International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 2, 2019 (Special Issue)
© Research India Publications. http://www.ripublication.com

Security Requirements and Attacks in Wireless Sensor Networks

Anuj Kumar Singh
Department of Computer Science
Amity University Haryana
Gurgaon, India

B.D.K.Patro
Department of Computer Science
Rajkiya Engineering College, Kannauj
Kannauj, India

***Abstract*—Today's computing environment has become highly ubiquitous defined by the phrase anytime anywhere computing. With the growth of Internet of Things the integration of different computing platforms has evolved. Wireless Sensor Networks (WSN) is a technology which provides computing in harsh and hostile environments. In this paper the main focus is on the security of WSNs. The paper has been divided into three sections, first section provides a general introduction of WSNs and their working principle. The security requirements of WSNs have been discussed in detail in the second section of the paper. The third and last section of the paper provides the description of all kinds of attacks made on to a WSN. This section also reveals the countermeasures of the attacks in WSN.**

Keywords—Security Requirement, Attacks, Wireless Sensor Networks

I. INTRODUCTION

Wireless Sensor Network (WSN) is a group of dedicated sensors scattered spatially for monitoring and capturing the physical conditions of a particular environment or location. WSN collects the data and organize it at a central location. The data is collected with the help of wireless sensors called nodes, which consist of radio transceiver, antenna, microcontroller, and a power source. The typical architecture of a WSN [7] is shown in Fig. 1.

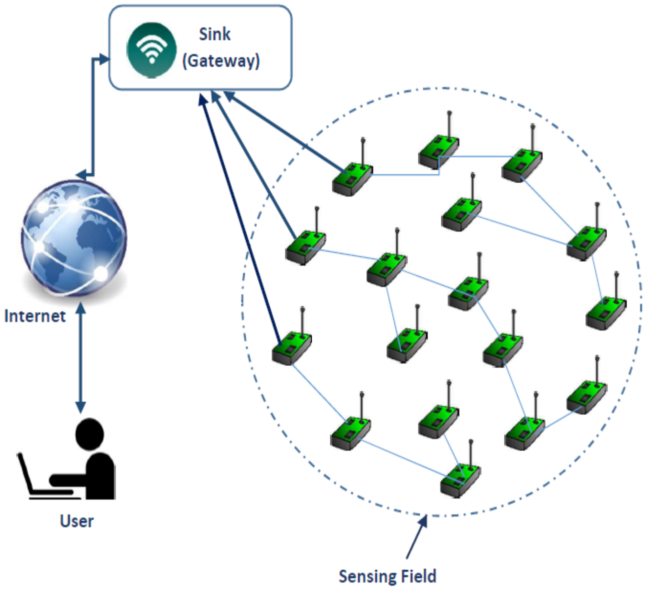

Fig. 1. Generic architecture of WSN.

The WSN uses a gateway also known as sink to provide connectivity between wired network and the distributed wireless sensors. The data is collected by the sensors is sent to the gateway which in turn send it to the user through a network or Internet. The application areas of WSN include military, healthcare, environment, robotics, medical, industrial, and many more. Due to the involvement of wireless communication, security in WSNs has been a primary concern for the researchers as WSNs suffer from three constraints – limited computational capability, limited power and unreliable communication.

A. *Limited Computational Capability*- The computational capability of a sensor node is very limited, typically having a few 10s MHz CPU clock, flash memory upto 1 MB, and few 100s MB RAM. With these specifications it is very challenging to implement security schemes providing adequate security.

B. *Limited Power*- Sensor nodes operate on power source, typically a battery. To ensure availability of the node, the battery power must not be spent on unnecessary heavy computations. Security schemes for WSN should be designed in a way that the operations within these scheme consume vry less power.

C. *Unreliable Communication* – Since the sensors communicate in an open wireless environment, there is a need of much stronger security mechanisms to thwart all kinds of attacks in an efficient manner.

Due to these constraints it has been a continuous challenge to implement lightweight security mechanisms for WSN which provide all the necessary security attributes at the same time providing protection from various attacks on WSN. Therefore, it is important to analyze the security requirements of WSNs and taxonomy of attacks on WSNs which have been discussed in the next section.

II. SECURITY REQUIREMENTS OF WSNS

The four major security attributes that any system should have are – confidentiality, authentication, integrity and non-repudiation. But, in a wireless environment there is a need of implementing more security features. J.Lopez et al. [1] have carried out a comprehensive survey on the security of WSNs and pointed out the security requirements of a WSN. According to them in a WSN security features including confidentiality, integrity, authentication, availability, authorization, data freshness, self-organization, forward security, and non-repudiation should be implemented efficiently to make it secure. A.Gaware and S.B.Dhonde [4] have divided the security requirements of WSNs in two broad categories – primary requirements and secondary requirements which have been shown in Fig. 2.

