International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013

Security Attacks & Prerequisite for Wireless Sensor Networks

Sunil Gupta, Harsh K Verma, A L Sangal

***Abstract*— Due to encroachment of software and hardware developed and its technology a feasible network can be composed of small, inexpensive sensor with several attributes. Security is one of major concern for wireless sensor networks (WSN) because of lots of their critical applications. This paper describes the security attacks and its prerequisite and vulnerability for processing and collecting the information in WSN.**

***Index Terms*— security attacks, wireless sensor network, requirements and vulnerabilities.**

.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are a new technology foreseen to be used increasingly in the near future due to their data acquisition and data processing abilities. Security for WSNs is an area that needs to be considered in order to protect the functionality of these networks. Wireless sensor networks are collection of nodes where each node has its own sensor, processor, transmitter and receiver and such sensors usually are low cost devices that perform a specific type of sensing task. Being of low cost such sensors are deployed densely throughout the area to monitor specific event. The wireless sensor networks mostly operate in public and uncontrolled area; hence the security is a major challenge in sensor

Sensor Networks are envisaged in military, emergency and surveillance applications today, where sensor nodes need to send sensed data to the sink. In many applications under hostile environment, sensor nodes cannot be deployed deterministically and thus are randomly deployed into the field. With the development of Internet, more and more people need to access and share the remote resources, which bring great challenges for the security of information systems.

Security is crucial as they can be deployed in hostile environments with active intelligent opposition. One obvious example is battlefield applications where there is a pressing need for secrecy of location and resistance to subversion and destruction of the network. Less obvious but just as important security reliant applications include [18] Disasters, Public Safety and Home Healthcare. The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers [15]. A Physical layer: responsible for frequency selection, carrier frequency generation, signal deflection, modulation, and data encryption. A Data link layer: responsible for the multiplexing of data streams, data frame detection, medium access, and error control; as well as ensuring reliable point-to-point and point-to-multipoint connections. Network layer: responsible for specifying the assignment of addresses and how packets are forwarded .A Transport layer: responsible for specifying how the reliable transport of packets will take place. A Application layer: responsible for specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user.

The major contribution of this paper includes classification of security prerequisite, security Vulnerability and attacks in Wireless Sensor Networks. Section 2 gives the detailed information about the security requirements in Wireless Sensor Networks. Security Vulnerability and their classification are discussed in section 3. Major discussion is on Section 4 about the various security attacks followed by the conclusion section.

II. SECURITY PREREQUISITE FOR WSN

Sensor networks are used in a number of domains that handle sensitive information. Due to this, there are many considerations that should be investigated and are related with protecting sensitive information traveling between nodes (which are either sensor nodes or the base station) from been disclosure to unauthorized third parties.

A WSN is a special type of network. It shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The most important security requirements in WSN are shown in figure 1

Data confidentiality: Data confidentiality is a property of data, usually resulting from legislative measures, which prevents it from unauthorized disclosure. The security mechanism should ensure that no message in the network is understood by anyone except intended recipient. This is the most important issue in network security. Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential.

Manuscript received June, 2013.

Sunil Gupta, Department of Computer sc & Engineering, NIT Jalandhar, Jalandhar, Punjab, India

Dr. Harsh K Verma, Department of Computer sc & Engineering, NIT Jalandhar, Jalandhar, Punjab, India

Dr. A.L.Sangal, Department of Computer sc & Engineering, NIT Jalandhar, Jalandhar, Punjab, India

