RESEARCH ARTICLE OPEN ACCESS

Wireless Sensor Network and Its Security Threats – A Study

T.Vijayalakshmi
Assistant Professor Department of Computer Science Vidhya Sager Women's College, Chengalpattu,Tamilnadu

ABSTRACT
A data network is a digital telecommunications network that allows nodes to share resources. Two types of networks are available, wired and wireless networks. Wireless networks become popular because of its wireless setup and its abundant applications in home, business and telecommunications networking. With the invent of sensor which react and notice some type of input from the physical or environmental conditions, such as pressure, temperature, beam, Wireless sensor network developed. The WSN are stretchy, simple to employ and straight forward. They are growing because of low cost and efficient. Wireless Sensor Networks consist of many sensor nodes that are distributed in a field and have physical capabilities to measure or sense things in the real world, do some computations, communicate with each other and deliver result to base station. With the rising expertise, the things on security are also advancing day by day. Though the network completely secured during the time of designing, intruders and attackers always find their way to get inside it and accomplish attacks. This paper presents a noteworthy analysis on the security threats of wireless sensor network. Threats are of two types active and passive attacks. Passive attacks are just listening the communication lines, whereas active attacks are modifying the data in communication lines. Different threats belonging to active and passive threats are studied in detail.

Keywords- Flooding, Jamming, Sensor node, Sybil Attack, Tampering.

Date of Submission: 18-12-2018 Date of Acceptance: 31-12-2018

I. INTRODUCTION

A data network or computer network is a digital telecommunications network that permits nodes to share resources. In computer networks, computing devices swap data with each other using connections between nodes. These data links are established over cable media such as optic cables or wires or wireless media. Network computer devices that initiate route and terminate the data are called network nodes. Nodes are recognized by network addresses and can include hosts such as phones, personal computers, servers and networking hardware. Two such devices may be said to be networked together when one device is capable to exchange information with the other device, whether or not having direct connection to each other.

1.1 Wired Network

A wired network is a general type of wired configuration. The majority wired networks use Ethernet cables to transfer data between linked PCs. In a small wired network, a single router used to connect all the computers. Larger networks frequently involve switches or multiple routers that connect to each other.

1.2 Wireless Network

The computer network that uses wireless data connections between network nodes is called a Wireless Network. It is a method by which homes, business installations and telecommunication networks avoid connection between various equipment locations or the costly process of introducing cables into a building. Wireless telecommunications networks are usually implemented and administered using radio communications and this takes place at the physical level layer of the OSI network structure. Common areas of wireless networks include Cell Phone Networks, Wireless Local Area Networks, Satellite Communication Networks, Wireless sensor networks and Terrestrial Microwave Networks.

II. WIRELESS SENSOR NETWORKS

Wireless sensor network is wireless network consisting of spatially distributed autonomous devices using sensor to monitor physical and environmental conditions. WSN application areas include health care, utilities and remote monitoring. In health care wireless devices make less hostile patient monitoring. For utilities such as electricity grid, streetlights and water municipals wireless sensors offer low cost method for collecting data to reduce energy usage and resource management. WSN complements Wireless Network by reduce wiring cost. Remote monitoring application include air soil water management, structural monitoring for building and bridges, asset tracking and industrial machine monitoring. WSN network constructed using three topologies such as star, Cluster tree & Mesh

topologies [1, 2]. In Mesh topology, networking all nodes lend a hand to distribute data among each other. A cluster tree topology is a unique case of tree topology in which a parent with its children is called a cluster. Every cluster is recognized by a cluster Identity number. In star topology, each host is coupled to a central hub. In simplest figure solitary central hub acts as a channel to send out messages.

III. COMPONENTS OF WIRELESS SENSOR NETWORK

Wireless Sensor Network is a hardware and software package that typically consists of four parts that are Sensor field, Sensor Node, Sink, Task Manager.

3.1 Sensor Node

A sensor node is a node in a sensor network that gathers sensory information performs some processing and communicating with other connected nodes in the network. Sensor node is also called as mote. A node is not always a mote but mote is a node. The main parts of sensor node are a Microcontroller, Transceiver, External Memory, Power Source and one or more Sensors.

3.1.1 Controller

The controller processes data, controls the functionality of other components and performs tasks in the sensor node. Most common controller is a microcontroller. A microcontroller used in many embedded systems such as sensor nodes because of its flexibility to connect to other devices, low cost, low power consumption and ease of programming.

