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
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.249 – 267

Wireless Sensor Networks: A Survey on Security Threats Issues and Challenges

Asha P N[1], Mahalakshmi. T[2], S.Archana[3], Dr. S.C.Lingareddy[4]

[1]Research and Development center Bharathiar University, India

[2]Shri Pillappa College of Engineering, Bangalore, India

[3]Shri Pillappa College of Engineering, Bangalore, India

[4]HOD, Dept. of CSE, Alpha College of Engineering, India

ABSTRACT: Wireless sensor network (WSN) is an emerging technology that is growing rapidly since from decades, which has posed unique challenges to researchers. Today wireless communication technique has become an essential tool in any application that requires communication between one or more sender (s) and multiple receivers [14]. Due to the inclusion of wireless channel in WSN, security has become a huge concern. Even though there is numerous ways to secure a wireless network and protect the network from numerous attacks, providing 100% security and maintaining confidentiality is a huge challenge in recent trends [14]. Here, we will present you a survey about various security threats to wireless network, the various advancement in securing a network and the various challenges in implementing the same. Lastly it proposes some security mechanisms against these threats in wireless sensor network.

Keywords- motes, cryptography, adversary, security, goal, challenge

---

1. INTRODUCTION

Wireless sensor network (WSN) are the clique of spatially distributed and dedicated sensors to monitor physical or environmental conditions such as temperature, pressure, etc. and systematizing the collected data through the network to a main location. Collecting the information from the physical world is one of the primary goals for wireless sensor networks. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future [1]. Wireless sensor network (sometimes also called as wireless actuator network) [2] is built of sensor nodes that varies in size from that of shoebox down to the size of a grain dust. WSN are infrastructure independent, where they can be built virtually to work in any harsh environment, without the need of wired connection. The development of WSN was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and consumer applications(such as, industrial process monitoring and control, machine health monitoring and so on)[2].

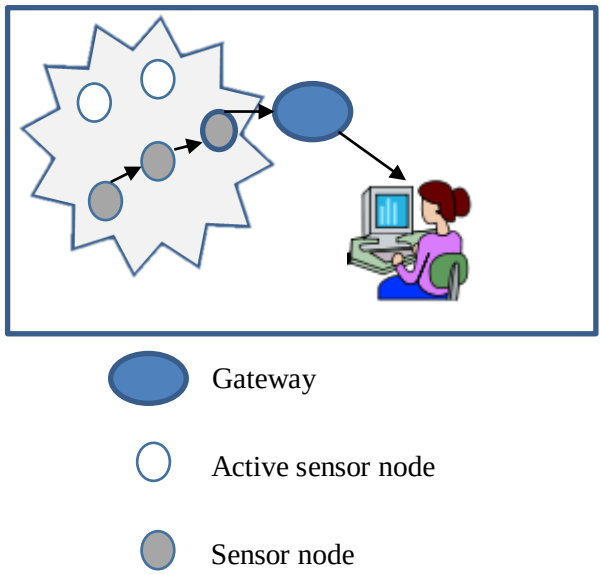

Fig.1.1 wireless sensor network

Every sensor node in the network contains components like controller, transceiver, external memory, power source and one or more sensors (discussed in the below sections). Base stations are the other components of WSN, which act as a gateway between the sensor nodes and end user [3]. In many applications, WSN communicates with a LAN (Local area network) or WAN

(wide area network) by the help of gateway (which act as a bridge between two networks) [3]. Other special components can be routers (intended to compute, calculate and distribute the routing tables) in routing based network [3]. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communication bandwidth. The sensor nodes stood in WSN may gamut from few to several hundreds or even thousands. Cross layer approach is applicable for WSN than using a traditional layered approach for wireless communication, because traditional layered approach does not have ability to adopt to changing environments, cannot share different information among different layers [3]. So the cross layer can be used to make optimal modulation to improve transmission performance, such as data rate, energy efficiency, QoS (Quality of service), etc. The contemporary networks are bidirectional also empowering control of sensor activity. Recent advances in micro-electro mechanical systems (MEMS) technology has made it possible for building sensors [4].There are three subsystems for every node in the Wireless sensor network (WSN) [4]:

i. Subsystem which is used to sense the environment.
ii. The processing subsystem which performs local computations on the sensed data, and
iii. The communication subsystem which is responsible for message exchange with neighboring sensor nodes.

These sensor nodes used in WSN are also termed has "motes". In other words WSN can also be called as collection of motes.

