International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:12, 2014

A Survey of Attacks and Security Requirements in Wireless Sensor Networks

Vishnu Pratap Singh Kirar

***Abstract*—**Wireless sensor network (WSN) is a network of many interconnected networked systems, they equipped with energy resources and they are used to detect other physical characteristics. On WSN, there are many researches are performed in past decades. WSN applicable in many security systems govern by military and in many civilian related applications. Thus, the security of WSN gets attention of researchers and gives an opportunity for many future aspects. Still, there are many other issues are related to deployment and overall coverage, scalability, size, energy efficiency, quality of service (QoS), computational power and many more. In this paper we discus about various applications and security related issue and requirements of WSN.

***Keywords*—**Wireless Sensor Network (WSN), Wireless Network Attacks, Wireless Network Security.

I. Introduction

WIRELESS Sensor Networks (WSNs) are new emerging technology that holds the potential to develop various useful and revolutionize applications for real world. Modern development in small sized microprocessors, microelectromechanical devices, and low powered wireless radio techniques combined form multifunctional, low-power, low-cost tiny sensor devices, which able to detect and react to small changes in physical characteristic of any system. These tiny sensor devices form a network with wireless environment and provide their functionality of sensing and tracking.

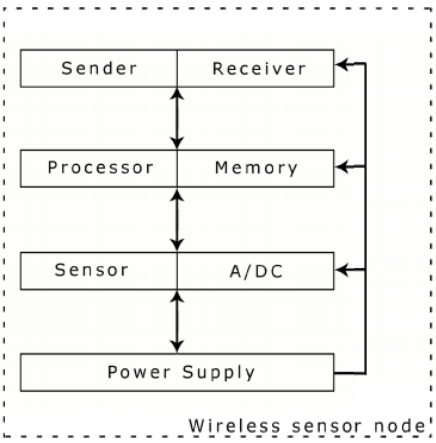

Fig. 1 Simplified Architecture of WSN

Vishnu Pratap Singh Kirar is with the Computer Science Department, University of Bedfordshire, Luton, United Kingdom (Phone: +44 7405400182; +91 9826020913; e-mail: Vishnu.kirar@study.beds.ac.uk).

A WSN consists of many small sensor nodes, these nodes are consisting of mainly four fundamental components: processor and memory (Microcontroller), sender and receiver (transceiver), power supply and sensor along with analog to digital converter (A/D converter). The simplified architecture of a sensor node is depicted in Fig. 1. A sensor, which is analogous to human organs like eyes and ears, gathers information about the surrounding environment, for instance, temperature, pressure, light, humidity, motion, acceleration, velocity, vibrations, and magnetism. When implemented in a systematic way, these sensors organize themselves automatically and built a dedicated ad-hoc multi hop network and each node can communicate with other node with in this network. At the sink, user remotely gives the command to nodes via the wireless network and collect the data and after processing stored in to storage device. These nodes also receive the sensed data from the sink node [1].

It seems too difficult to imagine that these small sensors have such a numerous qualities but these sensors are implemented in wide area such as environment, military, medicine, inventory monitoring, machine malfunction, motion tracking, agriculture, and many other fields. In the field of medical, WSN able to track and monitor different physical parameters of any patient. This data is sending to nearest hospital when parameters are changed and need some medical facilities. In agriculture, sensor senses different climatic conditions of particular area and suggest needs of cultivation. These techniques also apply in pollution detection systems and it can be implement to monitor different weather conditions and other natural disasters. WSN are more effective than traditional monitoring systems because they not only use for detection or monitoring but they can use to predict future aspect of any attribute. Nowadays, military is use WSN in their most of applications and operations to surveillance enemy's activities and collect the secret information. They can also monitor those areas, which are far away to reach and have bed climatic conditions. Many researcher present many surveys [2] and describe various possibilities in WSN.

In this survey we discuss various development, applications and challenges of WSN, and also discuss about various attacks on WSN and security requirements.