3.1.2 Transceiver

Sensor nodes use ISM band, which gives spectrum allocation, free radio and global availability. The possible choices of wireless transmission media are laser, Radio Frequency and infrared. WSNs use license-free communication frequencies: 915 GHz, 2.4 GHz, 433, 173 and 868. Features of transmitter and receivers combined into a single device called a Transceiver.

3.1.3 External memory

Flash memories that if off-chip RAM. It used due to their storage capacity and cost. Memory requirements are application dependent. Two categories of memory are: user memory used for storing application related or personal data, and program memory used for programming the device.

3.1.4 Power source

The sensor node consumes power for communicating, sensing and data processing. Extra energy is required for data communication than any other process. The energy fee of transmitting 1 Kb a distance of 100 meters is roughly the same as that used for executing 3 million instructions by a 100 million instructions per second/W processor. Power is stored either in capacitors or batteries. Batteries (rechargeable and non-rechargeable) are the key source of power supply for sensor nodes. Current sensors are able to renew their energy from Solar energy sources, Thermo generator differences, or Vibration powered generator .Two power saving policies used are Dynamic Voltage Scaling (DVS) and Dynamic Power Management(DPM) . DPM preserves power by closing down parts of the sensor node which are not currently used or active. A DVS method varies the power levels in sensor node based on the non-deterministic workload. By changing the voltage along with the frequency, it is probable to obtain quadratic reduction in power consumption.

3.1.5 Sensors

Sensor act as module, device or subsystem used to sense actions or changes in its environment and send the information to other electronics, frequently computer processors. A sensor is constantly used with other electronics, simple as a light or as complex as a computer. Sensors used by wireless sensor nodes to capture data from their environment. Since wireless sensor nodes are normally very tiny electronic devices, they can only be prepared with a limited power source of less than 0.5-2 ampere-hour and 1.2-3.7 volts.

Sensors are classified into three categories: passive, narrow-beam sensors; passive, omnidirectional sensors; and active sensors. Without actually manipulating the environment by active probing, passive sensors sense the data. The energy is needed only to amplify their analog signal, so that it is called self-powered. Active sensors actively explore the environment, for example, radar sensor and they require uninterrupted energy from a power source. Narrow-beam sensors have a well defined notion of direction of measurement, alike to a camera. Omni directional sensors have no notion of direction in their measurements. Many theoretical works on WSNs utilizes passive, omnidirectional sensors. Each sensor node has a certain area of coverage for which it can accurately and reliably report the particular quantity that it is monitoring. Several sources of power consumption in sensors are: conversion of physical signals to electrical ones and signal sampling, signal conditioning, and analog-to-digital conversion. Spatial density of sensor nodes in the field can be as high as 20 nodes per cubic meter.

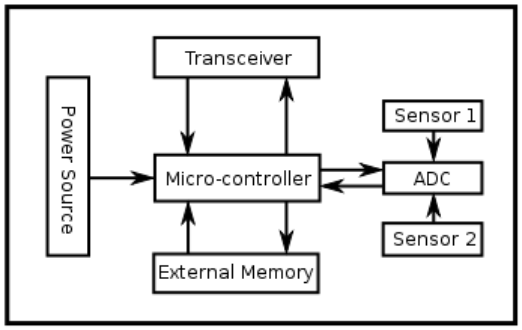

Fig 1. Sensor Node [1]

The components of sensor node are represented in fig 1. It consists of microcontroller, transceiver, power source, external memory, ADC and sensors. ADC gets signals from sensors. Power supplied to microcontroller.

3.2 Sensor Field

Sensor field is an area in which the nodes are placed. Wireless sensor node is frequently placed in difficult to reach out location. Each sensor node has a definite area of coverage for which it can reliably and precisely report the specific quantity that it is detecting.

3.3 Sink

A sink also known as data aggregation points is a sensor node, which receives, process and store data from the other sensor nodes.

3.4 Task Manager

The task manager also called as base station. It is a centralized point of control within the network, which mine information from the network and distribute control information back into the network. The base station is either a workstation or a laptop.

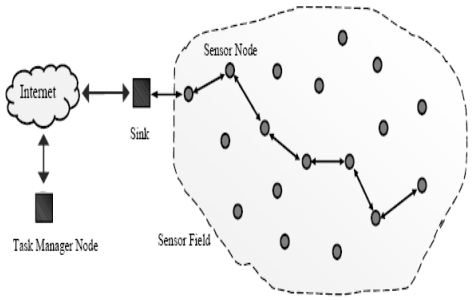

Fig 2. Components of Wireless Sensor Network

Fig 2 describes the component of Wireless sensor Network. The area that covers sensor nodes is termed as sensor field. Task manager connected to sensor nodes through internet and intermediate Base station.