A. *Characteristics of WSN*

The motes in WSN have the ability to collect the data (moisture, light, etc.) and ability to communicate with each other. These minuscule, inexpensive motes (sensor nodes) have the following characteristics [2]:

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to withstand harsh environmental conditions
- Mobility of sensor nodes
- Ability to cope with node failures

- Low processing power and radio ranges
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ease of use cross-layer design

Collection of motes toil together to attain a common goal. For example [3], if the goal is to collect information about the microclimates around all sections of redwoods in a forest, the motes are placed in trees to form a network. After the deployment of the motes in the network, they communicate with other motes to transmit the information among other motes to reach the main computer. All the motes in the WSN will not involve in the data communication, due to the motes maximum broadcast range and interference from the surroundings [3]. Fig1.3 shows the data being transmitted from the group of sensor nodes to sink node and finally to the user.

The limited broadcast range can be achieved by saving the considerable amount of power by each mote. This broadcast range is approximately 30 meters [3]. If the motes have a short radio broadcast range, and many motes are more than 30 meters off the ground, how can one collect data from the motes farthest away from the computer (or station)? Motes solve this problem by packaging their information and broadcasting it to multiple other motes, which then communicate with others, to find the most rapid or successful route for the information to travel to reach the main computer located elsewhere [3]. Communication with other motes in WSN happens by the help of radio transceiver used in each mote. The information from the child motes are transmitted to the parent mote, where that information is given for computer or PDA type device (which is used to collect and process the data given by child motes to its parent mote). Fig 1.2 illustrates one possible path the data can travel between the motes and the computer/station.

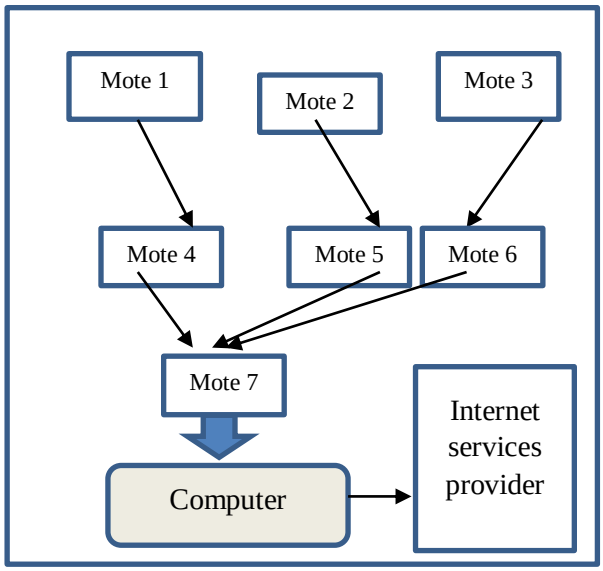

Fig.1.2 The Motes 1 through 6 are termed as children motes, Mote 7 is the parent mote. The "Computer" can be any type of Computer (like PDA, laptop, etc.), that is capable of accessing the internet via a specified ISP. The arrows connecting the motes are not fixed, and to illustrate this, they are purposefully organized.

The motes in WSNs communicate within themselves and with a user (not necessarily near a network location). These motes deployed in the WSN collect the data from the surrounding about what is happening and perform some action according to the data collected (be it moving, setting of alarms, or simply recording of data [3]). Any change that occurs in the WSN affects each mote the collected information from the children motes is routed to the parent mote. This parent node is connected to a computer of higher power that performs a function for which the motes are not designed, one such function is to access the internet and transfer the motes data to the user's computer. Even the user can be involved in the communication with the motes. If the user gives some directives, the directives will be sent over the internet to the computer (or station) [3]. The computer (or station) will communicate the same directives to the parent mote,

Which then disperses the message amongst its "children" [3]?

B. *Components of WSN*

Each sensor node in WSN consists of components like microcontroller, radio transceiver (external or internal antenna), energy source (usually a battery), external memory, and one or more sensors.