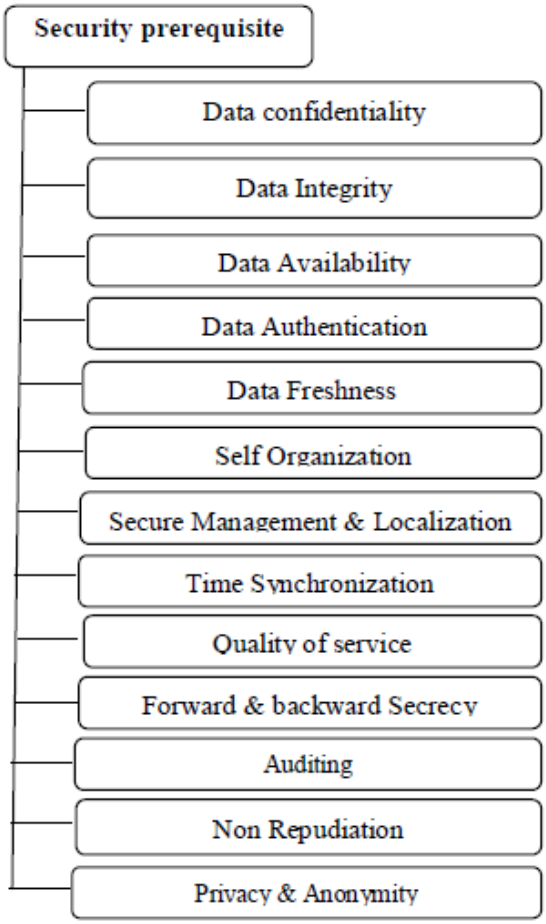

Fig: 1: Security Prerequisite for WSN

Data Integrity: The accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record. Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations.

Data Availability: Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. Availability ensures that services and information can be accessed at the time that they are required.ie. it must ensures that the desired network services are available even in the presence internal or external attack such as denial-of-service attacks In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks. Lack of availability may affect the operation of many critical real time applications.

Data Authentication: Authentication, which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network. Node Authentication objective is essential to be achieved when clustering of nodes is performed. clustering involves grouping nodes based on some attribute such as their location, sensing data etc and that each cluster usually has a cluster head that is the node that joins its cluster with the rest of the sensor network (meaning that the communication among different clusters is performed through the cluster heads). Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets [3].

Data Freshness: Freshness, which implies that the data is recent and ensures that no adversary can replay old messages Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. One of the many attacks launched against sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network. Data freshness objective ensures that messages are fresh, meaning that they obey in a message ordering and have not been reused.

Self Organization: Each node in a WSN should be self organizing and self-healing. This feature of a WSN also poses a great challenge to security. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station [4]. A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be devastating.

Secure Management & Localization: Management is required in every system that is constituted from multi components and handles sensitive information. In the case of sensor networks, we need secure management on base station level; since sensor nodes communication ends up at the base station, issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management. In many situations, it becomes necessary to accurately and automatically locate each sensor node in a WSN. For example, a WSN designed to locate faults would require accurate locations of sensor nodes identifying the faults. A potential adversary can easily manipulate and provide false location information by reporting false signal strength, replaying messages etc. if the location information is not secured properly. A sensor network designed to locate faults will need accurate location information in order to Pin point the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals.

Time Synchronization: Most of the applications in sensor networks require time synchronization. Any security mechanism for WSN should also be time-synchronized. Time synchronization is a critical piece of infrastructure in any distributed system. In sensor networks, a confluence of factors makes flexible and robust time synchronization particularly important, while simultaneously making it more difficult to achieve than in traditional networks.

Quality of Service: QoS is an overused term with various meanings and perspectives. Different technical communities may perceive and interpret QoS in

different ways. QoS generally refers to the quality as perceived by the user/application while in the networking community, QoS is accepted as a measure of the service quality that the network offers to the applications/users. For instance, RFC 2386 [5] characterizes QoS as a set of service requirements to be met when transporting a packet stream from the source to its destination two perspectives of QoS in WSNs:

A. Application-specific QoS

From this perspective, we may consider QoS parameters such as coverage, exposure , measurement errors, and optimum number of active sensors. In brief, the applications impose specific requirements on the deployment of sensors, the number of active sensors, the measurement precision of sensors and so on, which are directly related to the quality of applications.

B. Network QoS

From this perspective, we consider how the underlying communication network can deliver the QoS-constrained sensor data while efficiently utilizing network resources. Although we cannot analyze each possible application in WSNs, it is sufficient for us to analyze each class of applications classified by data delivery models, since most applications in each class have common requirements on the network. From the point of view of network QoS, we are not concerned with the application that is actually carried out; we are concerned with how the data is delivered to the sink and corresponding requirements. Generally, there are three basic data delivery models, i. e. , event-driven, query-driven, and continuous delivery models [6]. Before presenting the application requirements, we would like to provide some factors that characterize them as follows:

- End-to-end: The application may require end-to-end or non-end-to-end performance
- Interactivity: The application may be interactive or non interactive
- Characteristics: The application may or may not be delay tolerant
- Criticality: The application may or may not be mission critical

Forward and Backward Secrecy: a sensor should not be able to read any future messages after it leaves the network. It implies that a compromise of the current key should not compromise any future key.ie. No subsequent session keys can be recovered, given that an adversary managed to recover a contiguous subset of old session keys. While backward secrecy means a joining sensor should not be able to read any previously transmitted message. ie a compromise should not compromise any earlier key or an adversary managed to recover a contiguous subset of session keys, no previous session keys can be recovered.