II. Application of Wireless Sensor Networks

A. Applications of Military Surveillance

WSN plays a very important role in integral part of military communication, commands and intelligence systems and commands. Sensors allowed deploying a very large battlefield to monitor the presence of enemy and their vehicles, and

monitor as well as track their minor and major movements, enabling fast and efficient surveillance of opposing forces and unidentified objects.

B. Environmental Applications

Environmental applications include sensing and tracking the movements and patterns of insects, birds or small animals, which help to prevent them from various unwanted sources that may cause those harms.

C. Health Care Applications

Wireless sensor networks are used to monitor and track patients who cannot able to travel to the hospital. These sensors are able to monitor and track them from their home. This facility is very useful because it reduce the medical expenses because when sensor monitors a patient, meanwhile doctor can serve another patient. Thus it saves several times as well. When any patient faces some problem then this sensor alert the doctors and nearest health care service provide their services.

D. Weather Forecasting

WSN applications in weather forecasting include monitoring and tracking the environmental conditions affecting crops, monitoring temperature, humidity, wind speed, lighting, visibility, sounds and so on. These systems help to provide accurate information about weather so that we can prepare for any condition. It also gives pre-warning about bed weather and other natural hazards like earthquakes and thunderstorms and heavy rains.

E. Home Super Vision and Intelligence

Wireless sensor networks can be used to provide much better and suitable intelligent living environments for every human. Like, wireless sensors can be used to remotely read utility meters in a home like gas, water and electricity, now this collected reading and data send to a remote centralized server.

F. Agriculture

Now wireless sensor networks are widely use within the agricultural, by using this technique farmer can increase their productivity of crop. They can monitor and track their resources from remote location. By getting information from weather forecast they can make sufficient arrangements in bed weather. They can also track the water resources within the earth by using WSN.

G. Industrial Process Control

In industry, WSNs can be used to monitor manufacturing process or the condition of manufacturing equipment. For example, chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. These sensors are used to alert in case of any failures occurred.

H. Structural Monitoring

Wireless sensors can be used to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc. enabling engineering practices to monitor assets remotely without the need for costly site visits, as well as having the advantage of daily data, whereas traditionally this data was collected weekly or monthly, using physical site visits, involving either road or rail closure in some cases. It is also far more accurate than any visual inspection that would be carried out.

III. Attacks on Wireless Sensor Networks

Sensor networks are suffers from any types of attacks. Privacy, traffic analysis, and physical attacks are some of them. Most known attack is on 802.11 MAC protocol layer to jamming the sensor communication. Here we discuss various attacks on sensor network [3]-[5].

Passive Attack: When an unauthorized user attacks on tracking, sensing and monitoring on communication channel than is known as Passive attack. If there is violation in privacy than it is known as passive attack.

Active Attack: When an unauthorized attacker modified the monitor data in communication channel than it is known as active attack. Based on security requirements, attacks on WSN are understand by these points:

Attacks on Availability of Network: It can be referred as Denial-of-Services (DoS) and can be target any type of layer of WSN [6].

Stealthy Attacks against Service Integrity: In this type of attack an external agent make the WSN to accept incorrect or duplicate data via sensor node and sink node also accept this data [7].

Authentication related attacks: an unauthorized user can access the communication channel of WSN and access the private data [8].

As we discus earlier that DoS able to attack any layer of WSN, thus we describe attacks on each layer [9]-[12]. Table I shows all possible attacks on different layers of WSN.

A. Physical Layer

Signal detection, frequency selection, carrier frequency generation modulation and data encryption, these are the main task of the physical layer. As WSN is monitor and scenes the remote locations thus the attacks have a chance to access the physical layer of WSN. Jamming and Tampering are two vulnerability of WSN.

