A STUDY ON WIRELESS SENSOR NETWORK CHARACTERISTICS AND SECURITY CHALLENGES

D.Sudhakar[1] , Dr.V.S.Meenakshi[2]

[1]Asst.Prof, Department of Computer Science, Bishop Appasamy College of Arts and Science, Coimbatore, (India)

[2]Asst.Prof, PG & Research Department of Computer Science, Chikkanna Govt. Arts College, Tirupur. (India)

ABSTRACT

Wireless Sensor Networks (WSNs) and its application domains are gaining more importance in the current scenario due to their flexibility, ease of deployment, self-adoptational ability of the environment and minimal of their establishment cost. However, the growing demand of WSN applications has drastically increased the secured infrastructure, which has become a critical issue. Hence, solutions are required to minimize the impact of attackers on the application environment. In order to design such solutions, deep analysis of WSN is required with respect to their base characteristics efficiency. Thus, this paper discusses on various elements of Wireless Sensor Networks which contribute to the total security issues and how it is addressed. This paper also discuss the implication of few of these solutions for future research directions to enable efficient and secure WSNs

***Keywords:* Attacks on secrecy and authentication, layer wise attacks, security, security requirements, Wireless Sensor Networks**

I.INTRODUCTION

A Wireless Sensor Network is a group of specialized transducers with communications network infrastructures for monitoring and recording conditions at diverse locations. Fig.1 shows the general diagram of WSN. Potential applications of sensor networks include i) Industrial automation, ii) video surveillance iii) Traffic monitoring iv) medical device monitoring v) Monitoring of wealth conditions vi) Air traffic control vii) Robot control and in various applications used in military related services. Commonly monitored parameters are temperature, humidity, pressure, wind direction, speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentration, pollution levels and vital body functions.

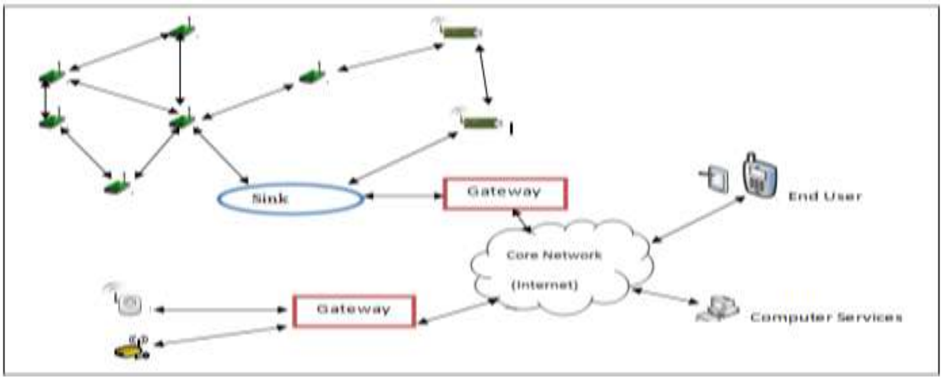

Figure 1. A general diagram of WSN

II.CHARACTERISTICS OF WSN

The fundamental characteristics of WSN depend on various aspects due to its architectural nature of applications where it is deployed. Those are:

Large Scale: Geographical coverage of large area is required in general applications of WSNs.

Limited Resources: Requirement in WSNs must be with low installation and operation cost necessitates that sensor nodes should have simple hardware. Hence the operation and communication resources in WSNs are very limited. Every protocol must be designed taking into account limitations in processor capacity, memory and radio communications.

Redundancy: Each event in the network is detected by the multiple sensor nodes because of the node redundancy and therefore increases the amount of data to be transferred over it. To get rid of data redundancy, clustering protocols may be used.

Security: WSN applications like military systems and medical monitoring systems are very sensitive in terms of security. Due to the limited resources of sensor nodes, traditional security mechanisms cannot be used in WSNs.