Auditing: A major application of wireless sensor networks is for zero overhead sensing and data collection. Many existing systems can simply have miniature sensors installed in situ to study dynamics, vibrations, strain, or almost any parameter. The Energy Auditing project is the application of battery powered wireless networks to measure potential sources of energy. Characterization of data in context will allow us to review reliability and latency or these networks for wiring replacement in industrial and transportation scenarios.

Non repudiation: It denotes that a node cannot deny sending a message it has previously sent. It is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Non-repudiation (NR) is one of the security services (or dimensions as defined in the document X.805 by the ITU) for point to point communications. Secure communications need to integrate a service in charge of generating digital evidence (rather than simply information logs) in order to resolve disputes arisen in case of network errors or entities' misbehavior when digital information is exchanged between both points. This is the case of fair exchange protocols, certified emil applications (in which a digital message is exchanged for a proof of receipt) and contract signing protocols (in which digital signatures on a document need to be fairly exchanged).

Privacy and anonymity: , Sensor networks are tools for collecting information, and an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, an adversary that gains access to both the indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and thus extract details about the inhabitants' private activities. The main privacy problem, however, is not that sensor networks enable the collection of information that would otherwise be impossible. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information in a low-risk, anonymous manner. Remote access also allows a single adversary to monitor multiple sites simultaneously. Anonymity is the state of being un-identifiable within a set of objects; the anonymity set. Untraceability refers to the inability of an adversary in tracing individual data flows back to their origins or destinations [7]. Unlinkability means preventing an adversary from learning the identities of the source and the destination at the same time.

III. SECURITY VULNERABILITIES IN WSN

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Wireless Sensor Networks are vulnerable to various types of attacks. These are classified into two types

Physical Vulnerability and technical vulnerability

Physical vulnerabilities: Due to the deployment nature (in public and hostile environments) renders more link attacks ranging from passive eavesdropping to active interfering, sensor nodes would be highly vulnerable to capture and vandalism. WSN can scale up to thousands of sensor nodes without any fixed infrastructure. This implies the need to develop simple, flexible, and scalable security protocols. And new nodes addition and failure make the network topology dynamic and the solutions more complex Physical vulnerability is categorized as Authentication and secrecy attack and network availability attack shown in fig 2.

Attacks on secrecy and authentication: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

Eavesdropping: Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, and videoconference or fax transmission. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside. This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. 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.

Replay: A replay attack occurs when an attacker copies a stream of messages between two parties and replays the stream to one or more of the parties. Unless mitigated, the computers subject to the attack process the stream as legitimate messages, resulting in a range of bad consequences, such as redundant orders of an item. A replay attack can be prevented using a strong digital signature that include time stamps and inclusion of unique information from previous transaction.

Node Replication attack : Nodes replication attacks are one of the most redoubtable attacks, where an attacker compromising a node, uses its secret cryptographic key materials to successfully populate the network with clones of it. Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the nodeID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.[8]

Traffic analysis: Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted.

Passive monitoring: Attacks on network availability: attacks on availability of WSN are often referred to as denial-of-service (DoS) attacks Stealthy attack against service integrity: in a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential. DoS attacks against WSNs may permit real-world damage to the health and safety of people. The DoS attack usually refers to an adversary's attempt to disrupt, subvert, or destroy a network. However, a DoS attack can be any event that diminishes or eliminates a network's capacity to perform its expected functions [9].

a) Denial of services
b) Software stealing
c) Hardware Stealing
d) Modification of data
e) Damage a system by code
f) Corrupt data by code
g) Illegally User Privileges

Technological vulnerabilities: Security services in WSNs must consider the hardware constraints of the sensor nodes:

