International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 9, September 2016)

Review of Threats in Wireless Sensor Networks

Sonal Garg[1], Mr. Vikas Malik[2]

[1]M. Tech scholar, [2]Assistant Professor, Department of Computer Science and Information Technology, Bhagat Phool Singh Mahila Vishwavidyalaya, Khanpur Kalan, Sonepat, Haryana, India

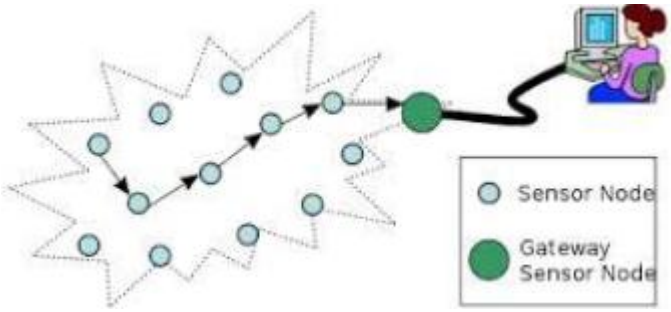
***Abstract*— Wireless sensor networks are networked systems, characterized by several energy resources, and the security mechanisms are actually used to detect, prevent and recover from the security attacks. In this security concerns must be addressed from the beginning of the system design. Securely communication among sensor nodes is a fundamental challenge for providing security services in WSNs. There is currently enormous research in the field of wireless sensor network security. Thus, the current research in this field will benefit the researchers. Many researchers have tried to provide security by using symmetric key cryptography, but thinking that public key steganography are feasible to implement in these networks because they are provided with more resources. This paper tends to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats for wireless sensor networks and also present the obstacles and the requirements in the sensor security, classify many of the current attacks.**

***Keywords*— WSN, DDos, Leach, Base Station, Cluster Head, Attacks.**

I. INTRODUCTION

Sensor networks refer to a heterogeneous system combiningtiny sensors and actuators with general purpose computingelements. Typical multi-hop wireless sensor networkarchitecture will consist of hundreds or thousands of selforganizing,low-power, low cost wireless nodes deployed enmasse to monitor and affect the environment. Wireless sensornetworks are quickly gaining popularity due to the fact thatthey are potentially low cost solutions to a variety of realworld challenges. Their low cost provides a means to deploylarge sensor arrays in a variety of conditions capable ofperforming both military and civilian tasks. But sensornetworks also introduce severe resource constraints due totheir lack of data storage and power. Both of these representmajor obstacles to the implementation of traditional computersecurity techniques in a wireless sensor network. To addressthe critical security issues in wireless sensor networks we talkabout cryptography, steganography and other basics ofnetwork security and their applicability. We also explorevarious types of threats and attacks against wireless sensornetwork and proposed schemes concerning security in WSNand also introduces the view of holistic security in WSN.

Issued need to be addressed in future research is alsoidentified, which provide vital information for futureresearchers. Finally we conclude the paper delineating theresearch challenges and future trends toward the research inWSN security.



II. BASIC SCHEMES OF SCEURITY IN WSN

- *Cryptography:* WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power. Applying any encryption scheme requires transmission of extra bits, henceextra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increasedelay, jitter and packet loss in wireless sensor networks.
- *Steganography:* While cryptography aims at hiding the content of a message, steganography aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.). The main objective of steganography is to modify the carrier in a way that is not perceptible and hence,it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want todistribute secret data publicly, it is very useful.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 9, September 2016)

III. Proposed Security Schemes

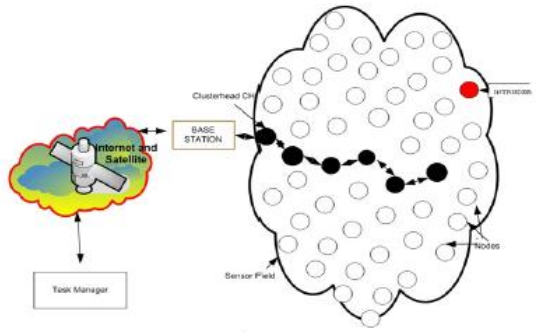
In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchersaround the world. In this section we review about the security schemes proposed or implemented so far for wireless sensor networks.

