ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

A Survey of Wireless Sensor Network Security

Mr. Prasad Mahajan[1], Miss Priyanka Bhute[2]

Assistant Professor, Information Technology Department, M.I.T. College, Aurangabad, India [1]

Research Assistant, Aurangabad, India [2]

Abstract: The appearance of sensor network as one of the presiding technology in the coming decades has given numerous unique challenges to researchers. These sensor networks consist of large set of homogenous nodes which have limited computed resources. A lot of real world applications on sensor network have been proposed in research literatures. When sensor networks deploy in a unintended or hostile environment, security issues becomes a central concern, as they are prone to different types of malicious attacks. In this paper we present the survey of security issues, attacks with countermeasures in wireless sensor network (WSN). Conclusion and future scope of the work has also been outlined.

Keywords: Wireless Sensor Networks, Security, Threats, Attacks.

I. INTRODUCTION

WSN monitors the physical or environmental conditions such as temperature, sound, pressure and humidity etc. WSN composed of large set of low power, low cost smart devices with extreme resource constraints. Each device is called as sensor nodes and each node is connected to one or sometimes several sensor nodes. It has capability of wireless communication and some sort of intelligence for signal processing and data networking. These sensor nodes are usually thrown in various random directions over the area to gather data, process that data and pass it to the central node for further processing. Each sensor node consists of three subsystems: sensor subsystem, processing subsystem and communication subsystem. Sensor subsystem used for sensing the environment. Processing subsystem is used to perform local computations on the sensed data and communication subsystem responsible for message exchange with neighbouring sensor nodes.

WSN are used in many applications. These applications includes

1) Military applications such as monitoring friendly forces and equipments, military theaters or battlefield surveillance, nuclear, biological and chemical attack detection.

2) Environmental applications such as microclimates, forest fire detection, precise agriculture and flood detection.

3) Health applications such as tracking and monitoring doctors and patients inside the hospital, drug administration, remote monitoring of physiological data.

4) Home applications such as food automation, instrumented environment, automated meter reading etc.

5) Commercial applications such as environmental control in industrial office buildings and vehicles tracking and detection, inventory control, traffic flow surveillance [1].

II. ARCHITECTURE OF SENSOR NODE

Sensor node is the important part of wireless sensor network which is capable to gather information through sensors and perform some computation on that information and communicate the result with other connected node in the network .Sensor node is also called as mote.

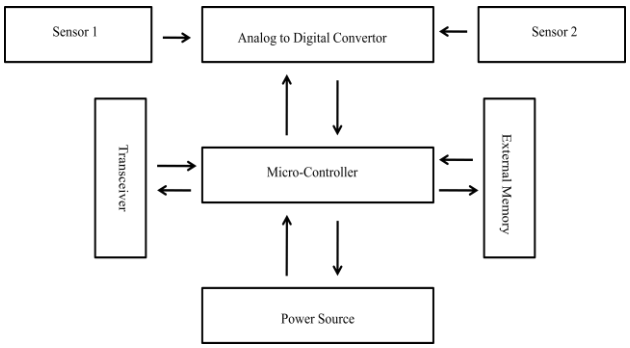

Fig. 1: Architecture of sensor node

Sensor node consists of following parts:

A. Controller

It is the brain of sensor node. It controls functionality of other parts in sensor node. It is able to process data and perform tasks.

Mostly Micro-controller is used as controller in sensor node than general purpose micro-controllers (digital signal processor, desktop microprocessor) because of its low cost, flexibility to connect to other devices, ease of programming, and low power consumption.

B. Transceiver

In Wireless transmission medium various ways are available like radio frequency (RF), optical communication (laser) and infrared. Laser has advantage that it requires less power but main disadvantage is that it is more sensitive to atmospheric conditions. Infrared is also a good choice, again it has limited broadcasting capacity. So most of WSN communications are RF based. Transceiver is able to perform functionality of both transmitter and receiver.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

C. External Memory
Due to cost and Storage capacity, flash memories are used.

D. Power Source
Power source is one of the most important units which may be finite for example single battery. It may be supported by scavenging devices (e.g. solar cells).

E. Sensors
To any change in physical conditions, sensors are the hardware devices that produce measurable data. They pass this measurable data to ADC in the form of analog signals and then ADC converts that into digital form. ADC passes that digital form data to microcontroller and microcontroller processes this data and performs some task.