A. *Confidentiality* – The data collected by the sensor nodes must be communicated to the gateway in a secure manner i.e. no other party must be able to understand the same. Data confidentiality can be implemented by using appropriate encryption algorithms.

B. *Integrity* – The data received by the sensor nodes and gateway must not be altered, deleted and tampered during the transmission.

C. *Authentication* – It is the assurance that the data received was sent by the right sender. All the parties involved in the communication must authenticate each other before sending or receiving the data.

D. *Availability* – The data at every node must be available all the time. To ensure availability the sensor nodes must be protected from attacks like denial of service and single point failure. Furthermore, the nodes must not perform heavy computations as this may lead to shortage of power which in turn may lead to unavailability [8].

E. *Authorization* – Only authorized nodes must be able to perform designated operations within the network. The members of the network need to have a proper authorization in order to perform certain tasks.

F. *Data Freshness* – WSNs are data centric network as the reliability of WSNs depends on the collection of correct data without delay. Therefore it must be ensured that data produced bt WSNs is recent. Data freshness have two dimensions, first is collecting data without delay and second to ensure that it is not forged.

G. *Self Organization* - Sensor nodes in the WSNs must be autonomous and flexible enough to independently react against problematic circumstances, organizing and healing themselves. Therefore, it is anticipated that all potential problems that may occur should be detected and prevented without any possibility of error.

H. *Forward and Backward Security* – When a new sensor node is installed in place of the failed node it must not be able to read past messages. Similarly the leaving node must not be able to read future messages of the network.

I. *Non-Repudiation* - A sensor node in the WSN can not deny after sending/receiving a message.

III. ATTACKS ON WSNS

WSNs are vulnerable to different threats and attacks. Some of them are very serious as WSNs work in harsh and hostile areas. Broadly the attacks on WSNs can be divided into two categories namely passive attacks and active attacks [2]. Passive attacks involve traffic analysis, monitoring, and eavesdropping and do not involve modification in the data stream. Active attacks involves modification in the data stream sent or received. These attacks include injecting false messages, impersonating, overloading, unauthorized access etc. A.R.Dhakne and P.N.Chatur [3] have given the detailed analysis and divided the attacks on WSNs in five categories based on different perspectives, layers, authentication, privacy and others. The taxonomy of attacks on WSNs has been shown in Table. 1.

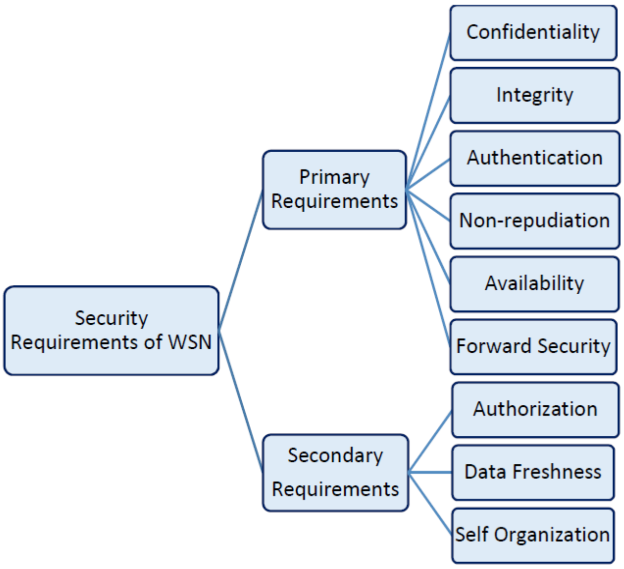

Fig. 2. Security requirements of WSNs.

TABLE 1. TAXONOMY OF ATTACKS ON WSNS

Category of Attack	Specific Attack
Attacks based on different perspectives	Outsider vs Insider
	Passive vs Active
	Node Capture Attack
Attacks on Layers	Physical Layer Attacks (Jamming, Tampering, Path based DoS)
	Link Layer Attacks (Collision)
	Network Layer Attacks (Black Hole, Sybil, Spoofing, Sinkhole, Wormhole, Hello Flood)
	Transport Layer Attacks (Flooding, Desynchronization)
	Application Layer Attacks
Attacks on Secrecy & Authentication	Node Replication
Attacks on Privacy	Eavesdropping
	Traffic Analysis
Other Attacks	Bad/Good Mouthing
	On-Off

A. *Outsider and Insider Attack* – In outsider attack an external sensor node is deployed in the WSN to be attacked. This external node does not have cryptographic keys or access to security parameters of the WSN. In insider attack the security of an internal sensor node is compromised to penetrate the security of the network.