- *Holistic Security in WSN:* A holistic approach aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer mightnot be an efficient solution rather employing a holistic approach could be the best option.The holistic approach has some basic principles like, in agiven network; security is to be ensured for all the layers ofthe protocol stack, the cost for ensuring security should notsurpass the assessed security risk at a specific time, if there isno physical security ensured for the sensors, the securitymeasures must be able to exhibit a graceful degradation ifsome of the sensors in the network are compromised, out of order or captured by the enemy and the security measuresshould be developed to work in a decentralized fashion. Ifsecurity is not considered for all of the security layers, forexample; if a sensor is somehow captured or jammed in thephysical layer, the security for the overall network breaksdespite the fact that, there are some efficient securitymechanisms working in other layers. By building securitylayers as in the holistic approach, protection could beestablished for the overall network.

IV. Attacks

Sensor networks are particularly vulnerable to several keytypes of attacks. Attacks can be performed in a variety ofways, most notably as denial of service attacks, but alsothrough traffic analysis, privacy violation, physical attacks,and so on. Denial of service attacks on wireless sensornetworks can range from simply jamming the sensor'scommunication channel to more sophisticated attacksdesigned to violate the 802.11 MAC protocol or any otherlayer of the wireless sensor network. Due to the potentialasymmetry in power and computational constraints, guardingagainst a well orchest rated denial of service attack on awireless sensor network can be nearly impossible. A morepowerful node can easily jam a sensor node and effectivelyprevent the sensor network from performing its intended duty.

We note that attacks on wireless sensor networks are notlimited to simply denial of service attacks, but ratherencompass a variety of techniques including node takeovers,attacks on the routing protocols, and attacks on a node'sphysical security. In this section, we first address somecommon denial of service attacks and then describeadditional attacking, including those on the routing protocolsas well as an identity based attack known as Sybil attack.



- *Passive Attacks:* The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.
- *Active Attacks:* The unauthorized attackers monitors, listens to and modifiesthe data stream in the communication channel are known asactive attack.

The most popular types of attacks are:

1) Denial of Service Attacks
2) The Sybil Attack
3) Traffic Analysis Attack
4) Node Replication Attack
5) Attacks against Privacy
6) Physical Attacks

Wireless networks are vulnerable to security attacks due tothe broadcast nature of the transmission medium.Furthermore, WSNs have an additional vulnerability because nodesare often placed in a hostile or dangerous environment wherethey are not physically protected. For a large-scale sensornetwork, it is impractical to monitor and protect eachindividual sensor from physical or logical attack. Attackersmay device different types of security threats to make theWSN system unstable. Here in this section we present a layerbased classification of WSN security threats and also basedon the capability of the attacker and defences proposed in theliterature.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 9, September 2016)

1. Based On the Capability of the Attacker

a) *Outsider versus insider (node compromise) attacks:* Outside attacks are defined as attacks from nodes, which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.To overcome these attacks, we require robustness against Outsider Attacks, Resilience to Insider Attacks, Graceful Degradation with Respect to Node Compromise and RealisticLevels of Security.

b) *Passive versus active attacks:* Passive attacks include eavesdropping on or monitoringpackets exchanged within a WSN; active attacks involvesome modifications of the data steam or the creation of afalse stream**.**

c) *Mote-class versus laptop-class attacks:* In mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities to the network nodes; inlaptop-class attacks, an adversary can use more powerfuldevices (e.g., a laptop) to attack a WSN. These devices havegreater transmission range, processing power, and energyreserves than the network nodes.

2. Attacks on Information in Transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink stored within a sensor node. The attacker might also attempt to load itsprogram in the compromised node.

a) *Software compromise:* This involves breaking thesoftware running on the sensor nodes. Chances are the operating system and/or the applications running in a sensor node are vulnerable to popular exploits such as buffer overflows.

b) *Network-based attacks:* It has two orthogonal perspectives layer-specific compromises, and protocol-specific compromises. This includes all the attacks on information in transit. Apart fromthat it also includes:

Deviating from protocol: When the attacker is, or becomes an insider of the network,and the attacker's purpose is not to threaten the serviceavailability, message confidentiality, integrity andauthenticity of the network, but to gain an unfair advantagefor itself in the usage of the network, the attacker manifestsselfish behaviors, that deviate from the intendedfunctioning of the protocol.