III.SECURITY REQUIREMENTS IN WSN

A sensor network is a special type of network in which it shares some common properties of typical computer network. A goal of security services in WSN's is to protect network i.e. information and resources from attackers. These security requirements are as follows [2]:

A. Data Confidentiality
Data Confidentiality in networking is most important issue in network security. It ensures that the given message is understood only by that desired recipients. The major problem in WSN is that wireless channels are open to everyone therefore that channels are used by anyone. Thus attackers can capture sensitive information through that radio communication. Thus it is very necessary to build a secure channel in WSN.

Sensor node may be highly sensitive, especially in military applications. Thus sensor network should be built in such a way that it should not leak any sensor readings to its neighbours. Applications like sensor identities, industrial secrets, and public keys should be encrypted to some extent to protect from malicious activity. The key approach to achieve confidentiality is to encrypt the data with a secret key that only desired receivers knows. Cipher Block Chain (CBC) is the most appropriate encryption technique for sensor network as per TinySec [3][4].

B. Data Integrity
An attacker may be not able to steal information with the implementation of confidentiality. But this doesn't mean that the data is safe. Data integrity ensures that the message send from one node to another node is not altered due to malicious intent or by an accident. For example in hostile environment a malicious node may add or manipulate the data within a packet. This manipulated new packet then sends to the indented receiver.

When the operational conditions are out of range like temperature, humidity, pressure, light, radiations etc, then that device works improperly this can cause errors in packets. Those errors may not be observed and those error packets are forwarded out. The unintelligible packets will be added at the other side's which can cause denial of service (DoS) attack that diminishes or eliminates a network capacity to perform its expected functions [5][6]. If an attacker knows the packet format, then more serious damages can be caused like he can modify the location of important event so that receiver obtains wrong information. Thus the basic requirements for secure communication are that the information or packets are not altered during communication. And also the receiver needs to know exactly what the sender wants to send. The use of message integrity code is the standard approach for ensuring data integrity.

C. Data Authenticity
Authentication is necessary for many administrative tasks like network reprogramming, decision making process etc. An adversary can easily inject messages if he knows the packet format defined in the network. Because of this, receiver receives the packets carrying false information. So it is necessary for the receiver to make sure that the data used in decision making process originates from the correct source. And the typical example of packet injection is Sybil attack [7].
Data authenticity ensures that the communication in between two nodes is genuine that is a malicious node cannot behaves as a trusted network node. Use of message authentication code, signature authenticating public keys etc is the standard approach for ensuring authenticity.

D. Data Freshness
To achieve either continuous monitoring or event direction applications, WSN are used. In continuous monitoring applications, each sensor node forwards its sensed data periodically to the base station and in event direction application, once an event occurs, nodes reported to the base station. In continuous monitoring application such as in hospital application, fresh data is required for taking the necessary and preventive action. Data reaching to the sink node or base station after a certain threshold is not useful for further processing, because the information in it is not valid. An attacker receives a packet from a network, and then replays it to the network after some amount of time. A typical example of this is Wormhole attack in wireless network [8].
Instead of confidentiality and data integrity, freshness of each message needs to be assured. Data freshness implies that the data is a recent and ensures that no attacker can replay old messages. Data freshness is ensured by using a timestamp i.e. a receiving node can compare its own time clock with the timestamp and checked whether the packet is fresh i.e. valid or not But this is an overhead because each time data is forwarded, the timestamp of the received data packet has to be checked.

E. Availability
Due to excess computation and communication, sensor nodes may run out of battery power and become unavailable. An adversary may jam communication to make the sensor nodes unavailable, which results in the degradation of network security leading to DoS. Availability which ensures that the desired network services are available even in the presence of denial of service attacks [9].

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

F. Self Organization

Self organization is the property of system to arrange its components, elements in a purposeful or non-random manner under appropriate conditions but without controlled by any agent or subsystem inside or outside of the system. Many sensor nodes of different types are placed in a heterogeneous and somewhat hostile environment therefore there is no fixed infrastructure is available for WSN.

Self organization of WSN is a challenging task because of limited energy resources available in this network. Self organization ensures that the decomposition of the network into connected, non-overlapping clusters of bounded size. Distributed sensor network must be self organize to support multi-hop routing, to conduct key management and building trust relations among sensors, deny oppose, withhold, discard [10].

G. Non-Repudiation

Non-Repudiation tells about source of the packet. Source proves of identity of the packet in authentication process. Non-Repudiation gives authority of source from denying that it sent a packet.

IV. SECURITY ATTACK IN WSN WITH COUNTERMEASURE

THREAT MODELS

A threat is a possible danger in computer security that causes possible harm to the system. According to Karlof, threats can be classified into the following categories.