IV. WIRELESS SENSOR NETWORK ARCHITECTURE

The OSI architecture Model followed as the most common WSN architecture. The WSN architecture includes five layers and three cross layers. Mostly sensor network require five layers, namely application, transport, network, data link & physical layer. The three cross planes are mobility management, power management and task management. These layers are used to complete the network and make the sensors work together to achieve complete efficiency of the network**.**

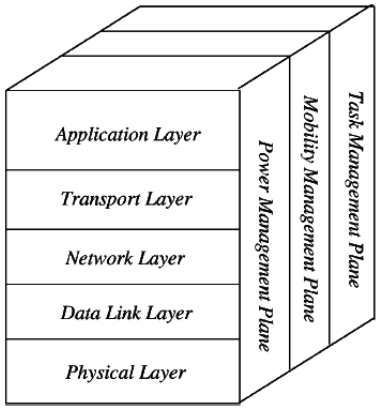

Fig 3. Wireless Sensor Network Architecture

Fig 3 represents the architecture and communication in Wireless Sensor Network with the Open System Interconnections layers and three management layers for task, mobility and power management respectively.

4.1 Application Layer: The application layer offers software for numerous applications that convert the data in a clear form to find positive information and is liable for traffic management. Sensor networks arranged in abundant applications in different fields such as agricultural, military, environment, medical, etc.

4.2 Transport Layer: The function of this layer is to deliver jamming avoidance and consistency. The transport layer is precisely needed when a system is planned to contact other networks. Providing a consistent loss recovery is more energy efficient so that TCP is not fit for WSN. In general, Transport layers can be separated into Event driven, Packet driven. Popular protocols in the transport layer are PORT (Price-Oriented Reliable Transport Protocol, STCP (Sensor Transmission Control Protocol) and PSFQ (pump slow fetch quick).

4.3 Network Layer

The main function of the network layer is routing, power conserving, partial memory, buffers, and sensor don't have a universal ID and have to be self-organized. There are a lot of on hand protocols for this network layer, they can be separate into flat routing and hierarchal routing or can be separated into time driven, query-driven & event driven.

4.4 Data Link Layer

The data link layer is responsible for multiplexing data frame detection, data streams, MAC & error control, confirm the reliability of point–point (or) point– multipoint.

4.5 Physical Layer

The physical layer provides a circumference for transferring a stream of bits above physical medium. This layer is liable for the selection of frequency, signal detection, generation of a carrier frequency, data encryption & Modulation. IEEE 802.15.4 is suggested as typical for wireless sensor network with low power consumption, cost, density, the range of communication to improve the battery life. CSMA/CA is used to support peer to peer & star topology.

V. SECURITY FUNDAMENTAL OF WSN NETWORK

In wireless sensor network the security is more challenging. Wireless sensor network and its applications are attacked by Intrusions and other attacks to interrupt the characteristics it serves. Wireless sensor network is frequently provided to the remote areas. Since sensor networks are commonly used in remote areas and in those areas, the operation of the network is left unattended, and unmonitored regularly that help the intruders to make an easy target for large attacks, unauthorized access and tempering. Sensor nodes have to negotiate with attacks due to resource tapered activities and operating in insensible surroundings also difficult to differentiate security violations from node failures. Problems are also created in mitigating link qualities and overall shut down of the network. These resource restrictions need security mechanisms that are designed for WSN applications, so that the limited resources can be used proficiently.

To maintain the wireless network secured, protect it from unauthorized access or unintended uses. There are three vital services for the security mechanisms are Confidentiality, Integrity and Availability are defined by The CIA security model [4]. Confidentiality defines that any illegal access to the network must be banned. Only consistent node of the network can access the resources. Integrity describes that a message must reach from sender to receiver without modification or changing. Sensitive information must not be changed or accessed by unauthorized individual.

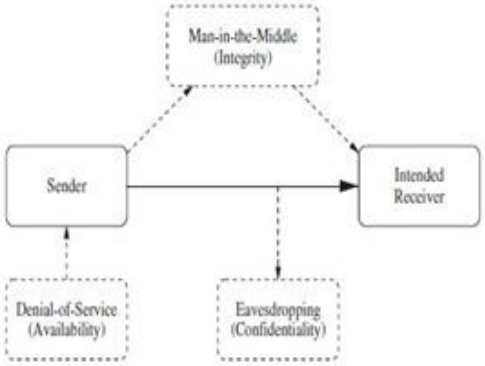

Fig4. Different types of attacks in CIA model

Availability guarantees all time uninterrupted access to the network for the legitimate nodes. Fig 4 shows some common attacks in CIA model. To prevent the greeting of a message by an unauthorized individual which is called Eavesdropping, suitable confidentiality procedure can be followed.

