Security Attacks in Wireless Sensor Networks: A Survey

Prachi Dewal, Gagandeep Singh Narula, Vishal Jain and Anupam Baliyan

Abstract Security is one of the major concerns in sensor networks. Wireless sensor network comprises of huge amount of nodes called as tiny sensor nodes. The nodes are required to exchange information with different nodes via wireless links in short intervals. The information may be potentially private regarding people and business processes. These networks suffer from adversary due to distributed behavior and deployment in distant areas. The networks are governed by some constraints at sensor node level like less battery power, less memory capacity, and low transmission range while at network level, they are governed by ad hoc networking and irregular connectivity. The paper analyzes the challenges, main security issues, security breaches in wireless sensor networks and lists their defensive measures.

Keywords Wireless sensor networks (WSN) · Protocols · Security breaches
Security mechanism

1 Introduction

Wireless sensor networks (WSN) are self-configured network with tiny sensor nodes. Each wireless node possesses low energy, memory space, and computational power. Components of sensor node include front end of radio, microcontroller,

P. Dewal (✉) · G. S. Narula
C-DAC, Noida, India
e-mail: prachidewal123@gmail.com

G. S. Narula
e-mail: gagan.narula87@gmail.com

V. Jain · A. Baliyan
Bharati Vidyapeeth's Institute of Computer Applications (BVICAM),
New Delhi, India
e-mail: vishaljain83@ymail.com

A. Baliyan
e-mail: anupam_hod1976@yahoo.co.in

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems
and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_6

main power supply, and sensors. The task of sensors is to monitor physical and environmental conditions such as humidity, pressure, sound, temperature, and many more. After monitoring, they send data to their main location. The data is requested on basis of these parameters in sensor networks (Fig. 1).

Wireless sensor network has resource constraints that act as hindrance in using existing security approaches. In fact, threats in sensor networks in context of routing are susceptible due to simple routing protocols. There are many obstacles in security for example, limited resources, unreliable communication, and unattended operation.

This paper is organized as follows: In Sect. 2, literature survey is presented. Section 3 discusses various protocols for wireless sensor networks. Section 4 gives the security framework discussing standard goals, constraints, obstacles, security breaches, and security mechanism. Finally, concluding the paper in Sect. 5 with conclusion and security threats in different protocol layer along with their defensive measure.

2 Literature Review

The nature of wireless sensor networks includes multiple nodes that make system vulnerable to adverse effects and loss of information. It has led to look into security and privacy aspects of networking by introducing new insistent technologies like wireless sensor networks [1]. Author proposed a security framework for wireless sensor networks, i.e., adaptive security architecture. It includes low-, medium-, and high-level security modes. SENP protocol is used which aims at securing patterns providing authenticity, confidentiality, and integrity. Agent-based secure routing scheme involves use of trusted neighbors that is proposed in [2] which employs use of probability and MAC model for identifying trustworthy neighbors, through which secure routes are set up. The work given in [3] presents a group-based security scheme for wireless sensor networks which includes sequential procedure: Cryptographic key pre-distribution, group-based deployment, secure data aggregation and rekeying. The author in [4] employs use of virtual grid connection to secure data from end to end at multiple base stations. In revocation scheme, random

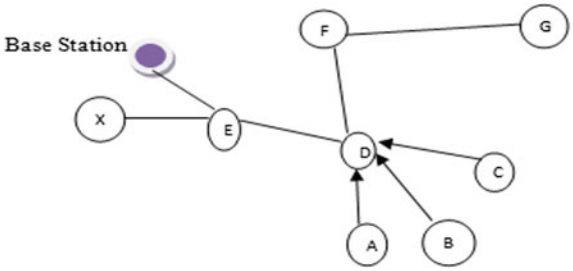

Fig. 1 Sensor network (all other nodes are sensor nodes except base station)