- Mote-class Attacks and Laptop-class attacks

In mote-class attacks, an adversary has access to a few sensor nodes with similar capabilities as that of network nodes. In contrast, in laptop-class attack an attacker may have access to more powerful devices like laptop or their equivalent which have greater transmission range and processing power.

- Outsider attacks and Insider attacks

In outsider attacks, an adversary has no special access to sensor networks and occurs from the nodes which do not belong to a WSN. Insider attacks occur when an authorized participant in the sensor network has gone badly which behaves in unintended or unauthorized ways. These attacks are difficult to detect.

- Passive and Active attacks

In former case, there is eavesdropping on or monitoring of packets exchanged within a WSN while in active attacks attackers add some modifications or the creation of a false stream in a WSN [11].

ATTACKS

Attack is defined as any attempt to destroy, expose, alter, steal or gain unauthorized access to a service. WSN are vulnerable because the sensor nodes are deploying in a heterogeneous manner where they are not physically protected.

Attacks on computer system or network can be broadly classified as follows:

- Interruption is an attack on the availability of the network for e.g. Insertion of malicious code into the network which potentially destroying the network.
- Interception is an attack on confidentiality in which the sensor network can be compromised by an attacker to gain unauthorized access to sensor node. An attacker can locate the node by intercepting the messages containing the physical location of sensor nodes and destroy them.
- Modification is an attack on integrity means an unauthorized party access the data an also tampers it. The main aim of an attacker is to confuse or mislead the parties involved in the communication.
- Fabrication is an attack authentication in which an attacker injects false data that gives incorrect information about the environment to the user [12] [13].

Some of the critical attacks in each layer of a sensor network with their countermeasures are as follows [14] [15] [16].

A. Physical Layer

1) Jamming:

This is one of the DoS attacks in which an attacker interface with the communication frequencies due to which the operation of network disrupted. Jamming attack in WSN classified as: - constant jamming attacks corrupts package as they are transmitted and requires a significant amount of energy, a deceptive jammer sends a constant stream of bytes into the network to make it look like a legal traffic, a random jammer randomly alternates between sleep and jamming to save energy and reactive jamming transmits a jam signal when it senses traffic.

Various forms of spread-spectrum techniques such as frequency hopping and code spectrum are used as defense against jamming. In frequency hopping spread spectrum, all communication nodes maintain hopping sequence. Here, if jammer observes the transmission, he can get the hopping sequence and thus hopping should be done very fast. Code spectrum technique requires greater design complexity and energy, thus the use of code spectrum is restricted in WSNs.

2) Tampering or destruction:

Tampering is another physical attack in which an attacker can get the access to the sensor node physically and also attacker may add some identical sensor nodes from their own side into the sensor network field. This is due to the number of sensor nodes are distributed over the large area and it become\s impossible to control the access to all nodes from others.

The defense mechanism from this attack includes tamper-proofing the physical package of node.

- Self Destruction- When anyone access the sensor nodes physically the nodes take out their memory contents which prevents from the leakage of information.
- Fault tolerant-protocols-The protocols designed for a WSN should be so resilient that the network should function properly even if some nodes are removed from the network.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

3) Sybil Attack:
Sybil attack generally occurs in higher layers like link layer and network layer but the base of it is physical layer. In this attack an adversary introduces a malicious node into the network by compromising any legal sensor node. Using this attack, an attacker as a single node presents multiple identities to the other nodes in the network.
Sybil attack is normally tackled in higher layers through their origin is from physical layer. One can fix the number of nodes to network which will the attacker from fabricating new identities.

B. Data Link Layer

Data link layer used to achieve point to point and point to multipoint connections in a communication network. Also it deals with data frame detection, medium access and transmission errors. Attacks on the data link layers are:

1) Collision:
A Collision occurs when two nodes transmit the data simultaneously on the same frequency. When packet collide , a small change will occur in data portion of the packet which leads to an error in the checksum of whole packet and the packet then will be discarded as invalid and asks for transmission of the same packet.
This kind of attack can be tackled by using error correcting codes which is incorporated in the data packets. But this code requires a greater computational complexity and additional processing.

2) Exhaustion:
In this type of attack, an attacker continuously disturb the communication in between two nodes and force the source node to continuously retransmit which leads to decay in the energy level of the sensor node.
The defense against exhaustive denial of service attack is to apply a rate limits to the MAC admission control like network can ignore excessive request which save energy caused by repeated transmission. A second solution is to use time division multiplexing. In this each node having a time slot, i.e. if a node retransmits a message for more than threshold value then node identifies itself as under attack and goes to sleep mode and later it may resume its operation.