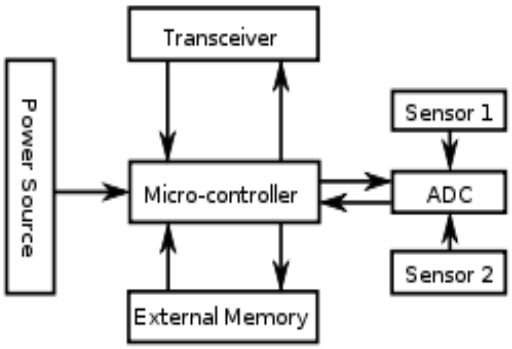

Fig.1.3 Typical architecture of sensor node

1) *Controller:* Microcontroller is the most commonly used controller in WSN, other controllers that can be used are: a general purpose desktop microprocessor, microcontroller, digital signal processor, ASICs and FPGAs. The controller processes the data, performs tasks and controls the functionality of other component in the sensor node [5]. Microcontroller are preferred to be used more in WSN because of its flexibility to connect to other devices, low cost, less power consumption and ease of programming. Usually microprocessor is not used in embedded systems because of its high cost and high power consumption physiognomies.

2) Transceiver*:* Transceiver must exist for every mote, which helps to communicate fully with the other motes in the WSN. Transceiver has both radio transmitter and radio receiver in it. While transmitting, it makes use of transmitter to broadcasts the data too other motes according to the network connections. In other way, while receiving, it receives the information from another motes radio and transmits it to the electronic brain.

3) *External memory:* From an energy perspective, the most relevant kinds of memory are the on-chip memory of microcontroller and flash memory off-chip RAM is rarely, if ever, used [5].Flash memories are used because of its storage capacity and cost constraint. The memory depends on the application to be used. The two categories of memory based on the purpose of

storage are: user memory used for storing application related or personal data, and program memory used for programming the device, program memory also contains identification data of the device if present [5].

4) *Power source:* The sensor node (mote) in WSN is usually battery operated (rechargeable or non-rechargeable) or an embedded form of energy harvesting. Since these motes are deployed in unreachable sites, so replacing the batteries every now and then is a tedious job. Hence, every mote in WSN must consume minimum energy to carry out the task like sensing, transmission, computation (processing of data), etc. Motes consume more energy for data transmission than performing any other operation. If the mote is designed to last a very long time, say one year, it will have a larger power source than a mote that is only meant to run for a month, the power sources usually range between a couple of AA batteries, and a watch battery, but with the new smart-dust motes, also called "Spec", they can collect enough energy to sustain themselves from ambient light, or even vibrations [3].

5) Sensors: WSN is built of nodes from a few to several or even thousands, where each mote is connected to one (or sometimes) sensors [2]. These sensors used by wireless sensor node have the characteristics of capturing the data from physical world. The size of each mote vary from the applications they are used by, usually size of mote vary from iota of dust to that of shoebox. Most sensor nodes are small in size, consume little energy, operate in high volumetric densities and are adaptive to the changing environment [5]. As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source of less than 0.5-2 ampere-hour and 1.2-3.7 volts [5]. Each sensor node has a certain area of coverage in WSNs. Analog-to-digital convertor (ADC) is being used to convert the analog signals (that produced by the sensors) into digital signal. Spatial density of sensor nodes in the field may be as high as 20 nodes per cubic meter [5].

C. *Applications of WSN*

The sensor nodes are used in wide ranges of application, which require constant monitoring and detection of specific events, some of the application that makes use of sensor nodes are listed below [2]:

1) *Area monitoring:* This is the application that is used most commonly, where constant monitoring of specific events is required. For example, in military application, the use of sensors detects enemy intrusion and nuclear, biological and chemical attack detection.

2) *Forest fire detection: A* collection of sensor nodes are deployed to detect when the fire as flinched in the forest. The sensor used in the mote collects the information from the physical world like temperature, humidity and gases which is produced by fire in the trees or vegetation, use of WSN in this application helps the fire brigade to know when a fire is started and how it spread in a network [2].

3) *Air pollution monitoring:* The sensor nodes are deployed in various cities (London, Stockholm and Brisbane) to monitor the concentration of dangerous gases for cities [2]. The wireless technology is an advantage that is taken in this application, which makes them more portable for testing readings in different areas.

*4)Natural disaster prevention'*s can effectively act to prevent the consequences of natural disasters like floods, wireless nodes have successfully deployed in rivers where changes of the water levels have to be monitored in real time [2].

5) *Water/waste water monitoring:* This application includes checking the quality of underground or surface water and safeguarding the country's water infrastructure for the salvage of both human and animal [2]. The sensor nodes can be deployed permanently in the water bodies (like dam, river, lakes, oceans etc.) to monitor the properties of water.

2. SECURITY THREATS AND ISSUES IN WSN

Providing security is one of the major challenges in WSN. The sensing technology combined with low processing power and wireless communication makes it lucrative for being exploited in abundance in future [1].These are the constraints on which the WSNs is more vulnerable to threats.