polynomial is used. The author in [5] proposed security protocol for verifying model, i.e., TinySec + LEAP. TinySec holds binary operations, viz., authentication and semantic secured encryption. In [6], author proposed improved fiestal based ciphers for WSN. All of WSN's block ciphers are designed using a 16 round fiestal data block. Author proposes to use controlled permutation boxes for implementation of a fiestal scheme. The author in [7] proposed two secure and efficient data transmission(SET) protocols for cluster-based wireless sensor networks, called SET-IBS and SET-IBOOS, y using the identity-based digital signature(IBS) scheme and the identity-based online/offline digital signature scheme, respectively. In [8], the author presented an architecture utilizing concept of autonomic computing and a simple object access protocol (SOAP) based interface to metadata access points (IF-MAP) external communication layer to create a network security sensor. A flexible two-level communication layer based on autonomic computing and service oriented architecture is presented. In [9], the author proposed an adaptive specification based intrusion detection system (IDS) for detecting malicious unmanned air vehicles (UAVs). An IDS audits UAVs in a distributed system to determine if the UAVs are functioning normally or are operating under malicious attacks. In [10], the author proposed a realistic and reliable IDS architecture for the advanced metering infrastructure (AMI). An AMI system is responsible for collecting, measuring, and analyzing energy usage data and transmitting this information from a smart meter to a data concentrator and then to a headend system in the utility side.

3 WSN Protocols

Protocols are the set of rules and communication standards that must be followed by source and destination in order to communicate with each other. There are several types of communication protocols which can be grouped into the lower level, high-level, and application-based protocols. Example includes TCP/IP that is set of protocols consisting of more than 65,000 protocols (Tables 1 and 2).

Table 1 Protocols associated with different network layers [11]

Layer	Protocol
Physical layer	Sonet, ISDN, SDH
Data link layer	Frame relay, FDDI, Ethernet
Network layer	RIP, OSPF, EGP, IPX, IPV6, ARP
Transport layer	TCP, UDP, SPX
Session layer	NFS, NCP, SMB
Presentation layer	MIME, HTTP, FTP, NNTP
Application layer	DNS, HTTP, POP3, BOOTP, SSH, TELNET

Table 2 Classification of protocols [11]

TCP/IP	IP, TCP, UDP, SMTP, POP3, RIP, FIP, DHCP
Cellular	GPRS, GSM, WAP AND CDMA
VOIP	SPX, RIP, MEGACO, MGCP AND H.323
General	Frame relay, ATM, X.25, PPP

4 Security in WSN

Dimensions of security includes: Goals, obstacles, constraints, security breaches, and security mechanism. All these dimensions are described below.

4.1 Standard Goals

(a) Confidentiality: Confidentiality implies that message or data is not understood by unauthorized personnel, i.e., for security, the information needs to be hidden from unauthorized access. In wireless environment, information is easily available that makes difficult to enforce confidentiality.
(b) Integrity: Unwanted changes can also be created by an interruption in the system. It is not necessarily the result of a malicious act.
(c) Availability: It ensures that the information and the network services need to be available to authorized entities.

4.2 Constraints

In comparison to traditional computer networks, wireless sensor network has many constraints. To develop security mechanisms, it is necessary to understand the resource constraint as given below:

Resource constraint:

(1) Limited Storage: This constraint leads to less storage of data as well as cryptographic keys. It is a challenge to design security protocol that uses at most number of encryption keys for secured network.
(2) Limited Computational power: Computations are based on available amount of power. Due to limited amount of power, computations are constrained. This constraint reduces the computation power of RSA public cryptographic algorithm and makes it expensive to use [11].
(3) Limited Power: Due to lack of wires and small size of sensor nodes, power restriction is there in WSNs. Sensor nodes are battery driven. Power limitation affects security, since encryption algorithm causes communication overhead.

4.3 Obstacles

Obstacles in WSNS include limited resources, untrusted communication, and unattended operation.

(1) Limited Resources: Resource limitation is a big concern is wireless sensor networks. As discussed above there are limited storage, computational power, and power in WSNs.
(2) Untrusted Communication: An untrusted wireless communication channel leads to generation of packet loss and insecurity.
(3) Idle nature of nodes: It may be possible that sensor nodes are left idle for long time depending on the function of a given network. Due to this, these nodes are exposed to attacks.