III. SECURITY REQUIREMENTS AND SECURITY GOALS OF WSN

The security requirements of WSNs are mandate in data integrity, data confidentiality, data availability, authentication [1] through which the WSNs can achieve the security goals such as secure localization, data freshness, self-organization, time synchronization. Fig.2 shows the security requirements and goals of WSN.

3.1 Security requirements of WSN

3.1.1 Data Integrity: Data integrity ensures that the message transmitted in the sensor network will not be altered during communication. A suspicious unauthorized node can cause the network to work improperly by disrupting the message without letting its presence known to other nodes involved in communication. Thus, it is very important to set message authentication code or cyclic codes to ensure data integrity. The mechanism should ensure that no message can be altered by an entity as it traverses from the sender to the recipient.

3.1.2 Data Confidentiality: The security mechanism in WSN should ensure that no message in the network is accessed by anyone except intended recipient. In a WSN, the issue of confidentiality should address the following requirements [2]: (i) a sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so, (ii) key distribution mechanism should be extremely robust, (iii) public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks. A sensor node should not rely on the data derived from the environment to its neighbors. In addition routing data also be kept secret against malicious nodes because these nodes can exploit data and reduce performance of network.

3.1.3 Data Availability**:** Availability denotes the capability of WSN in sustaining its service continuity even in the presence of internal or external attacks such as a denial of service.

3.1.4 Authentication: It ensures that the communicating node is the one that it claims to be. Since WSNs use public wireless environment they need authentication mechanisms to pick up messages and deceptive packets that come from malicious nodes. Authentication mechanisms aid a node in verifying the identity of a node that it is in contact with. An adversary can not only modify data packets but also can change a packet stream by injecting fabricated packets. It is, therefore, essential for a receiver to have a mechanism to verify that the received packets have indeed come from the actual sender node. In case of communication between two nodes, data authentication can be achieved through a message authentication code (MAC) computed from the shared secret key. Transmitter and receiver can compute the verification code of all the messages sent by a common hidden key.

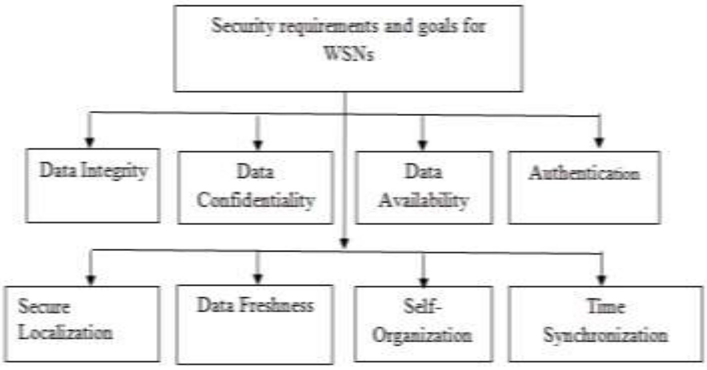

Figure 2. Security requirements and goals for WSNs

3.2 Security goals of WSN

3.2.1 Secure localization: It is very essential to locate the nodes accurately and automatically in a WSN in many situations. If the location information of the sensor nodes is not secured properly a potentially adversary node can easily generate and provide false location information by reporting false signal strength, The position of a device is accurately computed from a series of known reference points in verifiable multi-alteration (VM) technique which uses authenticated ranging and distance bounding to ensure accurate location of a node. An attacking node can only increase its claimed distance from a reference point due to the use of distance bounding,. The attacker would also have to prove that its distance from another reference point is shorter to ensure location consistency. As it is not possible for the attacker to prove this, it is possible to detect the attacker. [3].

3.2.2 Data Freshness: In WSN structures, it is possible that an attacker can retransmit the copy of old key as the new key is being refreshed and propagated to all the nodes in the WSN. It is therefore important to check that the data is new. A time-specific counter may be added to each packet to check the freshness of the packet. A time-specific counter may be added to each packet to check the freshness of the packet.