Jamming: Jamming is occurs when external sources attacks on sensor node by interference of radio frequencies. These external sources can jam the WSN completely or partially and become a part of network. As we know wireless sensors are low powered and low cost devices thus they are limited to use single frequency. This may cause for jamming in the WSN. To protect from jamming various techniques are introduce including frequency hopping and code spreading. By using of frequency hopping spread spectrum method a signal is continuous transmitted in different communication channels with the generation of pseudo random sequence that is recognized by both sender and receiver. In mobile communication well-known method to avoid jamming is code spreading. It has a hug complexity in designing and implementation that's why it is less use in WSN.

TABLE I
ATTACKS ON WIRELESS SENSOR NETWORK

OSI Network Layers	Attack	Action
Transport Layer	• Flooding	• Authentication
	• Desynchronization	• Client puzzles
Network and Routing Layer	• Sybil	• Authentication, Probing
	• Wormholes	• Authentication, Packet leashes by using geographic location
	• Hello Flood Attack	• Verify the bidirectional link
	• Sinkhole	• Redundancy, monitoring, Authentication
	• Spoofed/Replayed Routing Information	• Egress Filtering, Monitoring, Authentication
	• Acknowledgement Spoofing	• Authentication
	• Selective Forwarding	• Redundancy, Probing
Data Link Layer	• Collision	• Error correction code
	• Exhaustion	• Rate Limitation
	• Unfairness	• Small frames
Physical Layer	• Jamming	• Spread Spectrum, Priority Messages, lower duty cycle, region mapping, mode change
	• Tampering	• Tamper proofing, hiding

Tampering: Second type of attack on physical layer is tempering. In this type of attack a node can alter by a fake node and attacker can easily get sensitive information and data. To avoid tampering we introduce temper proofing to sensor node. It can add additional cost to WSN.

B. Data Link Layer

Multiplexing of data, frame detection, error correction and medium access, these are the main tasks of data link layer. It also provides the point to point and point to multipoint reliable connection within the network. At this layer attacks that generally occur are collision, exhaustion and unfairness.

Collision: When two nodes transmit same frequency simultaneously on the same communication channel than collision is introduced in WSN. Hence, two packets collide and their data may corrupt and checksum mismatch occurs at receiver end. A receiver does not able to identify the packets. Error correcting code applies to overcome this collision problem. Mechanism of these codes is to add some additional overhead like communication and processing. But it is not a full proof solution because it can only work on low-level collisions.

Exhaustion*:* When an attacker send corrupted packets again and again i.e. repeated collisions then the receiver get exhausted. Thus the energy of sensor node reduced till prevention of retransmission of packets. The solution of this problem is to apply time division multiplexing (TDM), so that nodes have specific time to transmit their data. We can also apply rate limits on MAC layer to ignore excessive transmission of packets.

Unfairness: Unfairness can be described also as a form of DoS. By using this attack an unauthorized user make amendment on priorities of transmission and its time. To overcome this problem we have to use small size frames because it take less time to transmit and in is small time for attacker it is not easily to make any amendments.

C. Network and Routing Layer

To improve power efficiency, to make sensor network more data centric and awareness of location and addressing, network and routing layer plays an important role. Some attack on this layer is as follows:

Spoofed or replayed routing information: any attacker can perform the easiest and direct attack by attack on its routing information. Thus he can able to alter the traffic and create a fake routing loop. It can make WSN weak and create many corrupt nodes by attacker. To prevent this situation message authentication code is applied at MAC along with time stamping of message.

Selective Forwarding: In idea WSN all nodes forward accurate data to sink node. By adding some fake nodes an attacker can have power to forward some special messages. This message can be a black hole that drops the actual meaningful messages and sink receive some false data. To prevent this situation network should follows different path or multiple path for sending the data. Another solution is to detect these black holes and send them to a different path [13], [14].

Sinkhole: In sinkhole attack, attacker creates an attractive node to misguide the routing information. Thus the many surrounding nodes choose this node to forward information on selective route. By using this sinkhole method, selective forwarding becomes easier for attacker [15].

Sybil: When one node has more than one identity in any network then Sybil attack occurs. Network get confuse to perform some task like fault-tolerance, topology and storage because it cannot able to select suitable node for task and some time they may occur at same time.