3. Based On Protocol Stack

This section discusses about the WSN layer wise attack.

a) Physical Layer:

i) Jamming: This is one of the Denial of Service Attacks in which the adversary attempts to disrupt the operation of the network by broadcasting a high-energy signal.

Jamming attacks in WSNs,classifying them as constant (corrupts packets as they aretransmitted), deceptive (sends a constant stream of bytes intothe network to make it look like legitimate traffic), random(randomly alternates between sleep and jamming to saveenergy), and reactive (transmits a jam signal when it sensestraffic). To defence against this attack, use spread spectrumtechniques for radio communication. Handling jamming overthe MAC layer requires Admission Control Mechanisms.Network layer deals with it, by mapping the jammed area inthe network and routing around the area. Algorithms thatcombine statistically analyzing the received signal strengthindicator (RSSI) values, the average time required to sense anidle channel (carrier sense time), and the packet delivery ratio(PDR) techniques can reliably identify all four types ofjamming.

ii) Radio interference: In which the adversary either produces large amounts ofinterference intermittently or persistently. To handle thisissue, use of symmetric key algorithms in which thedisclosure of the keys is delayed by some time interval.Tampering or destructiongiven physical access to a node, an attacker can extractsensitive information such as cryptographic keys or other dataon the node. One defence to this attack involves tamperproofingthe node's physical package.

iii) Self-destruction (tamper-proofing packages): When eversomebody accesses the sensor nodes physically the nodesvaporize their memory contents and this prevents any leakageof information.

*iv) Second -Fault Tolerant Protocols:*Theprotocols designed for a WSN should be resilient to this typeof attacks.

b) Data Link Layer

i) Continuous Channel Access: (Exhaustion) malicious node disrupts the Media Access Control protocol, by continuously requesting or transmitting over the channel. This eventually leads a starvation for other nodes in the network with respect to channel access.

One of the counter measures to such an attack is Rate Limiting to theMAC admission control such that the network can ignoreexcessive requests, thus preventing the energy drain causedby repeated transmissions. A second technique is to use timedivision multiplexing where each node is allotted a time slotin which it can transmit.

ii) Collision: This is very much similar to the continuous channel attack. Acollision occurs when two nodes attempt to transmit on thesame frequency simultaneously.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 9, September 2016)

When packets collide, achange will likely occur in the data portion, causing achecksum mismatch at the receiving end. The packet will then be discarded as invalid. A typical defence against collisions is the use of error-correcting codes.

iii) Unfairness: Repeated application of these exhaustion or collision based MAC layer attacks or anabusive use of cooperative MAC layer priority mechanisms, can lead into unfairness. This kind of attack is a partial DOS attack, but results in marginal performance degradation.

iv) Interrogation: Exploits the two-way request-to send/ clear to send(RTS/CTS) handshake that manyMAC protocols use to mitigate the hidden-node problem.

v) Sybil Attack: This type of attack is very much prominent in Link Layer.First type of link layer SybilAttack is-

1. Data Aggregation: in which single malicious node isact as different Sybil Nodes and then this may many negativereinforcements to make the aggregate message a false one.

2. Voting: Many MAC protocols may go for voting for finding the better link for transmission from a pool of available links. Here the Sybil Attack could be used to stuff the ballot box. An attacker may be able to determine the outcome of any voting and off course it depends on the number of identities the attacker owns.

c) Network Layer

Sinkhole: Depending on the routing algorithm technique, a sinkholeattack tries to lure almost all the traffic toward the compromised node, creating a metaphorical sinkhole with theadversary at the centre. Geo-routing protocols are known asone of the routing protocol classes that are resistant tosinkhole attacks, because that topology is constructed using only localized information, and traffic is naturally routed through the physical location of the sink node, which makes it difficult to lure it elsewhere to create a sinkhole.