3.2.3 Self-Organization: Each node in a WSN should be self-organizing and self-healing. The dynamic nature of a WSN makes it sometimes impossible to deploy any pre-installed shared key mechanism among the nodes and the base station [4]. The nodes in a WSN need to be self-organized by themselves for routing as well as to carry out the key management[5] and for developing trust relations.

3.2.4 Time synchronization: Most of the applications in sensor networks require time synchronization. Any security mechanism for WSN should also be time-synchronized. A collaborative WSN may require synchronization among a group of sensors.

IV. TYPES OF ATTACKS TOWARDS WSNS

WSNs are exposed to various types of attacks. These attacks can be usually classified into following types [6]:

(i) Passive attacks

(ii) Active attacks.

In passive attacks, attackers are usually secret and intend to observe the message link to gather the data. In active attacks, attackers affect the operations of the network. Network services may put down or terminates as a result. The attack could be accomplished from inside, outside, or both, the network.

These attacks may affect the data with one of the following threat [7]

(i) Interruption: It is an attack on the network’s availability. It mainly cause system assets unavailable or out of use.

(ii) Interception: It is an attack on confidentiality. In this type of attack, attacker tries to compromise the network to gain illicit access to the node or data store on it.

(iii) Modification: It is an attack on system’s integrity. In this type of attack the illicit party not only accesses the data but also change the message content.

(iv) Fabrication: It is an attack on authentication. The attacker makes an inclusion of messages in the network and consider as it is received from an unauthorized node.

4.1 Categories of attacks

Broad categories of these attacks are as follows

i) Attacks on secrecy and authentication: Standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks

ii) Stealthy attack against service integrity: In this attack, the goal of the attacker is to make the network accept a false data value. An attacker compromises a sensor node and injects a false data value through that sensor node.

iii) Attacks on network availability: these attacks are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.

4.1.1 Attacks on secrecy and authentication

There are different types of attacks under this category

i) Node replication attack: In a node replication attack, an attacker attempts to add a node to an existing WSN by replication (i.e. copying) the node identifier of an already existing node in the network [8]. A node replicated and joined in the network in this manner can potentially cause severe disruption in message communication in the WSN by corrupting and forwarding the packets in wrong routes.

ii) Attacks on privacy: Privacy preservation of sensitive data in a WSN is particularly a difficult challenge [9]. An adversary may gather seemingly innocuous data to derive sensitive information. if he knows how to aggregate data collected from multiple sensor nodes. This is in analogy to the panda hunter problem, where the hunter can accurately estimate the location of the panda by systematically monitoring the traffic [10]. The privacy preservation in WSNs is even more challenging since these networks make large volumes of information easily available through remote access mechanisms. Remote access allows a single adversary to monitor multiple sites simultaneously [11].

iii) Eavesdropping and Passive monitoring: This is most common and easiest form of attack on data privacy. If the messages are not protected by cryptographic mechanisms, the adversary could easily understand the contents. Packets containing control information in a WSN convey more information than accessible through the location server

iv) Traffic analysis: In order to make an effective attack on privacy, eavesdropping should be combined with a traffic analysis. Through an effective analysis of traffic, an adversary can identify some sensor nodes with special roles and activities in a WSN[12]. For example, a sudden increase in message communication between certain nodes signifies that those nodes have some specific activities and events to monitor. Deng et al have demonstrated two types of attacks that can identify the base station in a WSN without even underrating the contents of the packets being analyzed in traffic analysis [13].

4.1.2 Attack on Integrity

Camouflage: An adversary may compromise a sensor node in a WSN and later on use that node to act as a normal node in the network. This camouflaged node then may advertise false routing information and attract packets from other nodes for further forwarding. After the packets start arriving at the compromised node, it starts forwarding them to strategic nodes where privacy analysis on the packets may be carried out systematically.