A Man-in-the-middle attack is when an unauthorized person receives a message from the sender then alters it before sending to the receiver. The authorized receiver never knows where the message came from and what occurs on transmission. Denial-Of-Service attack explains to an intruder's effort to interrupt the transmission or service that a sender provides to its receiver. Away from these three attacks of CIA model, authentication is another important term of establishing or confirming the identity of a user or a station, verifying that a data arrived from authorized user. Digital signature supports both authentication and acknowledgement of receiving the data to the proper receiver. Each communication network possesses its own way of integrity, confidentiality and availability. Security of network also relates with cryptography. The encryption-decryption techniques applied for the usual wired networks are not appropriate for wireless sensor networks [2, 3].

5.1 Security Threats in WSN

Wireless networks are vulnerable to security attacks because of the broadcast nature of the transmission medium. In addition, as WSNs nodes are unfriendly unsafe which are physically unprotected because of location adds an extra vulnerability to security. It's actually difficult and complicated to manage each node and defend them, when a sensor network is really outsized. Different types of security threats are always formed by the attackers to make the WSN system unsteady and unstable [5]. Two main types of attacks that an

intruder may adopt are (i) Passive attacks and (ii) Active attacks.

5.1.1 Passive Attacks

These attacks are refers to just listening the communication. An intruder watches the communications silently but do not make any changes in communication [6]. But, these attacks are normally beginning arrangements before the active attacks. This is mostly an attack against privacy. Eg. Eavesdropping, Traffic Analysis etc

(i) Eavesdropping

This is very frequent violence against privacy. By prying to personal data, an attacker simply learn the content of communication. When traffic delivers control data about configuration of sensor network, which consist of hypothetically thorough information, snooping or eavesdropping behave more efficiently against confidentiality.

(ii) Traffic Analysis

Messages transferred over the network are vulnerable yet if they are encrypted. There is a big opportunity that someone can analysis the patterns of communication. Sensor activities can possibly expose sufficient information to let an enemy to cause malicious harm to the wireless sensor network.

5.1.2 Active Attacks

Active attacks are referred to the modifying messages and genuine data steam or generating the false data in communication. An intruder may change the communicating messages, repeat old data streams or remove some selected part of important messages of communication.

(i) Replay Attack

It usually involves inactive imprisonment of the data unit and its succeeding retransmission to generate an unauthorized consequence [7, 8].This is carried out by an adversary or by an originator who interrupts the information and retransmits it.

(ii) Selective Forwarding

In this type of attacks, malicious systems act as the normal systems and drop selected packets. In selective forwarding attack, selection of the dropping nodes can be random.

(iii) Node Replication

In Node Replication attack, an intruder makes special easily affordable wireless sensor nodes and tricks entire network into accommodating them like the authentic nodes [9]. Node replication is hard to detect without centralized monitoring.

(iv) Masquerade Attack

This attack refers to the practice of a fake personality to gain the illegal access to any personal computer.

(v) Rushing Attack

A most modern threat that usually results in the denial-of-service (DoS) when utilized against all preceding network Routing practices. Attackers give out the malicious messages very quickly to authentic messages that reach later [10].

(vi) Modification of Messages

It is an attack where an attacker modifies or deletes the content of wireless network communication. In this attack, some piece of information is altered or real messages are delayed or recorded to produce an unauthorized effect [11].

Table 1. Security Attacks

Passive attacks	**Active attacks**
Traffic analysis	DoS attacks
Eavesdropping	Masquerade Attack
	Replay Attack
	Selective Forwarding
	Node Replication
	Wormhole Attack
	Sybil Attack
	Modification of Messages
	Sink Hole Attack
	Rushing Attack

5.1.3 Network Based Attacks

The two chief types of network base attacks are layer based attack and protocol based attack. These attacks frequently work on information during transmission time. These attacks also depart from the protocol.

A) **Application Layer Attacks**

This layer gears the services seen by users. Important application in WSN is time synchronization and data aggregation. Data aggregation sends data gathered by sensors to base station and time synchronization synchronizes sensor clocks for co-operative operations[12].