B. *Passive and Active Attacks* – Passive attacks monitors the traffic and tries to find out information about the messages. Theay do not alter the messages in transit. In contrast active attacks modify the message contents or inject false messages into the network.

C. *Node Capture Attack* – In this attack the attacker gets full physical access to a sensor node and from this point the attacker tries to obtain confidential information or damage the network.

D. *Physical Layer Attacks* – In remote locations the attacker make attacks on to the physical layer. The mot common physical layer attacks are jamming and tampering.

1.) *Jamming* - If the attacker has the knowledge about the wireless transmission frequency of WSN then this attack can be easily implemented by the attacker. A powerful jamming source is capable of creating traffic in the entire network, whereas less powerful jamming source is only able to disturb a smaller portion of the network. In this attack attacker send a signal to interfere with signal sent by some another node in the network.

2.) *Tampering* – In this attack a sensor node can get altered by a fake node or modify the node with some undesirable functionalities so that attacker can easily get confidential data and information.

E. *Link Layer Attacks* – Node outage is a situation when a sensor node stops its proper functioning. It becomes more serious when node outage occurs for a cluster node. In link layer attack the attacker tries to outage a functioning node in the network. Collision is another link layer attack in which the adversary tries to overload a particular channel so that collisions occur.

F. *Network Layer Attacks* - Awareness of location, power efficiency, addressing and to make sensor network more data centric, network and routing layer plays an important role. On netwrok layer the attackers perform different kind of attacks which have been highlighted in this sub-heading.

1.) *Black Hole Attack* – In this attack a node is forced to drop some or all the packets it receives.

2.) *Sybil Attack* – In this attack a node shows different identities to other nodes in the network. This attack upsets the functioning of routing protocols implemented in the network.

3.) *Sinkhole Attack* – In sinkhole attack the adversary targets an internal node of the network and make the node attractive so that all the other nodes forward their packets to the attacked node only [9].

4.) *Worm Hole Attack* – A warm hole attack occurs when a node at one end forwards packets to a node at other end through a tunnel and the node at other end replays these packets [9].

5.) *Hello Flood Attack* - In this type of attack the adversary sends a hello message to all surrounding nodes by using powerful transmitter and all other nodes that are not in the range of the radio signals think that the sender is in the radio range. This illusion makes node to send packets to the attacker node rather than to base station.

G. *Transport Layer Attacks* – The transport layer is responsible for end-to-end communication between the sending node and the receiving node. The two attacks made on to the transport layer in WSNs are flooding and desynchronization.

1.) *Flooding* – In flooding a source node is attacked by the adversary in a way that it receives many requests repeatedly and its memory becomes full. In this situation the source node rejects all the requests including the requests from genuine nodes in WSN.

2.) *Desynchronization* – In this attack, the connection between two sensor nodes get disrupted by the transmission of illegitimate fake sequence number or control flags in messages. Due to this, other nodes transmitting messages will waste their time and energy due to lack of synchronization.

H. *Application Layer Attacks* – All the data and information is available on application layer. Leaking confidential information at application layer can affect the working of the whole WSN. Localized Encryption and Authentication Protocol (LEAP) can verify whether a node has been compromised or not and if it is compromised then it can revoke that node by some efficient mechanism [5].

I. *Attacks on Secrecy and Authentication* – The main attack under this category is node replication attack. In node replication attack the adversary tries to duplicate the identity of a node by copying identifier of the another node. These duplicate identity nodes can disrupt the working of mrtwork by giving wrong or false information and erroneous routes to another node. This can lead to partitioning of the the network as it will lead to communicate false readings of sensor nodes to another sensor nodes.

J. *Attacks on Privacy* – The privacy of a node is compromised by eavesdroppind and traffic analysis. If the information has not been encrypted then an attacker can see and analyze the data. Even if the data sent is encrypted then also by using different tools and techniques the secret information can be revealed.

K. *Other Attacks* – Other attacks in WSNs focus on availability of servise and sometimes these occur to misguide the behaviour of neighbouring sensor nodes.

L. *Bad Mouthing and Good Mouthing Attack* – In bad mouting and good mouthing attack the attacked node always provides false information about the neighbouring nodes. When this false information is used in determining trust value for the nodes and cluster it leads to incorrect results.