Wormhole: A low potential link between two parts of a network is called wormhole. This link is between nodes of two-sub part of network which transfer message from one part to another and they forward information till the sink node. The situation of these sub parts may be neighboring or may be far way. An attacker can attack on this link and exchange the information by some error message or fake message. Hu et al proposed a mechanism to overcome this problem by introducing packet leashes i.e. temporal leashes and geographic leashes [16].

Hello Flood Attack: Introduction of HELLO packet make sure to receiving node that the sender node is within the same WSN or neighboring WSN. An attacker creates a imaginary node to confuse nodes that the sender is neighbor. If attacker

broadcast this node then all node transmit information to this false node.

Acknowledgement Spoofing: Sometimes there is need to use acknowledgment between sender and receiver nodes to transmit the information. An attacker can spoof this acknowledgment and provide some false information to receiver node.

D. Transport Layer

Transport layer provides end-to-End communication between sources to destination. Some possible attacks on this layer are discussed below:

Flooding: If source node receives many requests repeatedly, then its memory become exhausted through flooding. An attacker requests for new connection continuously till its maximum limit. In this situation sender decline all request including the genuine request of any node in WSN. Thus, attacker can waste resources of WSN and communication between nodes will stop.

Desynchronizaton: Interference between existing connections between communication channels known as desynchronization. To take advantages of this situation an attacker send a spoof message to end node. If end node refuses its request then by the time attacker can able to exchange private information or data. To overcome this problem we use the authentication method between sender and receiver.

IV. Security Requirements for WSN

WSN can be applied in variety of applications. Some of them are private and contains very sensitive information. Thus there are many concerns that are related to protect the sensitive information which exchange in between the nodes of WSN. As WSNs are connected to other networks like Internet or any local networks but the characteristics of WSN are different from these networks. Hence the security requirements are also different from conventional network. Here we discus some security requirement of WSN [17], [18].

A. Data Confidentiality

One of the main characteristics of data is Data Confidentiality. A network should be secure enough and have mechanism that can ensure that message should be delivering to dedicated receiver. Confidentiality prevents the network from passive attacker so that message within the WSN remains private and confidential.

B. Data Integrity

Data is accurate and consistent if there is no change in data between consecutive updates. In WSN data integrity means sensor node must be reliable so that there is no change in stored data between tracking of continuous data from surrounding environment.

C. Data Availability

Data availability in WSN means that node has ability to sense or monitor network in the presence or absence of communication channel. Node must be transmitting data to sink node periodically or when sink node calls for data. Availability is essential property of WSN and also essential for security because without data availability WSN cannot perform any task.

D. Data Authentication

Data authentication makes sure that message or data must be deliver to destination node i.e. communication can be performed between source and destination nodes. When number of nodes in network is more i.e. cluster then authentication is very essential. Every cluster has its cluster head. Cluster head is connected with other nodes of WSN. Authentication involves reliability of each message and its origin and destination.

E. Data Freshness

Data freshness means sensor node sense new data each time. Along with data confidentiality and data integrity WSN must ensure about data freshness. Node must be ensure that data must be fresh and arrange in proper sequence.

F. Self-Organization

To ensure the security of WSN, each sensor node must Self-organization and self-healing. WSNs are dynamic in nature thus it is impossible for some cases. WSN is an Ad-HOC network in which each node is independent to other and there no fix or predefines structure for it. Thus, there is much chance to attack on WSN.

G. Secure Management & Localization

To handle the sensitive data and co-ordination between different components, management is very essential for nay network. In WSN sensor nodes send the information to sink node and sink node store the data. Sink node collect data and send it over a communication channel. In many cases it is very important to locate the sensor node because they carried sensitive data. In condition of fault then network should verify the defective node and take action accordingly. If network in not able to locate the defective node then it is very easy for attackers to detect this sensor node and get its information. Thus Secure Management & Localization is an important aspect of WSN.