Hello Flood: This attack exploits Hello packets that are required in many protocols to announce nodes to their neighbours. A nodereceiving such packets may assume that it is in radio range ofthe sender. A laptop class adversary can send this kind ofpacket to all sensor nodes in the network so that they believethe compromised node belongs to their neighbours. This causes a large number of nodes sending packets to this imaginary neighbour and thus into oblivion. Authentication isthe key solution to such attacks. Such attacks can easily beavoided by verify bi-directionality of a link before takingaction based on the information received over that link.

i) Node Capture: It is observed and analyzed that even a single node capture issufficient for an attacker to take over the entire network. Good solution to this problem would definitely constitute aground breaking work in WSN.

d) Transport Layer

Flooding: An attacker may repeatedly make new connection requestsuntil the resources required by each connection are exhaustedor reach a maximum limit. It produces severe resourceconstraints for legitimate nodes. One proposed solution tothis problem is to require that each connecting clientdemonstrate its commitment to the connection by solving apuzzle. As a defence against this class of attack, a limit can beput on the number of connections from a particular node.

De-synchronization Attacks: In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missedframes. Hence, these messages are again transmitted and ifthe adversary maintains a proper timing, it can prevent theend points from exchanging any useful information. This willcause a considerable drainage of energy of legitimate nodesin the network in an endless synchronization-recoveryprotocol.

e) Application Layer

Overwhelm attack: An attacker might attempt to overwhelm network nodes withsensor stimuli, causing the network to forward large volumesof traffic to a base station. This attack consumes networkbandwidth and drains node energy. We can mitigate thisattack by carefully tuning sensors so that only the specifically desired stimulus, such as vehicular movement, as opposed toany movement, triggers them.

Path-based DOS attack:

It involves injecting spurious or replayed packets into the network at leaf nodes. This attack can starve the network oflegitimate traffic, because it consumes resources on the pathto the base station, thus preventing other nodes from sending data to the base station. Combining packet authentication andanti replay protection prevents these attacks.

ii) Deluge (reprogram) attack: Network programming system let you remotely reprogramnodes in deployed networks If the reprogramming processisn't secure, an intruder can hijack this process and take control of large portions of a network. It can use authentication streams to secure the reprogramming process.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 9, September 2016)

V. Challenges Of Sensor Networks

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. A wireless sensor network is a special network which has many constraint compared to a traditional computer network.

a) *Wireless Medium:* The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed byan adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks.

b) *Ad-Hoc Deployment:* The ad-hoc nature of sensor networks means no structure canbe statically defined. The network topology is always subjectto changes due to node failure, addition, or mobility. Nodesmay be deployed by airdrop, so nothing is known of thetopology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration. Security schemes must be able to operate within this dynamic environment.

c) *Hostile Environment:* The next challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical accessto the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. cryptographic keys). The highly hostile environment represents a serious challenge for security researchers.

d) *Resource Scarcity:* The extreme resource limitations of sensor devices poseconsiderable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory.

VI. Conclusion

In this paper, we have described the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defences. Within each of those categories wehave also sub-categorized the major topics including routing, trust, denial of service, and so on Wireless Sensor Networks, are self organising, self healing networks of small "nodes" have huge potential across industrial, military and many othersectors. While appreciable sales have now been established, major progress depends on standards and achieving twenty year life.

REFERENCES

[1] Kumar, P.; Cho, S.; Lee, D.S.; Lee, Y.D.; Lee, H.J. Tri Sec:A secure data framework for wireless sensor networks using authenticated encryption. Int. J. Marit. Inf. Commun. Sci. (2010).

[2] Hadim, Salem, Nader Mohamed (2006). "Middleware Challenges and Approaches for Wireless Sensor Networks" IEEE Distributed Systems Online.

[3] Protocols and Architectures for Wireless Sensor Networks, Holger Karl, Andreas Willig, ISBN, January 2009.

[4] H. Mohamed and B. Majid, “Forest Fire Modelling and Early Detection using Wireless Sensor Network” in Ad Hoc & Sensor Wireless Networks Philadelphia: Old City Publishing, 2013.