A. *Types of attacks*

WSNs are vulnerable to security attacks. Furthermore, WSNs have an additional vulnerability because nodes are often deployed in a hostile or dangerous environment where they are not physically protected [6]. Basically the attacks are classified into two types, according to the interruption of communication act. They are:

1) *Passive attack:* The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack [1]. This attack obtains the data exchanged in the network without interrupting the communication. The attacks against privacy are passive in nature [6]. Passive attacker may do the following functions:

- Attacker is similar to a normal node and gathers information from WSN;
- Monitoring and eavesdropping from communication channel by unauthorized attackers;

The illicit feats like monitoring and eavesdropping, traffic analysis and camouflage adversaries come under passive attacks. Fig.2.1illustrates various kinds of passive attacks.

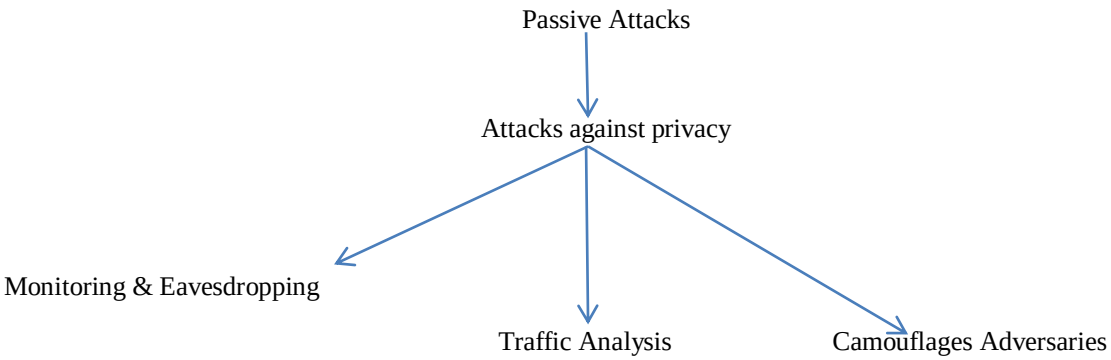

Fig.2.1 Illustrates passive attack

Monitor and Eavesdropping is the most serious security threat to a WSN, the adversary (attacker) discovers the communication contents by snooping to the data. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection [7]. The omnidirectional antenna present in the sensor node is liable to eavesdropping, which can be reduced by making use of directional antenna (radiates radio signals in desired location). Here an attacker node may get the MAC address.

Traffic analysis is little more complicated and hard to detect, it would be like this if we had a way to hide the information on a message and the hacker still viewed the information it would be traffic analysis attack. Even though the message is encrypted, it still leaves the possibility of analyzing the communication patterns [1]. Sensor activities reveal the enough information to the intruder to harm the network [8].

Camouflage Adversaries Intruder can insert their node or compromise the nodes to hide in the sensor network. Where that node can replicate itself has a normal node to attract and misroute the packets it is going to collect. Passive attacks are very difficult to discern, because an attacker does not modify the data, he just monitor and eavesdrops to obtain the data. When the messages are exchanged between the sender and receiver, neither the sender nor the receiver is aware that a third party (intruder or adversary or attacker) has read the messages. Encryption technique can be used to prevent this type of attack.

2) *Active attack:* The unauthorized attacker monitors, listens to and modifies the data stream in the communication channel are known as active attack [1].This kind of attacker performs the following operation:

- Injecting fault data into the WSN;
- Impersonating;
- Packet modification
- Unauthorized access, monitor, eavesdrop and modify resources and data stream;
- Overloading the WSN;

Attacker modifies the data, while it is being transmitted between the two sensor nodes. Attacker can be present either inside or outside the sensor network. Hence, the attacker can be of two types, external and internal attacker.

External attacker: If the attacker is out of the WSN's scope it is termed has outsider (external). This type of attack may lead to effects like:

- Jamming the entire communication of the WSN
- WSN's resource consumption

Internal attacker: If the attacker is in the WSNs scope it is termed has insider (internal). An authorized node in the network can get the required confidential data. The goal of these attacks type is:

- Revealing secret keys
- Partial/total degradation

Routing attack in sensor networks is the type of attack happens when sensor nodes are routing the information across the network. The attack which act on the network layer is called routing attacks [1]. Here, the attacker can involve in changing the routing information.