(i) DoS Attack

Denial of service (DoS) attacks is done by overwhelming targeted server by putting extra traffic than the server's maximum processing limit. DoS attack is naturally performed by overwhelming the targeted node with excessive requests to overload the systems and stops all or some legitimate requests from being answered. The scheme of WSN devices normally favors reduced cost over enlarged capabilities. These vital features of sensor network devices make them susceptible to DoS attacks.

(ii) Cloning attacks

In this attack the adversaries attacks a sensor node and deploys unlimited number of clones in the sensor network. Since these clones have unlimited access to the sensor network likes keys, legitimate IDs, other security credentials, etc. it can deploy itself into the sensor network operations similar to the legitimate node. If these clones are undetected then the sensor network is open to attackers, and making it extremely vulnerable.

B) Transport Layer Attacks

The aim of Transport layer protocols in WSN contain setting up of end-to-end connection, endto-end flow control, reliable delivery of packets, congestion control, and clearing of end-to-end connection. The mobile node is susceptible to the classic SYN flooding attack or session hijacking attacks. However, a WSN has an advanced channel error rate. Main attack in transport layers is flooding attack.

i) Flooding Attack

This is a Denial of Service (DoS) attack that destroys the entire network by flooding with large amount of traffic. Since the server is flooded with connections that cannot be completed, servers memory is completely occupied and letting its buffer to get full. Hence no further connections can be made, and thus resulting in a Denial of Service

C) Network Layer Attacks

Network layer is answerable for locating calculating ideal path to destination, by tampering with routing services such as replicating data packets and modifying routing information. Invaders can fail communication in WSN. Some attacks in Network are Hello flood, Wormhole Attack, Sybil Attack, Sink Hole Attack.

(i) Hello Flood

In this attack an intruder sends HELLO packets to adjacent nodes informing them the survival of its own so that it can obtain and send them information packets.

(ii) Wormhole Attack

This is mostly a very severe attack in which an intruder records the stream of bits or packets at specific position in wireless network and channels those to some other locations. Capturing and retransmitting of bit streams or packets could be done in choosy manner [12]. Wormhole Attacks usually used with the eavesdropping or selective forwarding attacks. Detection is relatively problematic when used in combination with Sybil attack.

(iii) Sybil Attack

In these attacks, a node presents as several duplicate nodes using the identities of other authentic nodes. Sybil attack actually goals to fault accepting schemes such as distributed storage and multipath routing [15]. Sybil attack causes an important risk to "geographic routing protocols". Position knowing routing normally requires different nodes to share data with their near nodes to capably route the geographically addressed packets.

(iv) Sink Hole Attack

A malicious node represents itself as a black hole to appeal and catch all traffic in WSNs. An attacker snoops requests paths then shows to targeted systems that it contains best quality or shortest distance to base station. Attacker itself stuck between the collaborating nodes, then it capable to make any changes in information passing among them [16].

D) Link layer attacks

This layer is responsible for access to the medium, physical addressing of the network's topology, error detection or correction, flow control and ordered mesh distribution [17].

i) Collision

Collision arises when two nodes attempt to send packet on the same time and same frequency. Packets loss, errors initiate in checksum at the receiver and therefore the receiver discarded the message. A stranger tries to do match with a legitimate node to send data exactly with it to keep the authentic node down from the network. To defeat this problem, error correcting code is used.

ii) Exhaustion

Here the battery power will be exhausted using an interrogation attack. A compromised node sends repeated data and thus consuming the battery power.

.

E) Physical Layer Attacks

The physical layer is in authority for the selection of the carrier frequency generation, signal detection, frequency, modulation, and encoding of the data. The nodes in WSN can be organized in a secure and hostile environment in which the attacker has physical access [18].

i) Jamming

This happens by prying with the radio frequencies of the networks devices. It is dissimilar from normal radio propagation in the way that it is unwanted and disruptive, thus resulting in denial-of-service conditions.

ii) Tampering

Tampering is also called as node capturing where a node is compromised. Tampering happens by physically modifying or altering and destroying the sensors nodes.

Table 2. Security Attacks in WSN Layers

Layers	Attacks
Application	DoS
	Cloning
Transport	Flooding
Network	Hello flood
	Wormhole Attack
	Sybil Attack
	Sink Hole Attack
Link layer	Collision
	Exhaustion
Physical	Jamming
	Tampering

Different types of attacks in WSN layers listed out in Table 2. DoS, Cloning in application layer, flooding in Transport layer, hello flood& wormhole attack in network, collision in Link layer and jamming in physical layer.