3) Unfairness:
This kind of attack is partial DoS attack. Repeated application of these exhaustion and collision, an attacker may cause unfairness in network. An attacker degrades the performance causing other nodes to miss their transmission deadline. The solution for this attack is the usage of small frames so that any node captures the communication channel for smaller duration only.

4) Interrogation:
To lighten the hidden node problem, many medium access control layer implementations uses two-way request-to-send and clear-to-send handshake. An attacker can repeatedly send RTS packets to a target node by ignoring CTS replay packets which can flood the network link of targeted node. A technique to overcome this attack is that anode can limit itself in accepting connection from same identity i.e. a particular node will accept a fixed number of connections from the same identity.

5) Sybil Attack:
There are two Sybil attack as follows:
Data Aggregation: where one node presents more than one identity to the network which may give negative re-enforcement. It reduces the bandwidth requirements for message transmission as well as power consumption in the network.

Voting: Voting is nothing but the choice for number of tasks in a network. Many MAC protocol uses voting for choosing a better link from a pool of available link for transmission. An adversary can determine the outcome of any voting depending on the number of identities the attacker owns.

The popular defence against Sybil attack is Radio Resource Testing which relies on the assumption that any physical device has only one radio. If a node wants to verify that none of its neighbours are Sybil identities, then it can assign of its n neighbours a different channel to broadcast some message on. It can then listens to any channel and finds out whether the neighbour that was assigned that channel is legitimate [17].

C. NETWORK LAYER

Network layer is generally responsible for specifying the assignment of addresses and now the packets are forwarded out. The attacks in the network layer include the following:

1) Spoofing and Altering the routing information:
An adversary may spoof, alter or replay the routing information while it is being exchanged between nodes and disturbs traffic in the network. With the help of this, an attacker may be successful to create the routing loops, attract or repels network traffic from the select nodes, generate fake messages, partition the network.
A typical defense against spoofing and alteration is to append a message with message authentication code (MAC) which helps to verify whether the messages have been spoofed or altered.

1) Misdirection:
This is more active attack in which an attacker adds some malicious node in the routing which sends the packet in the wrong direction causing the packets are unreachable to the destination.
To overcome this victim node can be scheduled into sleep mode for some time if that node is getting flooded without any useful information.

2) Internet Smurf Attack:
In this type of attack, the attacker steals the address of the victim node and broadcast echoes in the network. And also routs all the replays to the victim node. This kind of attack can be handled easily by scheduling into sleep mode for some time.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

3) Sybil Attack:
In Sybil attack, one node presents more than one identity to the networks i.e. these Sybil nodes gives an illusion of their presence at different geographic location. One can use unique shared symmetric key for each node with the base station as a defense to the Sybil attack. Actually there is no effective solution to overcome from Sybil attack in network layer.

4) Sinkhole:
In sinkhole attack, an attacker tries to stimulate almost all the traffic towards the comprised node i.e. it prevents the base station from obtaining complete and correct information. The defense for sinkhole attack is to use Geo-Routing protocols in which the topology is constructed using only localized information and also traffic is routed through the physical location of the base node.

5) Selective Forwarding/ Black hole Attack(Neglect and Greed):
WSNs are based on the assumption that all the nodes in the network will accurately forward receive messages. An adversary may add malicious node in the network which refuse to forward certain messages and drop them, so that they are not propagated further. The goal of this attack is to include itself on the actual data path flow. It is also called as Black hole attack if they drop all the packets i.e. they don't forward any packets it receives.

The solution for this is to use multiple paths to send data, or use implicit acknowledgements ensuring the packets are forwarded as they were sent.

6) Wormhole Attack:
Wormhole attack is a critical attack in which it receives packets at one point in the network, and tunnels them to another point in the network. This is usually done by a malicious node forwarding data in between two legitimate nodes. In wormhole attack, an adversary gives two distant nodes the illusion that they are close to each other through which he can collect and Manipulate network traffic. Wormhole attack is responsible for increasing routing race condition.The solution for this is to design routing protocols which avoid routing race condition for e.g. Geo-Routing protocols in which a topology is based on localized information and interactions [18].

7) Hello Flood attack:
In Hello flood attack, a laptop class attacker can send routing or other information with large radio range which causes every node in the network thinks the adversary is its neighbour and assumes that the packet is within the radio range of the sender. The goal of this attack is to enable wormhole attack by broadcasting wormholes.