4.4 Security Breaches

Security in sensor networks posses numerous challenges due to resource and computation constraints. Type of attacks is discussed below:

Attacks based on the protocol layer:

(1) Physical layer: This layer includes the following attacks:

- Jamming: It includes transmission of signal by attacker at base stations with same frequency as of transmitter. It disrupts the radio communication and causes radio interference in the network.

  Defensive measures: A prominent measure to mitigate jamming is use of spread spectrum communication, i.e., frequency hopping spread spectrum (FHSS). It forwards given data by performing swapping of carrier data among different frequency channels [12].

- Tampering: Attacker tries to access hardware apparatus like chips. It involves handling of motes and derives secret information from shared nodes (Fig. 2).

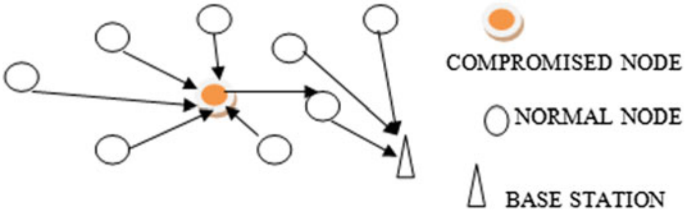

Fig. 2 Tampering attack

Defensive measures: It includes accessing of secret data that lies between external memory chip and microcontroller. This process is called as eavesdropping.

(2) Data link layer: This layer includes the following attacks:

- Collision: When an attacker listens a node transmitting a message, it forwards its own signals to make interferences. It leads to collision when multiple nodes transmit data with same frequency and data rate. It can alter the data and hence data packet can be treated as invalid.

  Defensive measures: Measures applied to jamming attacks can be applied to this attack.

- Exhaustion: Attacker continuously sends data or request over the channel which leads to starvation. The source of origination of attack can be pc or laptop.

  Defensive measures: According to [12], it is possible to reduce the MAC sending rate in order to ignore excessive request from sensor network. It prevents loss of energy as well as allows sensor node to transmit data in shorter time. In this way, nodes get attached to MAC channel for long time.

(3) Network layer: This layer consists of the following attacks:

- Selective forwarding: It includes dropping of packets by malicious node and forward most of the messages.

  Defensive measures: To counterattack multipath routing can be used. This reduces the probability of an attack by adversary. To supervise the system watchdog can be used.

- Acknowledge spoofing: Attacker may spoofs link layer acknowledgements. False error messages are generated by the attacker. Routing loops are created. As a result, end to end latency is increased and network is portioned (Fig. 3).

  Defensive measures: To counterattack all the packets must be encrypted.

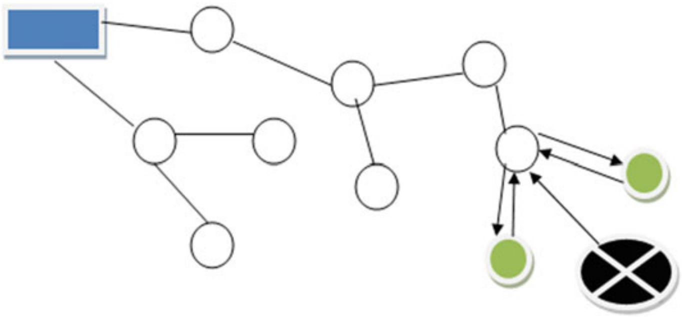

Fig. 3 Acknowledgement spoofing

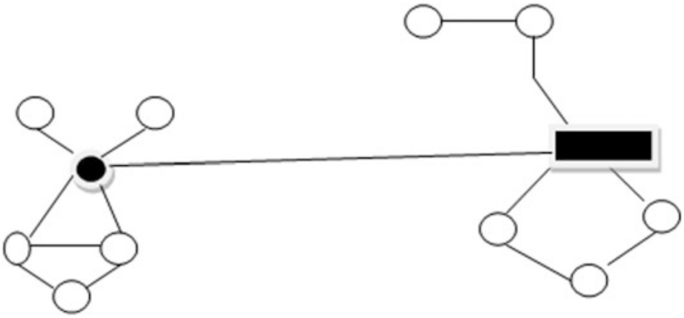

Fig. 4 Black hole attack

- Blackhole attack: Attacker intends to occupy available traffic in a network to a particular node called a black hole which is created in centre. A metaphorical sinkhole is created. All the traffic is directed to fake sinkhole (Fig. 4).

