Sikkim Manipal Institute of Technology. His area of interests includes Sensor Network Security, Visual Cryptography and Data Mining. He is also a certified Microsoft Technology Specialist.

Dr. Kalpana Sharma, Professor of the Department of Computer Science & Engineering at Sikkim Manipal. Institute of Technology, Majitar, Sikkim, India since August, 1998. She did her BE from National Institute of Technology, Silchar, India and M.Tech from IIT Kharagpur, India. She completed her PhD in the field of Wireless Sensor Network Security. Her areas of research interest are Wireless Sensor Networks, Steganography, Network & Information Security, Real Time Systems and Software Engineering. She has published a number of technical papers in various national and international journals in addition to presentation/ publication in several international/ national conferences.

Prof. (Dr.) M.K.Ghose is currently the Dean (R & D), SMIT and Professor and Head of the Department of Computer Science & Engineering at Sikkim Manipal Institute of Technology, Majitar, Sikkim. His areas of research interest are Data Mining, Simulation & Modeling, Network, Sensor Network, Information Security, Optimization & Genetic Algorithm, Digital Image processing, Remote Sensing & GIS and Software Engineering. Dr. Ghose chaired a number of national/international conference sessions. He has conducted quite a number of Seminars, Workshops and Training programmes in the above areas.