H. Time Synchronization

Another security requirement of WSN is time synchronization. As WSN consists of hug number of nodes and they sense continuously and send data for process thus it is necessary that each node perform its task in given time because many computational processes require sequential execution of data.

I. Quality of Services

Quality of Services has different meaning according to different applications. In general QoS refers that the data should be transmited in between particular sender and receiver. This data is dedicated to only these two parties. In WSN QoS is application specific and network specific.

J. Forward & Backward Secrecy

A sensor node must have quality of Forward and Backward Secrecy. Sensor node is working only till it is part of network. If it removes from then it cannot read any future message similarly it cannot provide data from past reading. Session key of any sensor kept always secret so that no one can recover or extract data from it.

K. Auditing

Main purpose of WSN is to collect data and zero overhead sensing. Smaller size and low power consumption are properties of WSN. Thus it can apply in many applications. Many small WSN exist to monitor the physical surroundings. WSN are replaced many traditional networks because it is more reliable than other.

L. Non-Repudiation

It means sensor node cannot deny sending any data that it sent previously. Non-repudiation is a security service for Point-to-Point network communication. To introduce fairness in communication Non-repudiation is very important.

M. Privacy & Anonymity

Sensor nodes are collecting very sensitive data and send to network over a communication channel. Thus, to secure the data as well as node is essential security aspect because any third party can attack on network and get this information or make amendment in it. Anonymity means to un-identify with in the network or group of same objects. Sensor node must have these two properties to make secure the WSN.

V. Conclusion

Wireless Sensor Network (WSN) indicates a combination of dedicated and isolated distributed sensors, which able to monitor and record the physical conditions and parameters of the environment and organize this useful collected data at a centralized location. Sensor networks means to a homogeneous as well as heterogeneous systems that are combines many tiny sensors and general-purpose actuators, which holds a computing capacity. In general architecture of multi-hop wireless sensor networks embraces a many hundreds of low powered, low cost, self- organizing wireless nodes or devices. These autonomous devices or nodes combine with networking devices like routers and a gateway to build a typical WSN system. We can also use routers to gain an additional communication link between end nodes of WSN and the network gateway. In this survey paper, we discuss various security issues of WSN starting with applications of WSN followed by attacks on different layers of WSN and its solutions. Wireless Sensor Networks are gaining attention of researchers very rapidly because they are potentially very cheap and have low cost solutions of various physical worlds' problems. At present, WSN are used and deployed at an accelerated pace by using it with Internet. This new technology holds many possibilities in the field of medical, transport, military, hazard management and environment domain.

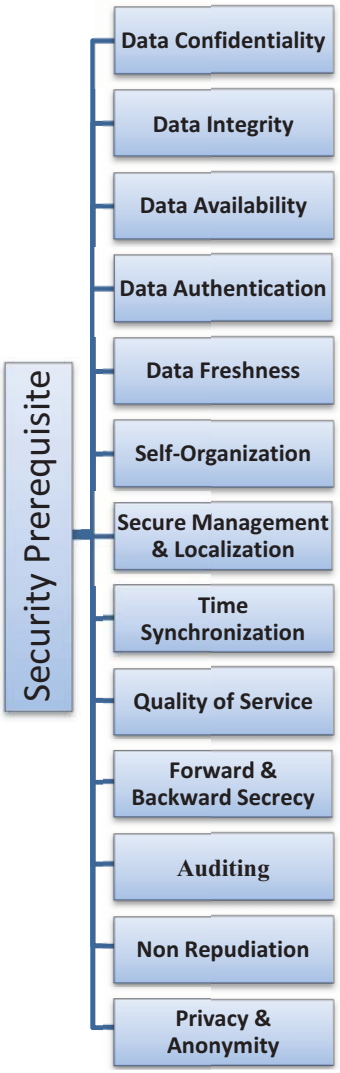

Fig. 2 Simplified Architecture of WSN

Due to their low cost availability give a chance to install a large arrangement of sensors in variety of applications to perform both civilian and military tasks. As they are very useful for men kind but they face some problems to implementation of traditional computer security techniques in a WSN, mainly in cryptography, steganography and other basics of network security and their applicability.