  Defensive measures: A scheme must be implemented so that all the nodes in network must comply with corrupt information produced by invalid nodes. Cryptographic methods can be used.

- Wormhole attack: According to [13], the packets are being received by attacker at specific position, transfers them to different positions and then sending back them into network from that point. The main aim of attacker is to challenge cryptography protection (Fig. 5).

  Defensive measure: To counterattack a four-way handshaking message exchange mechanism is used. Private channel can also be used for protection.

- Sybil: According to [14], self-duplicity property is attached with single node that keeps presence of node in multiple locations. Third parties target these multiple locations and cause problems in distributed storage access, multipath routing and distortion in topology (Fig. 6).

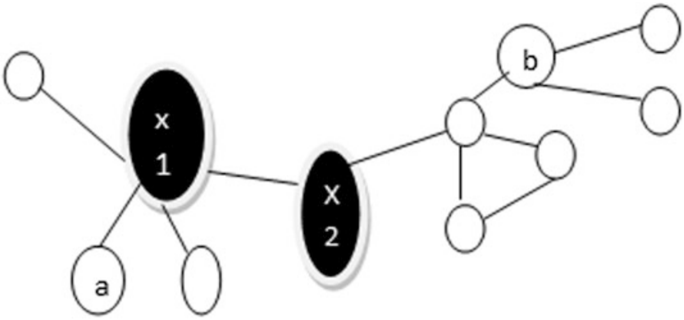

Fig. 5 Wormhole attack

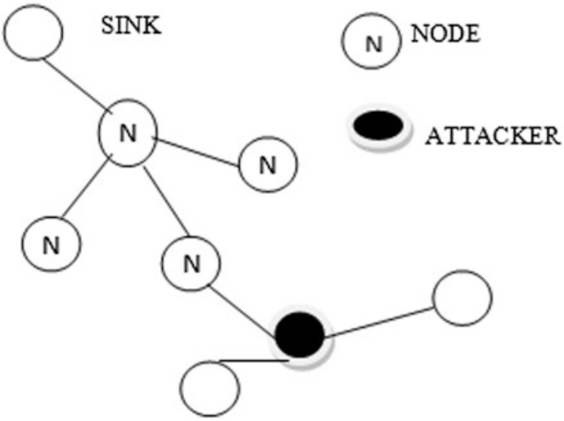

Fig. 6 Sybil attack

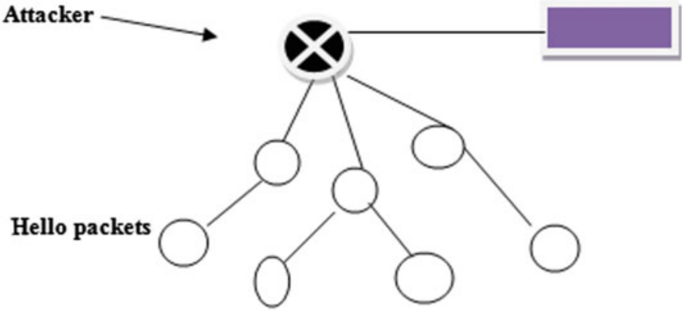

Fig. 7 Hello flood attack

Defensive measures: To counterattack validation technique must be used.

- Hello [15] flood: Attacker sends hello packets from one node to another. Attacker advertises cheap routes which lead to forwarding of messages to attacker (Fig. 7).

  Defensive measure: HELLO FLOOD can be counterattacked by using profile authentication protocol.

4.5 Security Mechanisms in WSN

See Fig. 8.

