Security Challenges in Wireless Sensor Networks

Monali Rajput
Assistant Professor
VES Institute of Technology,
Mumbai, Maharashtra, India

Usama Ghawte
P.G Student, Dept. of M.C.A
VES Institute of Technology,
Mumbai, Maharashtra, India

ABSTRACT
In recent years, Wireless Sensor Network (WSN) has shown a valid futuristic application in the field of medical, geology, industry and defence etc. The basic plan of a Wireless sensor network(WSN) is to spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. Wireless communication technology exhibits different forms of security threats. [1] This paper introduces numerous security problems in wireless sensor network, by distinguishing various threats and therefore analysing those problems and stating some security measures within the WSN. We additionally discuss the security for making certain layered and robust(strong) security in wireless sensor networks

Keywords
Wireless Sensor Network (WSN), Security.

1. INTRODUCTION
Wireless Sensor Network is an ad hoc (created or done for a purpose as necessary) network that consists of a number of resource or devices that can communicate the information gathered from a monitored field through wireless links. [2] It consists of base stations and numbers of nodes (wireless sensors) that are used to monitor physical or environmental conditions like sound, pressure, temperature and co-operatively pass data through the network to a main location

1.1 Security:
Security provides protection against the danger, loss and criminal activities, however within the networks it's the Protection of knowledge from theft, corruption or natural disaster and allows the information to be accessible only to the intended users. A **wireless sensor network** (WSN) consists of geographically distributed sensors to monitor physical or environmental conditions like temperature, sound, pressure, etc. and also the corresponding information are transmitted through the network to a main location. [3] The modern networks are bi-directional in nature that enables control of sensor activity. The introduction of WSN was motivated by military applications like battlefield surveillance

1.2 1.2 Basic Idea about WSN
The construction of wireless sensor networking will decide it's working. WSN initially consists of small or large Sensor nodes. These nodes vary in sizes and different sizes of sensor nodes work efficiently in different fields. WSN consist of nodes that have a microcontroller for monitoring, a radio transceiver for generating radio waves, different type of wireless communicating devices and also equipped with an energy source such as battery or an embedded kind of energy harvesting. The entire network worked on the phenomenon of multi routing algorithm which is also called wireless ad hoc networking.

The WSN (Figure 1) is a combination of few hundreds or even thousands of nodes, where each node is connected to one or more sensors.

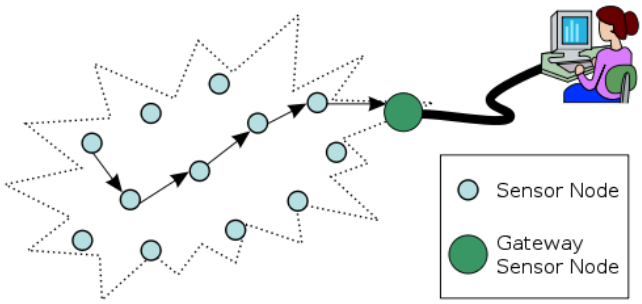

Figure 1: Wireless Sensor Network

The cost of sensing nodes depends on the complexity of the individual sensor nodes. [4] Cost and size Limitation on sensor nodes result in corresponding limitations on resources like energy, memory, computational speed and communications bandwidth.

2. WSN TOPOLOGIES
WSN nodes are usually organized in one of 3 styles of network topologies:

2.1 Star Topology
In a star topology, each node connects directly to a gateway. A gateway can send or receive a message to a number of remote nodes. Here the nodes are not permitted to send messages to each other, this allows low-latency communications between the remote node and the gateway (base station). [5]

This topology is dependent on single node to manage the network; hence the gateway must be within the radio transmission range of all the individual nodes.

The advantage is the simplicity of the topology and low cost.

The size of the network depends upon the connection of nodes to gateway.

2.2 Cluster Topology
In a cluster tree network, each node connected to the other node higher within the tree and then connected to the gateway, and information is routed from the lowest node on the tree to the gateway. [6]

The main advantage of the cluster topology is that the expansion of a network can be easily possible, and also error detection becomes easy.

The disadvantage is the dependency on bus cable which is quite high; if it breaks, all the network will collapse.

2.3 Mesh Topology

In a mesh networks nodes are connected to multiple nodes within the system and passes the data through the most reliable path available.[7]

The advantage of mesh topology includes easy isolation and detection of faults/bugs in the network.

The disadvantage is that the network is huge and needs heavy investment

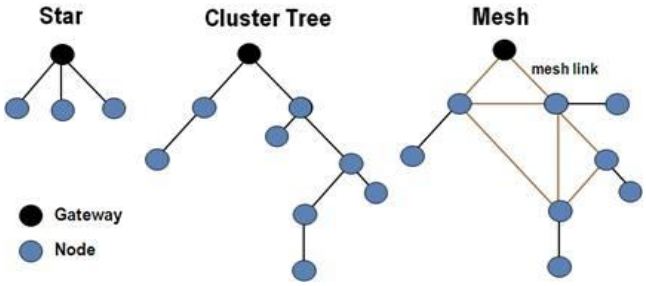

Fig 2. Common WSN Network Topologies

3. WSN WORKING

Wireless sensor Networks are collections of motes. Generally, Motes are the individual computers that job along to form networks. the basic requirements for motes are extensive. They must be small, energy efficient, multi-functional, and wireless. Motes communicate with each other using radio transmitters and receivers to reach a common goal. For example, if the goal is to collect data about the micro-climates around all sections of redwoods in a forest, the motes are placed within the trees to form a network. Once placed, they collect and transmit information to every alternative, and eventually to a main computer.

