Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.111 – 118

SURVEY ARTICLE

A Detail Survey on Wireless Sensor Networks (WSNs) Security Issues

Pratibha[1], Dr. Prem Chand Vashist[2]

[1]M-Tech. Student, [2]Head of Department & MVN University, Palwal, Haryana, India

Email: [1] preti238@gmail.com, [2] pcvashist@gmail.com

Abstract— Wireless sensor networks have become a growing area of research and development due to the vast number of applications and great impact in commercial applications such as traffic surveillance, habitat monitoring and smart workplaces and many more scenarios. Since a WSN consists hundreds of small size, low cost and battery powered sensor nodes. These nodes have the event sensing capabilities, data processing capabilities. One of the main challenges wireless sensor networks face today is security. The problem of security issues are arises due to constrained nature of resources on the wireless sensor nodes the wireless nature of the sensor networks and, which means that security architectures used for traditional wireless networks are not viable. Furthermore, wireless sensor networks have an additional vulnerability because sensor nodes are often placed in a dangerous hostile or environment where they are not physically protected. In this paper we have focused some security threats and challenges faced by WSNs.

Keywords-- Security, Wireless Sensor Networks (WSN), threats, Denial of Service (DoS)

I. INTRODUCTION

Wireless sensors network (WSN) is the collection of homogenous, self organized nodes known as sensor nodes. These nodes have the event sensing capabilities, data processing capabilities. The components of sensor node are integrated on a single or multiple boards, and packaged in a few cubic inches. A wireless sensor network consists of few to thousands of nodes which communicate through wireless channels for information sharing and cooperative processing. A user can retrieve information of his/her interest from the wireless sensor network by putting queries and gathering results from the base stations or sink nodes. The base stations in wireless sensor networks behave as an interface between users and the network. Wireless sensor networks can also be considered as a distributed database as the sensor networks can be connected to the Internet, through which global information sharing becomes feasible. Wireless Sensor Networks consist of number of individual nodes that are able to interact with the environment by sensing physical parameter or controlling the physical parameters, these nodes have to collaborate in order to fulfill their tasks as usually, a single node is incapable of doing so and they use wireless communication to enable this collaboration.

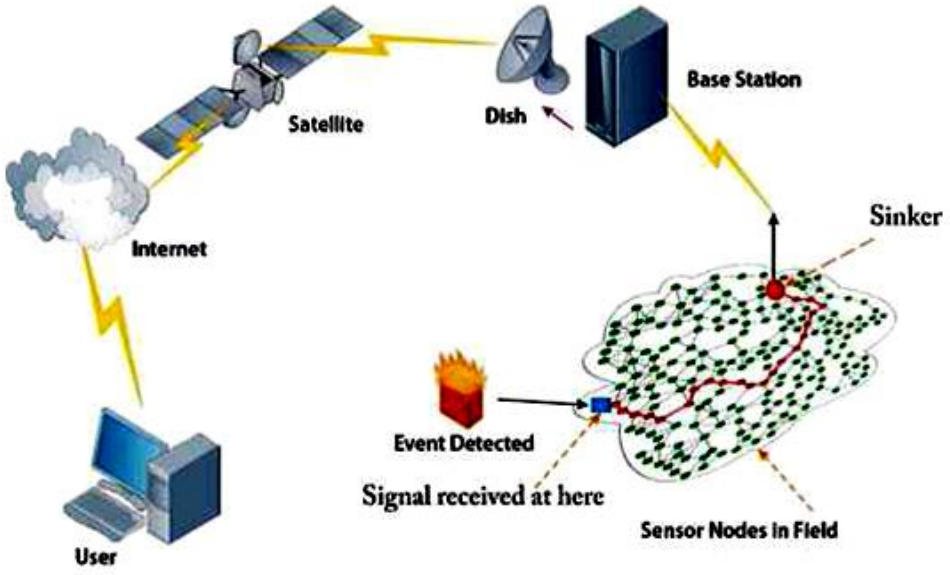

Figure 1.1 Wireless Sensor Network

This paper is organized as follows. Security goals for wireless sensor network are described in section II, WSN Applications and attacks are described in section III and IV. Finally conclusion and future works are given in section V.

II. SECURITY GOALS FOR WIRELESS SENSOR NETWORK

The security goals are classified as primary and secondary [5]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Availability Authentication and (CIAA). The secondary goals are Time Synchronization, Data Freshness, Self- Organization, and Secure Localization.
The primary goals are:

A. Data Confidentiality

Data confidentiality in wireless sensor networks is required to conceal messages from a malicious attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to the neighbors.

B. Data Authentication

Data authentication in sensor networks is required to ensures that the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets. It also verifies the identity of the sending nodes and receiving nodes. Data authentication is achieved through symmetric cryptography or asymmetric cryptography mechanisms where both sending and receiving nodes share secret keys.