4.1.3 Attacks on network availability

Comparable to any wireless network, WSNs are suffering from many different attacks. Layer wise major attacks to WSNs are as follows [14]

i) Physical Layer attacks

Jamming: One of the attacks interfering with the radio frequencies that a network's nodes are using is jamming. An attacker may continuously transmit radio signals on a wireless channel. This may lead to Denial-of-Service attacks at this layer. [15][16]

Tampering: Tampering is another type of physical layer attack. If a physical access is given to a node, an attacker can draw sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node controlled by the attacker.

ii) Data Link Layer attacks

The functionality of Data link layer protocols is to coordinate neighboring nodes to access shared wireless channels and to provide link abstraction to upper layer. The possible attacks are

Collision: A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. A typical defense against collisions is the use of error-correcting codes.

Exhaustion: Repetitive collisions can also be made use of by an attacker to cause resource depletion. A feasible solution is to impose rate limits to the MAC admission control such that the network can disregard excessive requests.

Unfairness: Instead of blocking access to a service outright, an attacker can degrade it in MAC protocol [17] to miss their transmission deadline. Using small frames reduces the effect of such attacks by decreasing the amount of time with which an attacker can take hold of the communication channel.

iii) Network Layer attacks

Selective Forwarding: A malicious node attempts to block the packets in the network by rejecting to forward or drop the messages passing through them. In addition, the malicious node may send the messages to the wrong path so that it can create unfaithful routing information in the network

Sinkhole Attack: The intent of the adversary is to attract almost all the traffic from a certain area by means of a compromised node, creating a metaphorical sinkhole with the enemy at the center.

Sybil Attacks: A single node duplicates itself and is presented in more than one location. The Sybil attack aims at fault tolerant schemes

Wormholes Attacks: In a wormhole attack, an attacker gets packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point[18].

HELLO Flood Attacks: A large number of protocols utilizing HELLO packets naively assume that receiving such packets means that the sender is within the radio range and is therefore a neighbor. An attacker may use a high-powered transmitter to deceive a large area of nodes into believing they are neighbors of that transmitting node

iv) Transport Layer attacks

Flooding: An attacker may make new connection requests over and over until the resources required by each connection are depleted or reached a maximum limit.

Desynchronization: The adversary repetitively pushes messages which convey sequence numbers to one or both of the endpoints.

v) Application Layer attacks

The type of attacks can be carried out in this layer such as overwhelm, repudiation, data corruption and malicious code. In overwhelm attack an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. Thus attack consumes network bandwidth and drains nodes energy.

TYPES OF ATTACKS	NAME OF THE ATTACK	INSIDE	OUTSIDE
Active attacks	Node Replication		✓
	Desynchronization		✓
	Denial-of-service(DoS)	✓	✓
	Jamming		✓
	Collision		✓
	Sybil	✓	
	Wormholes	✓	✓
	Sinkhole	✓	
Passive Attacks	Eavesdropping and passive monitoring		✓
	Camouflage		✓
	Tampering		✓
	Exhaustion	✓	

	Traffic analysis		✓
	Unfairness		✓
	Selective Forwarding	✓	
	HELLO Flood	✓	
	Flooding	✓	

The various attacks are tabulated and shown in TABLE 1.

Table1: Common types of security attacks in WSNs (sources[7][19][20])

V.CONCLUSION

With the advances in Computer Networking there is a growing curiosity in the usage of WSN. Protection is an imperative challenge in WSNs. Without the basic requirements like data confidentiality, data integrity, data availability and data freshness, many actual real-time applications of WSNs becomes ineffective. This paper describes various characteristics and security requirements and type of attacks exits under WSN environment. This paper also describes security challenges in WSNs, which differ from the ad hoc networks in terms of energy, computation capabilities and communications. Thus, it is necessary to develop a security solution which conforms to every aspect of the security requirements of WSN, but by taking into account the idea of high security and low power consumption for each requirement.

REFERENCES

[1]. Gupta Sunil, K Harsh, A L Sangal Verma, "Security Attacks & Prerequisite for Wireless Sensor Networks", *International Journal of Engineering and Advanced Technology (IJEAT), vol. 2,* June 2013.