M. *On-Off Attack* - In this kind of attack a node is made to work good or bad according to the situation.The node is then used to improve trust values of the other malicious sensor nodes.

Due to the importance of WSNs in a variety of crtitical applications the attackers have been continously targeting these networks to steal confidential information or to damage them. Therefore, it is utmost important to secure WSNs from different threats and attacks made on to them. The countermeasure of attacks [6,10,11] described in section III of the paper has been publicized in Table 2.

TABLE 2. ATTACKS ON WSNS AND THEIR COUNTERMEASURE.

S.No.	Attack	Countermeasure
1	Outsider	Strong authentication mechanism
2	Insider	MAC using shared secret key
3	Node Capture	Building a secure zone, Cryptographic fingerprinting
4	Jamming	Spread spectrum technologies, Polarization of antenna
5	Tampering	Building a secure zone, using sealed tamper resistant case
6	Collision	Frequency hopping
7	Blackhole	Strong authentication mechanism
8	Sybil	Use of ID based symmetric and location based key
9	Sinkhole	Geographic routing protocol
10	Warmhole	Directional antennas, pocket leashes and topology checking by server
11	Hello Flood	Mutual authentication
12	Flooding	Strong authentication mechanism
13	Desynchronization	Spending session tokens
14	Application Layer	LEAP protocol
15	Node Replication	Authentication through base station, location confirmation by neighboring nodes
16	Eavesdropping	Encryption of data and messages
17	Traffic Analysis	Encryption of data and messages with block chaining
18	Good/Bad Mouthing	MAC using shared secret key
19	On-Off	Symmetric authentication using shared key, Hash-lock

IV. CONCLUSION

Wireless sensor networks have a great significance in today's computing world as many critical applications are relying on them.Therefore security of WSNs is a big concern for the researchers. This paper has explained two important security aspects of WSNs. First the security requirements of WSNs have been discussed and second taxonomy of attacks on WSNs has been revealed. Furthermore, this paperprovides a glimpse of countermeasures to different attacks on WSNs. The work presented in this paper has a significance for the students, researchers and professionals working in the area of security of WSNs.

REFERENCES

[1] J.Lopez, R.Roman, and C.Alcaraz, "Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks", in Foundations of Security Analysis and Design V. Lecture Notes in Computer Science, Vol. 5705, A.Aldini, G.Barthe, R.Gorrieri Eds., Springer, Berlin, 2009, pp. 289-338.

[2] P.Asha, T.Mahalakshmi, S.Archana, and S.C.Lingareddy, "Wireless Sensor Networks: A Survey on Security Threats Issues and Challenges", International Journal of Computer Science and Mobile Computing, Vol.5 (5), pg. 249-267, 2016.

[3] A.R.Dhakne and P.N.Chatur, "Detailed Survey on Attacks in Wireless Sensor Network", Proc. of International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systems and Computing, Singapore, 2017 pp. 319-331.

[4] A. Gaware and S.B.Dhonde, "A survey on security attacks in wireless sensor networks", Proc. of 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp 536-539, 2016.

[5] Z.Tanveer and Z.Albert, "Security issues in wireless sensor networks", Proceedings of the International Conference on Systems and Networks communication (ICSNC'06), Washington, DC, USA, IEEE Computer Society, 2006..

[6] F.Shahzad, M. Pasha, and A.Ahmad, "Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures", International Journal of Computer Science and Information Security , Vol. 14, No. 12, pp 54-65, 2016.

[7] A.Rani and S. Kumar, "A survey of security in wireless sensor networks", Proc. of 3rd International Conference on Computational Intelligence & Communication Technology (CICT), pp. 1-5, 2017.

[8] X.Q.Chen, K.Makki, Y.Kang, and N.Pissinou, "Sensor network security: a survey", IEEE Commun. Surv. Tutor., vol. 11, no. 2, pp. 52-73, 2009.

[9] J. Grover, S.Sharma, "A review on security issues in wireless sensor networ Security issues in Wireless Sensor Network — A review", IEEE Conf-ICRITO, pp. 397-404, 2016.

[10] Y. Li, L. Qin and Q. Liang, "Research on wireless sensor network security," Computational Intelligence and Security, pp. 493-496, 2010.

[11] A. Jain, K. Kant, and M.R. Tripathy, "Security solutions for wireless sensor networks", Proc. of IEEE Second International Conference on Advanced Computing and Communication Technologies, pp. 430-433, 2012.