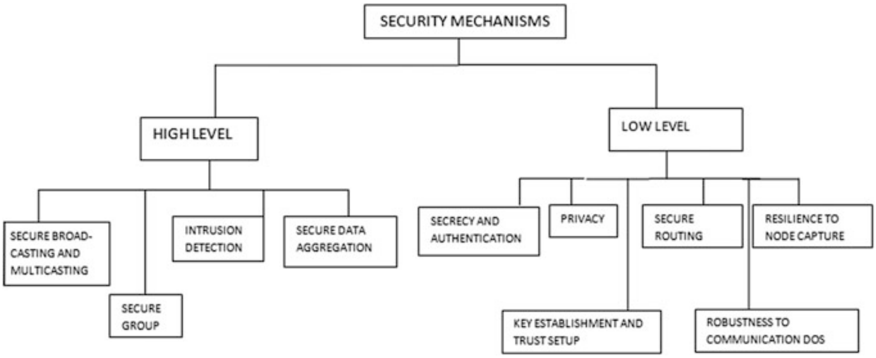
SECURITY MECHANISMS
HIGH LEVEL
LOW LEVEL
SECURE BROAD-CASTING AND MULTICASTING
SECURE GROUP
INTRUSION DETECTION
SECURE DATA AGGREGATION
SECRECY AND AUTHENTICATION
PRIVACY
SECURE ROUTING
RESILIENCE TO NODE CAPTURE
KEY ESTABLISHMENT AND TRUST SETUP
ROBUSTNESS TO COMMUNICATION DOS

Fig. 8 Taxonomy of security mechanisms in WSN [16–22]

5 Conclusion

There is a need for effective security mechanisms in wireless sensor networks. The paper describes constraints, goals, obstacles, and security breaches based on different protocol layers, defensive measures, and security mechanism for wireless sensor networks. The attacks in protocol layer and their measures are shown in Table 3.

Table 3 Security threats in different protocol layers along with their defensive measures

Protocol layer	Security breaches	Defensive measures
Physical layer	Jamming Tampering	Spread spectrum (FHSS) Eavesdrop on the wire which is between memory chip and microcontroller
Data link layer	Collision Exhaustion	Spread spectrum Limit the mac admission control rate
Network layer	Selective forwarding Acknowledgement spoofing Black hole Wormhole Hello flood Sybil	Multipath routing Encryption Cryptographic methods Four-way handshaking scheme Identity verification protocol Validation technique
Transport layer	Flooding Desynchronization	Bidirectional verification Authentication
Application layer	Data aggregation Distortion Clock skewing	Encryption Confidentiality protection Synchronization protocols