[2]. Perrig, A., R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. “SPINS: Security Protocols for Sensor Networks.” Wireless Networks, 8 (5): 521-534, 2002.

[3]. Capkun.s and J.P Hubaux, “Secure positioning in wireless networks”, *IEEE Journal on selected area in Communication, 28.11.2006,* Jeon,Seungwoo.

[4]. Eschenauer L., and V. D. Gligor.. “A Key-Management Scheme for Distributed Sensor Networks.” In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS’02), 41-47, November 2002Washington DC, USA.

[5]. Qusay Idrees Sarhan, "Security Attacks and Countermeasures for Wireless Sensor Networks: Survey", *International Journal of Current Engineering and Technology, vol. 3, no. 2, June 2013*

6 Yassine Malleh, Abdellah Ezzati, "A Review of security attacks and intrusion detection schemes in Wireless Sensor Networks", *International Journal of Wireless & Mobile Networks (IJWMN), vol. 5, no. 6, December 2013.*

[7]. Santar Pal Singh, S. C. Sharma, “Secure Clustering Protocols in Wireless Sensor Networks”, *Journal of Wireless Sensor Networks 2016, 3, 1-0013, ISSN: 2001-6417*

[8]. Parno, B., A. Perrig, and V. Gligor. "Distributed Detection of Node Replication Attacks in Sensor Networks." In Proceedings of the IEEE Symposium on Security and Privacy (S&P'05), 49-63, Oakland, California, USA, May 2005

[9]. Gruteser, M., G. Schelle, A. Jain, R. Han, and D. Grunwald. "Privacy-Aware Location Sensor Networks." In Proceedings of the 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX), Vol 9, 28, Lihue, Hawaii, USA, May 2003.

[10]. Ozturk, C., Y. Zhang, and W. Trappe. "Source-Location Privacy in Energy-Constrained Sensor Network Routing." In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04), 88-93, Washington DC, USA, October 2004.

[11]. Chan H., and A. Perrig. "Security and Privacy in Sensor Networks." IEEE Computer Magazine, 36 (10): 103-105, 2003.

[12]. Abdul Wahid, Pawan Kumar, "A survey on Attacks Challenges and Security Mechanisms in Wireless Sensor Network", *International Journal for Innovative Research in Science & Technology, vol. 1, January 2015.*

[13]. Deng, J., R. Han, and S. Mishra. "Countermeasures against Traffic Analysis in Wireless Sensor Networks." Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.

[14]. Murat Dener .,"Security Analysis in Wireless Sensor Networks". *International Journal of Distributed Sensor Networks, Volume 2014, Article ID 303501, 23 October 2014*

[15]. W.Xu et al, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", MobilHoc '05 Proc, 6th ACM International Symposium on Mobile AdHoc Networks and Comp, pp 46-57, 2005

[16]. W. Xu W.Trappe and Y Zhang,"Channel surfing Defending Wireless Sensor Networks from Interference" in Proceedings of Information Processing in Sensor Networks,2007.

[17]. Yanli YuKeqiu Li, Wanlei Zhou and Ping Li "Trust mechanisms in wireless sensor networks attack analysis and countermeasures", *Journal of Network and Computer Applications, Elsevier, 2011.*

[18]. T. K. Rao, M. Sharma, and M. V. Saradhi, "Wormhole attacks in Ad-Hoc networks," *International Journal of Latest Trend in Computing, vol. 4, no. 2, 2013.*

[19]. Jyoti Shukla, Babli Kumari, "Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview", International Journal of Application or Innovation in Engineering & Management (IJAIEM), *vol. 2, March 2013.*

[20]. K. Venkatraman, J. Vijay Daniel, and G. Murugaboopathi, "Various attacks in wireless sensor network: survey," *International Journal of Soft Computing and Engineering, vol. 3, no. 1, 2013.*