- Energy: energy consumption in sensor nodes can be categorized into three parts: energy for the sensor transducer,
- Energy for communication, energy for microprocessor computation.
- Computation: sensor nodes's processors are not generally powerful such as complex cryptographic algorithms cannot be used in WSNs.
- Memory: there is usually not enough space to run complicated algorithms after loading OS and application code.
- Transmission range: the communication range of sensor nodes is limited both technically and by the need to conserve energy. Each bit transmitted in WSNs consumes about as much power as executing 800-1000 instructions. Thus, communication is more costly than computation in WSNs.
- Wireless communication: its characteristics make traditional wired-based security schemes unsuitable. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications.

IV. SECURITY ATTACK IN WSN

Comparable to any wireless network, WSNs are suffering from many different attacks. In this section,We introduce the major attacks to WSNs. WSNs are vulnerable to various types of attacks. According to the security Prerequisite in WSNs, these attacks can be categorized as

Layered Wise: Layer wise attack is further categorized into five layers in which the physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation,

and data encryption [11]. The data link layer is responsible for multiplexing of data-streams, data frame detection, medium access control, and error control [11]. The network layer is responsible for routing, which is moving packets across the network using the most appropriate paths. The transport layer is responsible for delivering data to the appropriate application process on the host computers. The application layers are responsible for applications communicating between hosts

Type wise :This type of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur.

There are two types of attack:

Passive Attack: A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack: In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information.

Layer wise attack is further categorized into five layers in which an active attack is one where the attacker modifies network packets while they are in transit, or sends forged network packets .and A passive attack is one where the attacker merely eavesdrops on packets that others are sending, without injecting any new packets and without modifying any of the packets others have sent.

Physical layer attacks: Five types of Attacks in physical layer are Jamming, Interception, Eavesdropping, Radio Interference and Tampering.

Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic.

Interruption attacks are attacks against the availability of the network. These attacks can take the form of Overloading a server host so that it cannot respond. And blocking access to a service by overloading an intermediate network or network device.

An eavesdropping attack, also sometimes called sniffing, is a type of software attack where an attacker tries to gain access to private communications, using a utility such as Dsniff or Network Monitor, in order to steal the content of the communication itself or to obtain user names and passwords for future software attacks, such as a takeover attack.

Tampering: sensor networks typically operate in outdoor environments. Due to unattended and distributed nature, the nodes in a WSN are highly susceptible to physical attacks [12]. The physical attacks may cause irreversible damage to the nodes.

Data Link layer attacks

The different types of attacks are Traffic Analysis, Monitoring, Disruption MAC802.11, WEP Weakness, Channel Exhaustion, Unfairness, Interrogation and Sybil attack.

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted

WEP Weakness : When people do use WEP, they forget to change their keys periodically. Having many clients in a wireless network — potentially sharing the identical key for long periods of time

Interrogation: constantly request-to-send

Sybil attack. The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.

Network layer attacks: The network layer of WSNs is vulnerable to the different types of attacks such as: Wormhole, Sinkhole, Black hole, Byzantine, Flooding, Node Capture, Spoofing/Misdirection, Homing, Resources Consumption and Locator disclosure

Transport layer attacks: The attacks that can be launched on the transport layer in a WSN are Session Hijacking, Syv. Flooding

Session hijacking: It is the exploitation of a valid computer session—sometimes also called a session key to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server.

Syn flooding: This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produzes severe resource constraints for legitimate nodes.

Application layers attacks : The

different type of application layers attack is Overwhelm, BS Path DoS, Repudiation, Data Corruption and Malicious Code

Overwhelm: In this attack, an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.

BS Path DoS : In a PDoS attack, an adversary overwhelms sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replayed packets or injected spurious packets.

Repudiation Attacks - This makes data or information to appear to be invalid or misleading (Which can even be worse). For example, someone might access your email server and inflammatory information to others under the guise of one of your top managers. This information might prove embarrassing to your company and possibly do irreparable harm. This type of attack is fairly easy to accomplish because most email systems don't check outbound email for validity. Repudiation attacks like modification attacks usually begin as access attacks
Data corruption refers to errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data. Computer storage and transmission systems use a number of measures to provide data integrity, or lack of errors.