References

1. Prasad NR, Alam M (2006) Security framework for wireless sensor networks, Springer
2. Devanagavi GD, Nalini N, Biradar RC (2014) Trusted neighbour based secured routing scheme in wireless sensor networks using agents. Springer, New York
3. Hamid MA, Sarkar AMJ (2011) A group based security scheme in wireless sensor networks. Springer
4. Ferng H-W, Nurhakim J, Horng S-J (2013) Key management protocol with end to end data security and key revocation for a multi-BS wireless sensor network. Springer, New York
5. Tobarra L, Cazorla D, Cuartero F, Diaz G, Cambronero E, Model checking Wireless sensor network security protocols: TinySec + LEAP*, Spain
6. Pazynyuk T, Li J-Z, Oreku GS (2008) Improvrd Feistal based ciphers for wireless sensor network security. J Zhejiang Univ 9(8):1111–1117
7. Huang L, Li J, Guizani M (2014) Secure and efficient data transmission for cluster-based wireless sensor networks. IEEE Trans Parallel Distrib Syst 25(3):750–761
8. Vollmer T, Manic M, Linda O (2014) Autonomic intelligent cyber-sensor to support industrial control network awareness. IEEE Trans Ind Inf 10(2):1647–1658
9. Mitchell R, Chen I-R (2014) Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. IEEE Trans Syst Man Cybern Syst 44(5):593–606
10. Faisal MA, Aung Z, Williams JR, Sanchez A (2015) Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study. IEEE Syst J 9 (1):31–44
11. Stavron E, Wireless sensor network, part 2: limitations. http://webhosting.devshed.com/c/a/Web-Hosting-Articles/Wireless-Sensor-Networks-part-2-Limitations/
12. Fatema N, Brad R (2013) Attacks and counterattacks on wireless sensor networks. Int J Ad-Hoc Sens Ubiquit Comput 4(6):1–15
13. Hu Y-C, Perrig A, Johnson DB (2006) Wormhole attacks in wireless senor networks. IEEE J Sel Areas Commun 24(2):370–380
14. Padmavathi G, Shanmugapriya D (2009) A survey of attacks, security mechanisms and challenges in Wireless sensor networks. Int J Comput Sci Inf Secur 4(1 & 2):1–9
15. Xiong NN, Cheng H, Hussain S, Qu Y (2013) Fault tolerant and ubiquotous computing in sensor networks. Int J Distrib Sens Netw 2013:2. Article ID 524547
16. Christin D, Rosskopf C, Hollick M, Martucci L, Kanhere S (2012) IncogniSense: an anonymity-preserving reputation framework for participatory sensing applications. In: Proceedings of the IEEE international conference on pervasive computing and communications, pp. 135–143
17. Akyildiz I, Su W, Sankarasubramaniam Y, Cayirci E (2002) A survey on sensor networks. IEEE Commun Mag 40:102–114
18. Cristofaro E, Soriente C (2013) Participatory privacy: enabling privacy in participatory sensing. IEEE Netw 27:32–36
19. Erfani S, Karunasekera S, Leckie C, Parampalli U (2013) Privacy-preserving data aggregation in participatory sensing networks. In: Proceedings of the 8th IEEE international conference on intelligent sensors, sensor networks and information processing, pp. 165–170
20. Sharifnejad M, Shari M, Ghiasabadi M, Beheshti S (2007) A survey on wireless sensor networks security. SETIT
21. Cardenas AA, Berthier R, Bobba RB, Huh JH, Jetcheva JG, Grochocki D, Sanders WH (2014) A framework for evaluating intrusion detection architectures in advanced metering infrastructures. IEEE Trans Smart Grid 5(2):906–915
22. Vollmer T, Manic M (2014) Cyber-physical system security with deceptive virtual hosts for industrial control networks. IEEE Trans Industr Inf 10(2):1337–1347

Author Biographies

Prachi Dewal has completed her B.Tech. in Computer Science and Engineering from Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV) University, Bhopal. Now, she is pursuing M.Tech. in Computer Science and Engineering from CDAC, Noida affiliated to GGSIPU. Her research areas include networked systems and algorithms, mobile networking, and wireless sensor networks.

Gagandeep Singh Narula received his B.Tech. in Computer Science and Engineering from Guru Tegh Bahadur Institute of Technology (GTBIT) affiliated to Guru Gobind Singh Indraprastha University (GGSIPU), New Delhi. Now, he is pursuing M.Tech. in Computer Science from CDAC Noida affiliated to GGSIPU. He has published various research papers in various national, international journals, and conferences. His research areas include Semantic Web, information retrieval, data mining, cloud computing, and knowledge management. He is also a member of IEEE Spectrum.

Vishal Jain has completed his M.Tech. (CSE) from USIT, Guru Gobind Singh Indraprastha University, Delhi and doing Ph.D. in Computer Science and Engineering Department, Lingaya's University, Faridabad. Presently, he is working as Assistant Professor in Bharati Vidyapeeth's Institute of Computer Applications and Management, (BVICAM), New Delhi. His research area includes Web technology, Semantic Web, and information retrieval. He is also associated with CSI, ISTE.

Dr. Anupam Baliyan has completed his Ph.D. in Computer Science & Engineering from Banasthali University and M.Tech. in Computer Science & Engineering. His research area includes wireless network, routing in ad hoc network, and quality of services in delay-tolerant network. He published more than 10 research papers in various international journals and guided more than 100 students for their M.Tech. Dissertation. Presently, he is working as Associate Professor in Bharati Vidyapeeth's Institute of Computer Applications and Management, (BVICAM), New Delhi. He is also associated with CSI and ISTE.