A countermeasure against this attack is to verify the bi-directionality of a link whenever selecting a path. Also one can use authentication process for avoiding these kinds of attacks.

D. TRANSPORT LAYER

Following are the threats present in transport layer:

1) Flooding:
In this an adversary repeatedly creates new connection request until the resources reaches to a maximum limit due to which further legitimate requests will be ignored. The defence against flooding is to make the number of connections from a particular node under limit. Also this problem is minimized by solving a puzzle by each connecting client while demonstrating its commitment to the connection.

2) De-synchronization:
De-synchronization refers to the disruption of the communication protocol by altering the sequence numbers of packets. By repeatedly spoof messages to one or both end points and by maintaining proper time, an adversary end point from exchanging any useful information. This will results in considerable loss of energy of nodes in the network.
To overcome from this attack, the packets which are communicated between hosts should be authenticated including all control fields in transport packet header.

V. CONCLUSION

Security is the most challenging factor in WSN. Designing strong protocol for WSN is very hard. If one tries to focus on a particular issue like authentication or confidentiality while designing other issues like availability, data freshness gets affected.
Data in WSN needs to provide security. In this paper, we have studied security measures in WSN. In future one may provide some new countermeasures for the attacks that we have studied.

REFERENCES

[1] Kazem Sohraby, Daniel Minoli, Taieb Znati, "Wireless Sensor Networks Technology, Protocols, And Applications", John Wiley & Sons publications, ISBN 978-0-471-74300-2.
[2] Shio Kumar Singh, M. P. Singh, D. K. Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks" International journal of computer Trends and Technology, June 2011.
[3] M.J. Karmel Mary Belinda and C. Suresh Gnana Dhas, "A Study of Security in Wireless Sensor Networks", MASAUM Journal of Reviews and Surveys", Sept. 2009, vol. 1, Issue 1, pp. 91-95.
[4] Chris Karlof, Naveen Sastry, and David Wagner, "TinySec: A Link Layer security Architecture for Wireless Sensor Networks", ACM SenSys 2004, Nov. 3-5, 2004, pp. 162-175.
[5] A.D. Wood and J. Stankovic, "Denial of service in sensor network", IEEE Computer Magazine, vol. 5, no. 10, Oct. 2002, pp. 54-62.
[6] Raymond D.R. Midkiff.S.F, "Denial of Service in Wireless Sensor Network: Attacks and Defenses", IEEE Pervasive Computing, Vol:7, Issue 1, PP: 74 – 81, March 2008.
[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses" in Proceedings of the 3rd IEEE International Symposium on Information Processing in Sensor Networks (IPSN'04), Berkley, CA, Apr. 2004, pp. 259-268.
[8] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03), vol. 3, San Francisco, CA, Mar. 2003, pp. 1976-1986.
[9] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey', Computer Networks 38 (2002) ,pp. 393–422
[10] Travis C. Collier and Charles Taylor, "Self-Organization in Sensor Networks", December 2003.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

[11] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network (SNPA), Sept. 2003, pp. 293-315.
[12] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey" Journal of Theoretical and Applied Information Technology, 2010, pp. 14-27.
[13] W. Stallings, "Cryptography and Network Security Principles and Practice", Cryptography Book, 2nd Edition, Prentice-Hall, 2000, 0-13-869017-0.
[14] H.K. Kalita and A. Kar, "Wireless Sensor Networks Security Analysis", International Journal of Next-Generation Networks (IJNGN), vol. 1, no. 1, Dec. 2009, pp. 01-09.
[15] Youg Wang, Garhan Attebury, Byrav Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks", IEEE Communications & Tutorials, 2nd Quarter 2006, vol 8, no. 2.
[16] Hiren Kumar Deva Sarma, Avjit Kar, "Security Threats in Wireless Sensor Networks", IEEE A & E Systems Magzine, June 2008.
[17] J.R. Douceur, "The Sybil Attack", in 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), March 2002, LNCS 2429, 2002, pp. 251-260.
[18] Y.C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

BIOGRAPHIES

Prof. Prasad C. Mahajan received the B.E. degree in Information Technology from Sanjivani College of Engineering, kopargaon in 2011 and received M.E. degree in Computer Science and Engineering from Government College of Engineering, Aurangabad, in 2013. He is currently working as an Assistant Professor in MIT College Aurangabad.

Priyanka D. Bhute received the B.E. degree in Computer Technology from KITs Ramtek, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur in 2011 and the M.E. degree in Computer Science and Engineering at Government College of Engineering, Aurangabad in 2014.