Malicious Code: Viruses and worms are related classes of malicious code; as a result they are often confused. Both share the primary objective of replication. However, they are distinctly different with respect to the techniques they use and their host system requirements. This distinction is due to the disjoint sets of host systems they attack. Viruses have been almost exclusively restricted to personal computers, while worms have attacked only multi-user systems.

Active attacks: These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data , Black hole, Byzantine, Rushing, Replay, Sinkhole, Spoofing, Flooding, Jamming, Sybil, Overwhelm, Wormhole. Fabrication, Hellow Flood, Node Subversion, Lack of Cooperation, Modification, Impersonation, Node subversion, Man in middle Attack, Selective Forwarding and False Node as shown in fig 3.

Sinkhole: The sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack [18], a compromised node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes with respect to the routing metric. As a result, the adversary manages to attract all traffic that is destined to the base station.

Spoofing: spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Flooding: The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding [14].

Jamming: Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic

Sybil: The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.

Overwhelm: In this attack, an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.

Wormhole: Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data [15].

DoS: Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

Fabrication: The notation “fabrication” is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [18].

Hellow Flood: An attacker sends or replays a routing protocol’s HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are Ultimately spoofed by the attacker.[13]

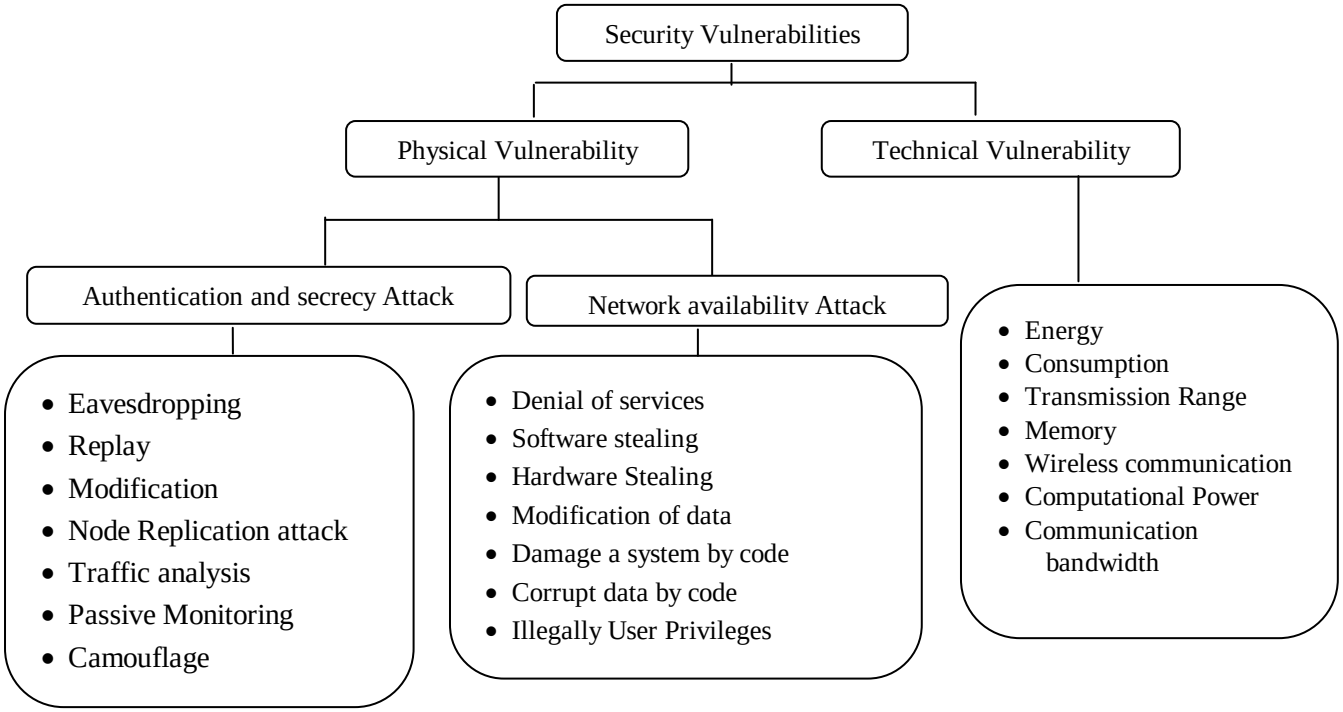

Fig: 2: Security Vulnerability on Wireless sensor networks

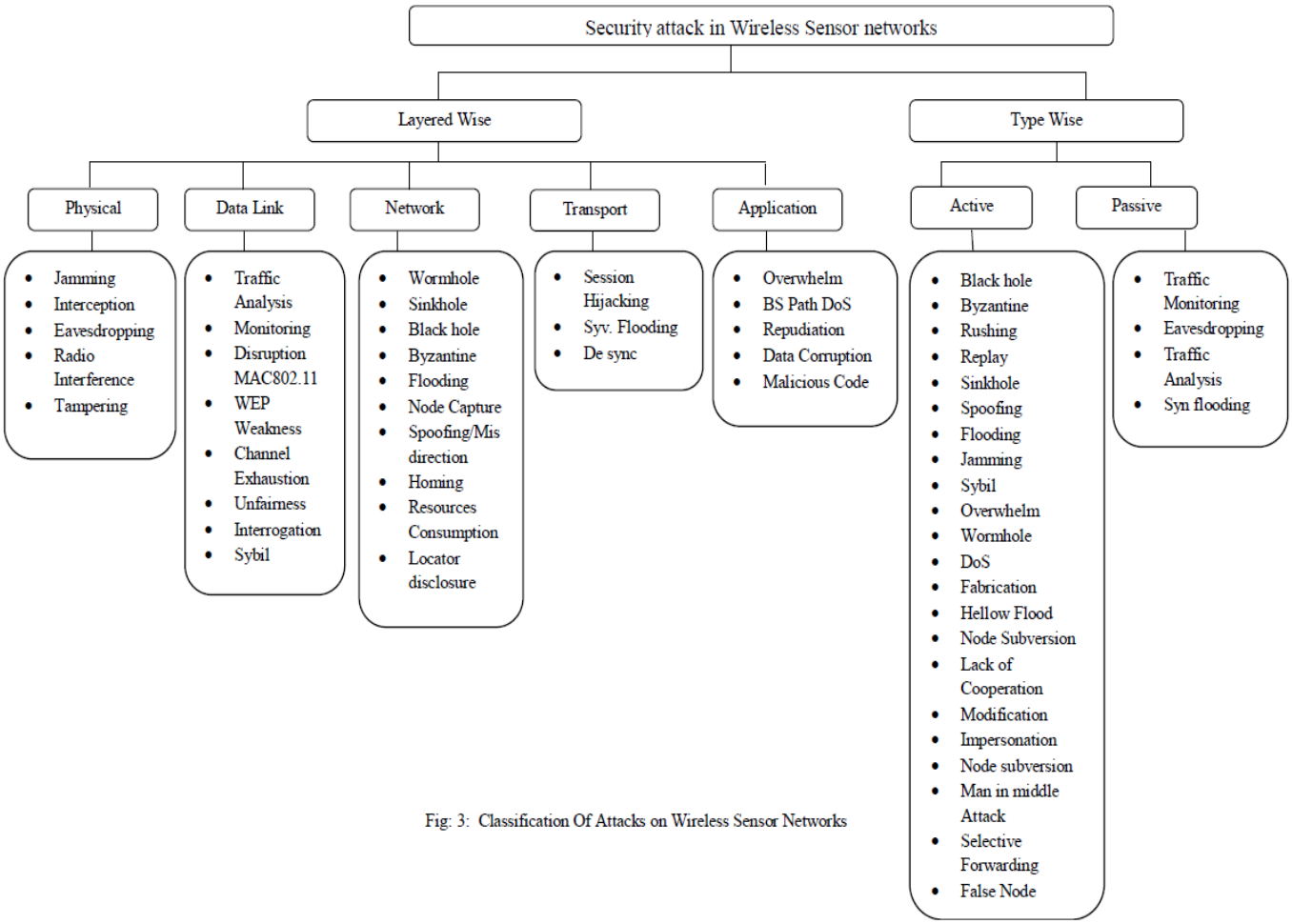

Fig: 3: Classification Of Attacks on Wireless Sensor Networks

Node Subversion: Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it

might be obtained by an adversary. [20]

Modification: The nature of wireless network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack [16].