C. Data Integrity

Data integrity in sensor networks is required to ensure the reliability of the information and refers to the ability to confirm that a message has not been tampered with, altered or changed. The integrity of the network will be in compromised when:
• A malicious attacker present in the network injects false data.
• Unstable conditions of wireless sensor networks cause damage or loss of data.

D. Data Availability

Data availability in sensor networks is required to ensure that whether a node has the ability to utilize the available resources and whether the network is available for the messages to communicate. However, in case of failure of the base station will threaten the entire sensor network. Thus availability gives the primary importance for maintaining an fully operational network.

The Secondary goals are:

E. Data Freshness

Data freshness in sensor networks is required to ensure that the data is recent, and it also ensures that no old messages have been replayed. In sensor networks even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. To solve this problem a time related counter can be added into the packet to ensure data freshness.

F. Self-Organization

A wireless sensor network is a an type of ad hoc network, that requires each and every sensor node should be independent and flexible enough to be self-healing and self-organizing varying according to the different scenarios. There is no fixed infrastructure available for the purpose of network management in a sensor network. So this feature brings a great challenge to wireless sensor network security.

G. Time Synchronization

Most sensor network applications rely on the time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications.

III. APPLICATIONS OF WIRELESS SENSOR NETWORKS:

Wireless sensor network can be developed for various types of application based on its data delivery, application type and application objective. Generally WSN application can be classified into following four classes.

A. Commercial and Industrial Applications:

1) Monitoring an Industrial Plant:

The wireless sensors are used to monitor the state of the physical plant and control device Cost savings can be achieved through inexpensive wireless means.

2) Inventory Control

Sensor nodes are used for warehouses products tagging. This will enable the users to track the exact location of the products as well as inventory the stock on hand. Inserting new products can be achieved by attaching the appropriate sensor nodes to the products. If the products are perishable, the senor node can also report the state of the products such as days in storage or temperature.

B. Health Applications

1) Gym Workout Performance Monitoring:

The gym member users pulse and respiratory rate can be monitored via wireless sensor nodes and transmitted to a personal computer for analysis. The gym club can monitors the exercise behavior of members and intervene when members need help reaching their goals.

2) Monitoring of Human Physiological Data:

Sensor nodes can collected the physiological data and stored over a period of time to study human habits and behavior. Sensor nodes allow greater freedom of movement and allow physicians to either monitor an existing condition.

C. Environmental Applications:

1) Soil Condition Monitoring:

Sensor nodes can monitor soil temperature and moisture for a given area. The sensor nodes can also be fitted with a variety of chemical and biological sensors so that the farmers can determine the level of fertilizer. This application is most suited for vineyards as minor changes in the environment can greatly affect the value of the crop and how it is subsequently processed.

2) Seismic Activity Detection:

Sensor nodes placed in regions for detection of seismic activity such as earthquakes, volcanic eruptions or a tsunami. Timely analysis of such information will enable cities to be evacuated. Sensor nodes placed in regions of seismic activity will enable geologists to monitor and predict the onset of an earthquake, volcanic eruption or a tsunami.

D. Security and Military Applications:

A wireless sensor network can be an integral part of military command, intelligence, surveillance, targeting systems, control, computing, and communications. They can be quickly deployed and are fault tolerant, which makes them an ideal sensing technique for reconnaissance and surveillance.

1) Monitoring of Force Movement and Inventory:

Wireless sensor networks can be used for monitoring of force movement and availability of equipment and ammunition. This will enable the military commander to give order to his forces or equipment to where it is needed most.

2) Battlefield Reconnaissance and Surveillance:

A wireless sensor network can be used to locate and identify targets for potential attacks or to support an attack by friendly forces Deployed .And wireless sensors networks can also be used in place of guards or sentries

IV. ATTACKS ON SENSOR NETWORKS:

Wireless Sensor networks are vulnerable to security attacks because of broadcast schemes used in the transmission medium. And wireless sensor networks required an extra vulnerability because some nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks.

A. Active Attacks

In this type of attacks the unauthorized attackers or a malicious node, monitors, listens and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

1. Denial of Service Attacks
2. Physical Attacks
3. Message Corruption
4. Passive Information Gathering
5. Routing Attacks in Sensor Networks
6. Node Subversion
7. Node Outage
8. False Node
9. Node Replication Attacks

1) Denial of Service

In this type of attack a malicious node disturb the whole network with the aim that the legitimate user can not uses its services. The main goal of this attack is not only for the adversary's attempt to disrupt, or destroy a network, but also disturb a network's capability to provide a service. In wireless sensor networks, different types of DOS attacks in different layers are presents that shown in table. At physical layer the DOS attacks could be tampering and jamming, at link layer it could be, exhaustion collision and unfairness, at network layer, black holes, neglect and greed, homing, misdirection and at transport layer this attack could be performed by malicious de-synchronization and flooding. The mechanisms to prevent DOS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

2) Physical Attacks

In this type of attack a malicious node destroys sensors permanently, as we know that Sensor networks operate in hostile outdoor environments. In this type of attacks the main aim of attacker is to completely destroy the sensor nodes.