Selective forwarding is the attack, the adversary covenants a node, that it scrupulously forwards some messages and plunge the others, and this hampers the quality of service in WSN. Suppose if the attacker drops all the packets that received by particular node or group of nodes then the adjacent sensor node becomes conscious and may evaluate that it is a blemish node. In order to avoid this attacker forwards some selective packets. It is hard to figure out selective forwarding attack in sensor network.

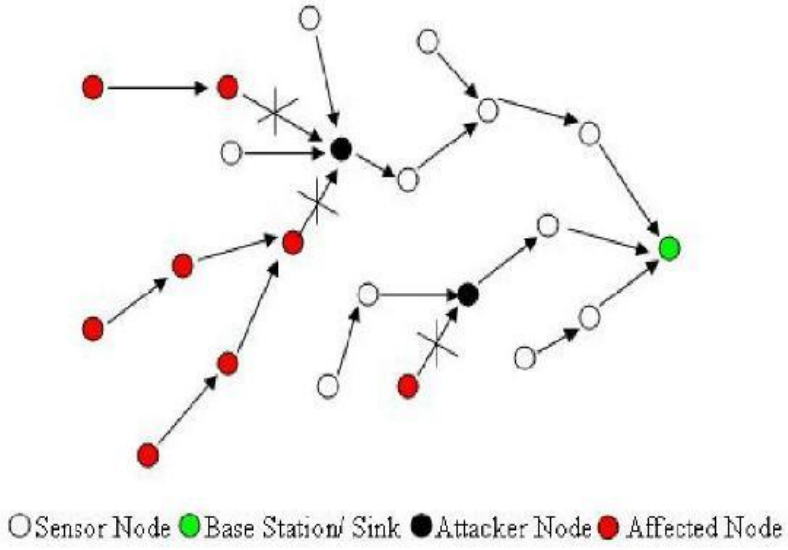

Fig.2.2 Selective forwarding

Here in the above figure, some of the information from the sensor node (affected node) are being dropped, which is shown by a cross mark for illustration. And information from the other sensor nodes is transmitted by the attacker node in the network.

Attacks on information in transit are the primary goal of sensor network is to collect the information from environmental conditions. This information can be spoofed, altered or replayed by an attacker in the WSNs. Thus the altered packets provide wrong data to the base station (sink node). Always the sensor nodes in WSNs monitor the physical condition and report that information to the sink node. Wherein this type of attack the sink node is not provided with correct information.

Black hole (or sinkhole attack) is the black hole attack is also termed as sink hole occurring at the network layer, where the attacker builds a covenant node that seems to very attractive in the sense that it promotes zero cost routes to neighboring nodes with respect to the routing algorithm [9]. This results maximum traffic to flow towards this false node, to attract all the packets that are destined to the sink node. This false node may modify or drop the packets coming through it. Nodes adjoining to this harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction [9]. Here in the fig.2.3 shows how a compromised node attract the packets from particular group of sensor nodes. The received packets by the compromised node is altered or dropped in the network. The altered packets are sent to the sink node (which is provided with the wrong information).

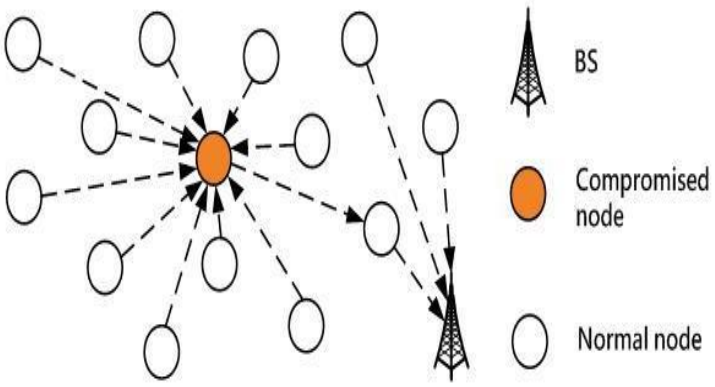

Fig.2.3 Sinkhole attack

In wormhole attack, a pair of awful nodes creates a wormhole tunnel to replay the packets. Malicious node receives the packet in one section of the network and sends them to another section of the network [9]. Attacker node copies a portion or whole packet and speed up to send the packet the through the wormhole tunnel, so that the packets arrive first to the destination before the original packets traverse the usual routes. This may cause congestion and retransmission of packets squandering the energy of innocent nodes. The fig.2.4 shows the wormhole attack.