Impersonation: In wireless networks a node is free to move in and out of the network. There is no secure authentication process in order to make the network secure from malicious nodes. The attacker use MAC and IP spoofing in order to get identity of another node and hide into the network. This kind of attack is also known as spoofing attack [16].

Man in middle Attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with reciever or impersonate the reciever to reply to the sender.

Selective Forwarding: In such attacks, malicious nodes may refuse to forward certain packets and simply drop them, ensuring that they are not propagated any further. An adversary will not, however, drop every packet. To avoid raising suspicions, the adversary instead selectively drops packets originating from a few selected nodes and forwards the remaining Traffic [19]

False Node: A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.[18]

Passive Traffic Monitoring: It can be developed to identify the communication parties and functionality which could provide information to launch further attacks.

Eavesdropping: The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place.
Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and fake message can be injected into network.
Traffic Analysis: Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

Syn flooding: This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.

CONCLUSION

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. In this paper, we have analyzed security attacks its prerequisite and vulnerability for processing and collecting the information in WSN and presented the security objective that need to be achieved.

REFERENCES:

[1]. R. Di Pietro et al. / Ad Hoc Networks 1 (2003) 455–468 459• Backward secrecy. Given that an adversary managed to recover a contiguous subset of session keys, no previous session keys can be recovered.
[2]. D.Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, 2002.
[3]. F. Akyildiz et al., "A Survey on Sensor Setworks," IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002, pp. 102–114.
[4]. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.
[5]. L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks", In Proceedings of the 9th ACM Conference on Computer and Networking, pp. 41- 47, Nov 2002.
[6]. E. Crawley et al., "A Framework for QoS-Based Routing in the Internet, " RFC 2386, http://www.ietf.org/rfc/rfc.2386.txt, Aug. 1998
[7]. S. Tilak, N. Abu-Ghazaleh and W. Heinzelman, "A taxonomy of wireless micro-sensor network communication models, " ACM Mobile Computing and Communication Review(MC2R), June 2002.
[8]. Pfitzmann, M. Kohntopp, Anonymity, unobservability and pseudonymity – a proposal for terminology, in: Hannes Federath(Ed.), Designing Privacy Enhancing Technologies, Lecture Notes in Computer Science (LNCS), vol. 2009, Springer-Verlag, 2001, pp. 1–9
[9]. A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.
[10]. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004
[11]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002.
[12]. X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan, "Sensor network configuration under physical attacks,", Technical report (OSU-CISRC-7/04-TR45), Department of Computer Science and Engineering, Ohio State University, July 2004.
[13]. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007
[14]. M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.
[15]. N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network".
[16]. C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.
[17]. C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys. And Apps., 1999.
[18]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," AdHoc Networks Journal, vol. 1, no. 2–3, pp. 293–315, September 2003.
[19]. Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT),

Page(s):6, year 2006
[20]. Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 – 40,

Mr. Sunil Gupta has done his Bachelor's degree in computer Science and Master's degree in Computer Science and Engineering from National Institute of Technology Hamirpur. Presently he is working as a research scholar in the area of Information Security at National Institute of Technology Jalandhar India.

Dr Harsh Kumar Verma is currently working as Associate Professor in the department of Computer Science and Engineering at Dr B R Ambedkar National Institute of Technology Jalandhar. He has done his Bachelor's degree in Computer Science and Engineering in May 1993. He did Master's degree in Software Systems from Birla Institute of Technology Pilani in Feb 1998 and Ph.D. from Punjab Technical University Jalandhar India in May 2006. He is presently working in the area of Information Security, Computer Networks and Scientific Computing. He has many publications of international /national level to his credit.

Dr A L Sangal is currently working as Professor in the department of Computer Science and Engineering at Dr B R Ambedkar National Institute of Technology Jalandhar. He has done his Bachelor's degree in Electronics and Communication Engineering from Panjab Engineering College Chandigarh. He did Master's degree in Computer Science from Thapar Institute of Engineering and Technology Patiala and Ph.D. from National Institute of Technology Jalandhar India. He is presently working in the area of Computer Networks, Scientific Computing and Information Security. He has numerous Publications of international/national level to his credit.