3) Message Corruption

In this type of attack a malicious node or attacker modify of the content of a message when transmission have been done. The main goal of these attacks is to misleading receivers.

4) Passive Information Gathering

In this type of attack a malicious node or attacker utilize powerful resources can collect information from the sensor networks if it is not encrypted. In this type of attack a malicious node or attacker with a powerful receiver and antenna that can easily pick off the data stream. The main goal of this attacks is an attacker can observe the application specific content of messages including message IDs, timestamps and other fields. To mitigate these types of threats of passive information gathering, powerful encryption methods are used.

5) Routing Attacks in Sensor Networks

The attacks that arise on the network layer are known as the routing attacks. There are following attacks that arise between routing of messages.

a) Spoofed, altered and replayed routing information

In this type of attacks every node acts as a router, and can therefore directly affect routing information. For example a malicious node can selectively create routing loops for misleading information and generate false error messages etc.

b) Selective Forwarding

In this type of attack a malicious node can selectively drop some data packets. In wireless sensor networks it is assumed that all nodes faithfully forward received messages. But actually some compromised node might refuse to forward data packets to others nodes; however neighbors might start using another route.

c) Sinkhole Attack

In this type of attack a malicious node attracting traffic to a specific node in called sinkhole attack. The adversary's goal is to attract nearly all the traffic data from a particular area through a compromised node.

d) Sybil Attacks

In this type of attack a malicious node a single node duplicates itself and presented in the multiple locations at the same time. The main goal of this attack is to targets fault tolerant schemes such as topology maintenance, distributed storage and multipath routing. In this type of attack, a single node shows multiple identities to other nodes in the network. Authentication and encryption techniques can prevent to a malicious launch a Sybil attack on the sensor network.

e) HELLO flood attacks

In this type of attack a malicious node broadcast a HELLO packets from one node to another node announce themselves to their neighbors. In this attack an attacker uses HELLO packets as a weapon to convince the sensors nodes in sensor network.

6) Node Subversion

In this type of attack a malicious node capture of a node and reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. In this type of attacks a particular sensor node might be captured by an attacker, and information (key) stored on it might be obtained by an adversary.

TABLE 1: WSNs Threats in layers & defense mechanisms

Attacks	**Layers involved**	**Defenses**
Denial of service	Physical, Link, Network, Transport Layers	Priority message, hiding, monitoring, authorization, redundancy, encryption
Wormhole attacks	Link layer, network layer	Proactive Routing protocols
Sybil attacks	Network layer	Suspicious node detection by signal strength
Hello flood attacks	Network layer	Suspicious node detection by signal strength
Sink hole attacks	Link layer, network layer	Detection on MintRoute.

7) Node Outage

In this type of attack a malicious node disturb a particular node due to this its stops working and its functioning. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.

8) False Node

In this type of attack a malicious node or intruder might add a node to the system that feeds false data or prevents the passage of true data. This type of attack is the one of the most dangerous attacks that can occur. Malicious code injected in the network

could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.

9) Node Replication Attacks

In this type of attack a malicious node or intruder replicate a node with other node to serve our purpose. This attack is quite simple; an attacker easily adds a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt whole wireless sensor network's performance. Packets can be corrupted or even misrouted. This can result in false sensor readings, a disconnected network etc.

TABLE 2: Denial of Service attacks and defences to combat at different protocol layers

Protocol layer	**Attacks**	**Defences**
Physical	Jamming	Sleep
	Node destruction	Hide nodes or tamper proof packaging
MAC	Denial of sleep	Sleep, authentication and anti-replay
Network	Spoofing, replaying	Authentication, anti-replay
	Hello floods	Geographic routing
	Homing	Header encryption
Transport	SYN flood	SYN cookies
	De synchronization attack	Packet authentication
Application	Path based DoS	Authentication and entire play protection.
	Reprogramming attacks	

V. CONCLUSION

All of the previously mentioned security attacks such as, the Sybil attack, sinkhole attack, Hello flood attack, wormhole attack, serve one common purpose that is to compromise the network integrity Also In the past, researcher and developers focus not only on the security of WSNs, but also with the various attacks and security issues arising and the importance of data confidentiality, security has become a major issue. Although some solutions have already been proposed, there is no single solution to protect against every threat. In this paper focuses on the security threats in WSN. In this paper also presented the summery of the WSNs threats that affecting different layers along with their defense mechanism. Thus in this paper we have tried to present the most common security threats in different layers and their most probable solution.