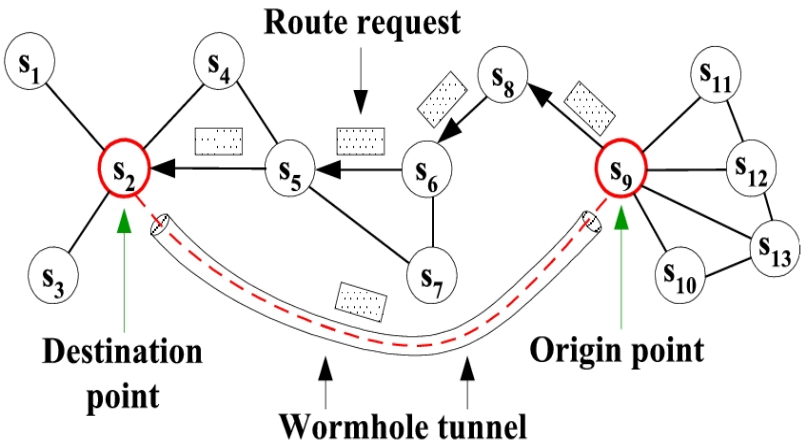

Fig.2.4 Wormhole attack

In Node subversion a particular node in the sensor network is captured by the adversary to obtain the necessary information from it. The node that is captured may reveal the information including the cryptographic keys and thus compromising the entire network.

In Message corruption an adversary node may modify the message that is transmitted in the network. The message is corrupted when the contents of the message is modified by the attacker.

False node the injection of malicious node into the network by an adversary is called as false node. This malicious node feeds the false data into the network or avoids the passage of true data.

Passive information gathering is an adversary with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream, interception of message containing the physical locations of the sensor nodes allows an attacker to locate the nodes and destroy them [10]. By making use of powerful resources the data is made available to the adversary node, when data is not encrypted. So encryption technique can be used to avoid these types of attacks. Besides the location of sensor node, an adversary can observe the application specific content of the messages including the message ID, timestamp and other fields [10].

Denial of services (DoS) is a simplest Dos attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packet and thus prevents legitimate network users from accessing services or resources to which they are entitled [10].A typical Dos attack structure is explained in the fig.2.5.

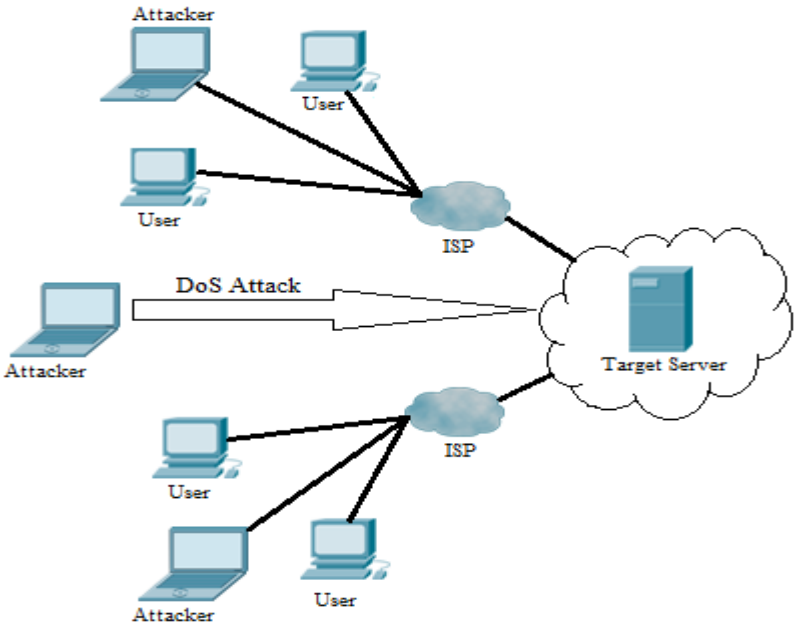

Fig.2.5 Denial of service

In Physical attacks the senor network is highly susceptible to physical attacks since they operate in hostile outdoor environment, .i.e. threats due to physical node destructions as the sensors are small in size, deployed with unattended environment [8]. Physical attacks are more dangerous because they destroy the sensors permanently, where the losses are irreversible. So there are chances of losing the cryptographic secrets, tamper with the associated circuitry, modify programming the sensors or replace them with malicious sensors under the control of the attacker [8].