VI. CONCLUSION

The privacy and security of data are the major issues concerning about the wireless sensor networks. Security threatening issue is one of the major drawbacks of communication system. Malicious or bad intruders are present everywhere and they will remain forever to gain success of their own by making this types of useful and important network defenseless or imperceptible. It is necessary to keep the system trustworthy and highly secured for outsiders. A few important steps should be maintained for uncompromised security of the network. DoS attack on WSN reduces the performance of the system. Special prevention techniques are required to deal with the DoS attacks in WSN. There are some approaches and techniques to prevent DoS attacks on the system. Future work is to propose cooperative immune system for wormhole attack with Sybil attack (DoS attack). This immune system is a security algorithm that detects and prevents the combination of Sybil attack with wormhole attack and it improves the accuracy of the system as well as provide authentication for each sensor node.

REFERENCES

[1]. L.Devi, Dr.S.P.Shantharajah, "A survey on Authenticationand SecurityMaintenance in Wireless Sensor Network", International Journal of Computer Science and Mobile Computing, Vol.4, Issue.5, pp. 53-70, 2015.

[2]. Anju Bala, "Security Attacks and Challenges of Wireless Sensor Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol.3, Issue 1, ISSN: 2456-3307 2018.

[3]. Waltenegus Dargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks", Wiley Series on WirelessCommunicaions and Mobile Computing. pp. 268, 2010.

[4]. Al-Sakib Khan Pathan, Hyung-Woo Lee and ChoongSeon Hong, "Security in Wireless Sensor Networks: Issues and Chaallenges", ICACT Transactions on Advanced Communications Technology, pp: 1043-1048, 2006.

[5]. Mohammad Hossain, UmmeMuslima and Humayra Islam, "Security analysis of wireless Sensor Network A Literature Review", Journal of Multidisciplinary Engineering Science and Technology, Vol. 2, Issue 1, ISSN: 3159-0040, 2015.

[6]. Mohit Saxena, "Security in Wireless Sensor Networks - A Layer Based Classification", Cerias Tech Report, 2007.

[7]. Syverson, Paul " A taxonomy of replay attacks [cryptographic protocols]", Computer Security Foundations Workshop VII, Proceedings. IEEE, 1994.

[8]. Das and ManikLal, "Two-factor user authentication in wireless sensor networks", IEEE Transactions on Wireless Communications, pp. 1086-1090, 2009.

[9]. Zhu and Wen Tao "Detecting node replication attacks in wireless sensor networks: a survey" Journal of Network and Computer Applications, pp. 1022-1034, 2009.

[10]. Hu, Yih-Chun, Adrian Perrig, and David B. Johnson,"Rushing attacks and defense in wireless ad hoc network routing protocols", Proceedings of the 2nd ACM workshop on Wireless security, 2003.

[11]. Beddoe, Marshall A., and KowsikGuruswamy, "Modification of messages for analyzing the security of communication protocols and channels", U.S. Patent No. 8, 2013.

[12]. Damandeep Karu and Parminder Singh, "Various OSI Layer Attacks and Counter measure to Enhance the Performance of WSNs during Wromhole Attack", International Journal on Network Security, Vol.5, No.1, 2014.

[13]. Mohamed-LamineMessai, "Classification of Attacks in Wireless Sensor Networks", International Congress on telecommunication, pp. 23-24,2014.

[14]. Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff," LITEWORP: a light weight Countermeasure for the wormhole attack in multihop wireless networks", International Conference on Dependable Systems and Networks ,IEEE, 2005.

[15]. Chris Karl of, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", pp. 299-302, 2003.

[16]. Ngai, Edith CH, Jiangchuan Liu, and Michael R. Lyu,"On the intruder detection for sinkhole attack in wireless sensor networks", Vol. 8,IEEE International Conference on Communications,IEEE, 2006.

[17]. Hector Kaschel,Jose Mardones and Gustavo Quezafa, " Safety in Wireless Sensor Networks: Types of Attacks and Solutions", Studies in Information,Vol.22,No.3,pp.323-329,2013.

[18]. Azzem Mohammed Abdul and Syed Umar,"Attacks of Denial of Service on Networks Layer of OSI Model and Maintaining of Security",Indonesian Journal of Electrical Engineeering and Computer Science,Vol.5,No.1,pp.181-186,2017.

T.Vijayalakshmi" Wireless Sensor Network and Its Security Threats – A Study" International Journal of Engineering Research and Applications (IJERA) , vol. 8, no.12, 2018, pp 13-20