REFERENCES

[1] E. C. H. Ngai, J. Liu, and M. R. Lyu, (2006)" On the intruder detection for sinkhole attack in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications (ICC "06), Istanbul, Turkey.

[2] Jamal N. Al-Karaki & Ahmed E. Kamal, (2004) "Routing Techniques in Sensor Networks: A survey", IEEE communications, Volume 11, No. 6, Dec. 2004, pp. 6-28.

[3] M. Tubaishat, S. Madria, (2003) "Sensor Networks : An Overview ", IEEE Potentials, April/May 2003

[4] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in feb.20-22,2006,ICACT2006,ISBN 89-5519-129-4 pp-1043-1048

[5] C. Karlof and D. Wagner, (2003). "Secure routing in wireless sensor networks:Attacks and countermeasures," AdHoc Networks Journal, vol. 1, no. 2–3,pp. 293–315.

[6] Feng Zhao,Leonidas Guibas,,"Wireless Sensor Networks", Morgan Kaufmann Publications.

[7] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun.ACM,2008, pp. 53 -57.

[8] Zaw Tun and Aung Htein Maw,(2008)," Worm hole Attack Detection in Wireless Sensor networks", proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.

[9] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)" DAWWSEN: A Defense Mechanism against Wormhole ttack In Wireless Sensor Network",Proceedings of the Second International Conference on Innovations in Information Technology (IIT"05).

[10] A. D. Wood and J. A. Stankovic, (2002) "Denial of service in sensor networks", Computer, 35(10):54–62, 2002.

[11] M. Zorzi and R. R. Rao, (2003) "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Transactions on Mobile Computing, vol. 2, no. 4, pp. 337-348, 2003.

[12] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks,"Mobil Computing and Communications Review, vol. 4, no. 5, October 2001.

[13] David R. Raymond and Scott F. Midkiff, "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.

[14] Chris Karlof, Naveen Sastry, David Wagner, (2004) Tiny Sec:a link layer security architecture for wireless sensor networks, Proceedings of the 2nd international conference on Embedded networked sensor systems , Nov 03-05,2004,Baltimore,MD,USA.

[15] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," IEEE Communications Surveys & Tutorials, 3rd Quarter 2008.

[16] K. Lu et al., "A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", IEEE Transactions on Wireless Communications, vol. 7, no. 2, Feb. 2008, pp. 639-647.

[17] O. E. Ochirkhand, M. Marine, V. Fabrice and K. Apostotlos, "Resiliency of Wireless Sensor Networks: Definitions and Analyses", 17th international conference on Telecommunications 2010, pp. 21-35.

[18] S. K. 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.

[19] T. G. Lupu "Main Types of Attacks in Wireless Sensor Networks" International Conference in Recent Advances in Signals and Systems 2009, ISSN: 1790-5109, ISBN: 978-960-474- 114-4.

[20] M.Y. Hsieh, Y. M. Huang, "Adaptive Security Modules in Incrementally Deployed Sensor Networks", International Journal on Smart Sensing and Intelligent Systems, vol. 1, no. 1, March 2008

[21] K. Sharma, M. K. Gosh, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Ad-hoc Networks MANETs, 2010.

[22] H. Ghamgin, M. S. Akhger, M. T. Jafari, Z. Branch, "Attackes in wireless sensor networks", Australian journal of Basic and applied Sciences, 2011. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, 2004.

[23] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges**",** International conference on Advanced Computing Technologies**,** Page1043-1045, 2006.

[24] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, 2003.

[25] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao, Page3-5, 2006.

[26] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006.

[27] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, 2009.

[28] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, 2002.

[29] Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 – 40, 2006.

[30] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2, page(s): 52-62, 2009.

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

[32] D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile ad hoc and Sensor Networks," *IEEE Commun. Surveys Tutorials*, vol. 7, pp. 2–28, 2005.

[33] S. Schmidt, H. Krahn, S. Fischer, and D. Watjen, "A Security Architecture for Mobile Wireless Sensor Networks," in *Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS)*, 2004.

[34] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tutorials*, vol. 8, pp. 2–23, year 2006.

[35] Yun Zhou, Yuguang Fang, Yanchao Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, 2008.

[36] N. Sastry and D. Wagner, "Security considerations for ieee 802.15.4 networks," in Proceedings of the 2004 ACM workshop on Wireless security, pp. 32–42, Philadelphia, PA, USA: ACM Press, 2004.