3. SECURITY CHALLENGES IN WSN

A. *Wireless medium*

Transmission in WSN is wireless in nature. Due to the inclusion of wireless medium WSN are more prone to security threats. Broadcasting nature in WSN makes eavesdropping simple for an attacker. The packets captured can be altered or replayed by an adversary.

B. *Ad-Hoc deployment*

The sensor network is infrastructure independent and can be built virtually at any nasty condition. The nodes can be deployed by air drop, so nothing is known of the network topology prior to deployment [1]. Even for deployment of sensor node, some of the node may

fail due to some reasons (battery lifeless), so when these nodes are replaced by other sensor node, the network must support self-configuration. Sensor network can Ad hoc network having the same flexibility and extensibility, sensor networks crave every sensor node to be independent and capable of being drawn enough to be self-organizing to different situations [11]. Hence deployment is dynamic in WSNs.

Ho*stile environment*

The next challenging factor is the hostile environment in which sensor nodes function, motes face the possibility of destruction or capture by intruders [1].

D. *Immense scale*

WSN must be highly scalable in nature, any addition node can be added in future (depends on the application) to the existing network. Simply networking tens to hundreds of thousand nodes has proven to be a substantial task; the proposed scale of sensor networks plays a significant challenge for security mechanisms [1].

4. SECURITY GOALS FOR WSN

The security goals are classified into two types: primary and secondary goals.

A. *Primary goals*

Primary goals are known as Standard security goals such as confidentiality, integrity, authenticity and availability [1].

1) Data confidentiality: Confidentiality is an ability to hide the message from a passive attacker and is the most important issue in network security [12]. In other words, confidential data is made available only to the authorized node in the network. Sensor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in WSN [12]. The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of the message [11].

2) *Data integrity:* The integrity of the message is said to be lost, when the contents of the message is altered (by an adversary) after sender sends it, but before it reaches the intended recipient [11]. Even if the WSN has confidentiality measures there is still a possibility that the data integrity can be compromised by alterations [1].

The integrity of the network will be trouble when [1]:

A malicious node present in the network injects false data

Unstable conditions due to wireless channel cause damage or loss of data

3)*Data authentication:* An adversary is not only limited to modify the data packet but it can change the complete packet stream by adding extra packets, so the receiver needs to confirm that the data used in any decision-making process comes from the correct source [12]. Data authenticity is an assurance of the identities of communicating nodes. Authentication mechanism helps to identify proof of identities, which ensures that origin of message or document is correctly identified [11].

4) *Data availability:* The principle of availability states that resource should be made available to authorized parties at all times [11]. For the proper operation of the network, the sink node must be made available, because failure of the sink node threatens the entire network. It is the ability of the node to utilize the resource and the network is available for the messages to move on [12].

B. *Secondary goals*

1) *Data freshness:* Data freshness ensures that the data communicated is recent and no previous messages have been replayed (repeated) by an adversary [11]. For ensuring the freshness of a packet, a timestamp can be attached to it. Destination node can compare the timestamp with its own time clock and checks whether the packet is valid or not. Data freshness ensures that message is recent, where the old message is not replayed. This requirement is especially important when there are shared-key strategies employed in the design and needs to be changed overtime [12].

2) *Self organization*: A typical WSN may have thousands of nodes fulfilling various operations, installed at different locations [11].Sensor networks are also ad hoc networks, having the same flexibility and extensibility, Sensor networks crave every sensor node to be independent and ductile enough to be self-organizing and self-healing according to different situations [12]. There is no fixed infrastructure available for the network management, so nodes must themselves adapt the topology and deployment strategy [12].

3) *Secure localization'*s makes use of geological based information for recognition of nodes, or for accessing whether the sensors correspond to the network or not, because some attacks

work by investigating the location of the nodes. Sensors may get displaced while deploying them or after a time interval or even after some critical displacement incident [12].

5. SECURITY MECHANISM IN WSN

Security mechanism is actually used to detect, prevent and recover from the security attacks [6]. Fig.4.1 shows the order of security mechanism. Some of the key mechanism (discussed in below sections) is essential before developing the intrusion detection system. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high-level (secure group management, intrusion detection, secure data aggregation) and low-level mechanism (key establishment, secrecy, privacy, secure routing and resilience to node capture) [6].

A. *Key establishment and trust setup*

Cryptographic key establishment is chief concern in setting up the sensor network. This technique need to scale to networks with hundreds or thousands of nodes. Security can be achieved in sensor network by encrypting the message.