References

[1] F. Oldewurtel and P. Mahonen. Neural Wireless Sensor Networks. ICSNC, 0:28, 2006.

[2] M. Govindrajan, P. Balamurugan, "Wireless Sensor Network: A Survey," International Journal of Computer Networks and Wireless Communication (IJCNWC), vol 2, issue 5, October 2012.

[3] S. Umrao, A. Kumar, P. Umrao, "Security attacks and their countermeasures along with node replication attack for time synchronization in wireless sensor network," International conference on Advanced Nanomaterials and Emerging Engineering Technologies (ICANMEET), pp.576-581, July 2013.

[4] K. R. Begam, M. S. Devi, “A complete Survey on Facts and Attacks in Wireless Sensor Network,” International Journal of Science and Research (IJSR), vol 3, issue 3, March 2014.
[5] M. Riecker, D. Thies, M. Hollick, "Measuring the impact of denial-of-service attacks on wireless sensor networks," IEEE 39th Conference on Local Computer Networks (LCN), pp.296-304, September 2014.
[6] A. Tayebi, S. Berber, A. Swain, "Wireless Sensor Network attacks: An overview and critical analysis," Seventh International Conference on Sensing Technology (ICST), pp. 97-102, December 2013.
[7] Xu Huang, M. Ahmed, D. Sharma, "Protecting from Inside Attacks in Wireless Sensor Networks," IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 186-191, December 2011.
[8] M. V. Ramesh, A. B. Raj, T. Hemalatha, "Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks," Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 783-787, November 2012.
[9] S. Prasanna, S. Rao, “An Overview of Wireless Sensor Networks Application and Security,” International Journal of Soft Computing and Engineering (IJSCE), vol. 2, issue 2, May 2012.
[10] S. Gupta, H. K. Verma, “Security Attacks & Prerequisite for Wireless Sensor Network,” Internation Journal of Engineering and Advanced Technology (IJEAT), vol. 2, issue 5, June 2013.
[11] A. Muruganandam, P. Bagyalakshmi, “A Study on Threats in Wireless Sensor Network,” International Journal of Science and Research (IJSR), vol. 3, issue 3, March 2014.
[12] K. Venkatraman, J. V. Deniel, G. Murugaboopathi, “Various Attacks in Wireless Sensor Network: Survey,” International Journal of Soft Computing and Engineering (IJSCE), vol 3, issue 1, March 2013.
[13] B. K. Mishra, M.C. Nikam, P. Lakkadwala, "Security against Black Hole Attack in Wireless Sensor Network - A Review," Fourth International Conference on Communication Systems and Network Technologies (CSNT), pp. 615-620, April 2014.
[14] L. K. Bysani, A. K. Turuk, "A Survey on Selective Forwarding Attack in Wireless Sensor Networks," International Conference on Devices and Communications (ICDeCom), pp.1-5, Ferbuary 2011
[15] Qi Jin, Hong Tang, Xiaohui Kuang, Qiang Liu, "Detection and defence of Sinkhole attack in Wireless Sensor Network," 2012 IEEE 14th International Conference on Communication Technology (ICCT), pp. 809-813, November 2012.
[16] D. Buch, D. Jinwala, “Detection of Wormhole attacks in Wireless Sensor Network,” 3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011), pp. 7-14, November 2011.
[17] B. Veeramulllu, S. Sathiya, Ch. LavanyaSusanna, “Confidentiality in Wireless Sensor Network,” International Journal of Soft Computing and Engineering (IJSCE), vol. 2, issue 6, January 2013.
[18] M. M. Patel, A. Aggarwal, "Security attacks in wireless sensor networks: A survey," International Conference on Intelligent Systems and Signal Processing (ISSP), pp. 329-333, March 2013.