B. *Secrecy and authentication*

Most of attacks like eavesdropping, injection of false node and modification of packets can be prevented by using cryptography technique. Cryptography provides high level of security but requires that keys be set up among all the end points and be incompatible with passive participation and local broadcast [6].

C. *Privacy*

WSNs must potency privacy. Initially sensor network are deployed for legitimate purpose might subsequently be used in unanticipated ways, providing awareness of the presence of sensor nodes and data acquisition is particularly important [6].

D. *Secure routing*

Routing and data forwarding is a crucial service for enabling communication in sensor networks, unfortunately, current routing protocols suffer from many security vulnerabilities [6].

E. *Resilience to node capture*

Most of the time the sensor nodes are placed in the application that are easily accessible to adversary, such exposure raises a possibility that an attacker might capture sensor nodes, extract cryptographic secrets, modify their programming or replace them with malicious node under the control of an attacker [6].

F. *Secure group management*

Each and every node in WSN is limited in its computing and communication capabilities, however interesting in-network data aggregation and analysis can be performed by group of nodes [6]. Consequently secure protocols are required for group management, securely admitting new group member and supporting secure group communication [6]. The outcome of the group key computation is normally transmitted to a base station; the output must be authenticated to ensure it comes from the valid group [6].

G .*Secure data aggregation*

Depending on the architecture of the WSNs, aggregation may take place in many places in the network; all the aggregation locations must be secure. The data from the group of sensor nodes are aggregated and is sent to the sink node.

6. CONCLUSION

The WSNs continue to grow and become widely used in many applications today. So need for security plays vital. However WSN suffers from many constraints like limited energy, processing capability, storage capability, as well as unreliable communication and unattended operation, etc. Providing an appropriate security method to sensor node is fundamental aim in WSN. Most of the attacks are caused by the insertion of false information All the previously mentioned threats i.e. wormhole attack, sinkhole attack serve on the purpose to compromise the network to obtain actual data. Security has become the major issue in providing confidentiality to data in the network. We have identified the threats and vulnerabilities to WSNs. And we have summarized various categories of attacks. These threats can even prone to collapse the entire systems and network, hence adding security in a resource constrained WSN with minimum overhead provides significant challenges, and is an ongoing research. A better security protocol must be used for better functionality of sensor network. Thinking like the attacker people understands better their goals and responsibilities. This will help us to create better intrusion detection systems. Even though there are so many types of attacks and

the possibility of having the system compromised people must not be given to the security systems like firewall, antivirus software, cryptographic systems and software .There are many ways to provide security, the main one is cryptography.

REFERENCES

[1] Vikash Kumar, Anshu Jain and P N Barwal, "wireless sensor networks: security issues, challenges and solutions", IJICT, Vol. 4, 2014.

[2] https://en.wikipedia.org/wiki/Wireles_ sensor_network#/issues

[3] http://www.writing.ucsb.edu/faculty/holms/2E_motes_report.pdf.

[4] C.Siva Ram Murthy and B.S.Manoj: Ad hoc Wireless Netwoks, 2nd Edition, Pearson Education, 2005.

[5] http://en.m.wikipedia.org/wiki/sensor_node#/issues

[6] Yogesh Kumar, Rajiv Munjal, Krishan Kumar, "Wireless Sensor Networks and Security Challenges", IJCA, 2011.

[7] Jaspreet Kaur, Tavleen Kaur, "A Comparative Study of Techniques Used in Detection and Prevention of Black Hole Attack in Wireless Sensor Networks", IJRASET, vol.2, March-2014.

[8] Sahabul Alam and Debashis De, "analysis of security threats in wireless sensor networks", IJWMN, vol.6, April-2014.

[9] Aashima single and ratikasachdeva, "Review on security issue and attacks in wireless sensor network, IJARCSSE, vol. 3, April-2013.

[10] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA, 2010.

[11] Vani. Hiremani and Monali.Madne, " Security mechanism for wireless sensor network-A review", IJRITCC, vol. 1, December-2013.

[12] Kahina CHELLI, "Security issues in wireless sensor networks: attacks and counter measures", proceedings of the world congress on engineering, vol.1, Jully 1-3,2015.

[13] Teodor-Grigore Lupu, "Main Type of Attack in Wireless Sensor Networks".

[14] K.Venkataraman, J. Vijay Daniel, G.Murugaboopathi,"Various Attacks in Wireless Sensor Network: Survey", IJSCE, vol.3, March-2013.