They form networks with other motes that change with the positions of the motes. These Motes create links with each other with in different configurations to maximize the performance for each mote. These links all linked to the 'parent' mote, which transmits the data from each of the "child" motes to whatever computer or PDA type devices that has been used to collect and process the data. [8]

Due to intrusion from the surroundings and the mote's maximum broadcast range, not all of the motes placed around trees can communicate with all others. The mote's radios have a limited broadcast range to save as much power as possible. This range is approximately Thirty meters (30 ms). If the motes have a short radio broadcast range, and many motes are more than Thirty meters (30 ms) 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 data and broadcasting it to multiple other motes, which then interact with others, to find the most rapid or successful route for the data to reach the main computer.

Figure 3 illustrates one possible path data can travel between the outer motes and those close to the computer/station.

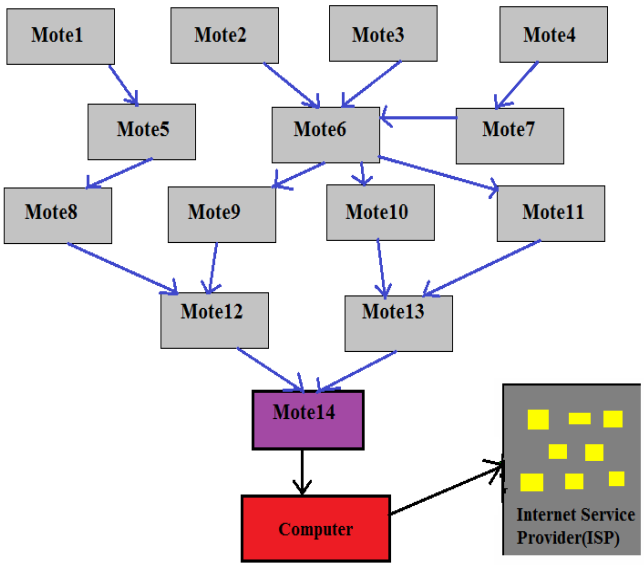

Fig 3. Motes Communication in WSN

Fig.3 The Motes 1 through 13 are the children motes (all the ones in light grey), Mote 14 is the parent (in purple). The "Computer" (in red) can be any type of computer such as PDA, laptop, etc. as long as it is capable of accessing the internet via a specified ISP (the grey building with yellow windows). The arrows connecting the motes aren't mounted (fixed), and to illustrate this, they're purposefully unorganized.

When the motes are linked together, they form components (parts) of a machine with greater computational power than any of the individual components (parts). These "machines" of motes change with position and with conditions. Generally high moisture and other situations can affect broadcast abilities of many motes. Changes in conditions can make some motes connections stronger than they used to be, and others nearly not possible. The thinking capability within the network allows the pieces to reorganize in such a way that each one motes will continue to be functional.

4. APPLICATIONS OF WSN

Wireless Sensor Networks (WSN) are found in various applications in wide-ranging areas. In this section I list some of the prominent areas of applications of WSN. The list would be very lengthy if I exhaust all the areas of WSN applications. Therefore, in this paper only certain applications are provided.

4.1 Military Application

Sensor nodes include battlefield surveillance and monitoring, guiding systems of intelligent missiles and detection of attack by weapons of mass destruction.

4.2 Medical Application

Sensors can be extremely useful in patient monitoring and diagnosis. Patients can wear sensor devices that will monitor their physiological data like heart rate or blood pressure.

4.3 Environmental monitoring

It includes Wild fire, traffic, habitat etc.

4.4 Industrial Application

It includes industrial diagnostics and sensing. For example: appliances, factory, supply chains etc.

4.5 Infrastructure Protection Application

It includes power grids monitoring, water distribution monitoring etc.

4.6 Miscellaneous Applications

Sensors will be prominent at homes in different commercial applications and even in industries. Generally, we know Smart sensor nodes can be built into appliances at home, such as refrigerators, ovens and vacuum cleaners, enable them to interact with each other and be remote controlled. [9]

5. SECURITY ISSUES IN WSN

Security issues in WSN depends on what we are going to protect. Four security goals in sensor networks which are Confidentiality, Integrity, Authentication, Availability. Confidentiality is that the ability to hide message from a passive attacker, wherever the message communicated on sensor networks remain confidential. Integrity refer to the ability to confirm the message has not been altered, tampered or changed while it was on the n/w. Authentication Need to know if the messages are from the node it claims to be determining, from the reliability of messages origin. Availability is to determinant if a node has the ability to use the resources and the network is available for the messages to move(proceed) on. Freshness implies that receiver receives the recent and fresh information and ensures that no adversary will replay the old(previous) information. This requirement is especially important when the WSN nodes use shared-keys for message communication(interaction), where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the Wireless Sensor N/w. To achieve the freshness the mechanism like nonce or timestamp should add to each data packet.

Why security is essential in WSN? There are numerous reasons for that; First of all, WSN are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, WSN have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically safe.

Attacks on WSNs can be classified from 2 different levels of views-

- Attack against security mechanisms.
- Attack against basic mechanisms (like routing mechanisms).

In many applications, the data obtained by the sensing nodes needs to be kept confidential and it has to be authentic. In the absence of security, a malicious node could intercept private information, or could send false messages to nodes in the n/w. The major attacks are- Denial of Service(DOS), Wormhole attack, Sybil attack, Selective Forwarding attack, Sinkhole attack, Node capturing, false or malicious node, Passive information gathering, Hello flood attack etc. In this section, a brief overview on these attacks are presented.

5.1 Denial of Service (DoS)

It happens by the unintentional failure of nodes or malicious actions. the simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unessential packets and thus prevents legitimate network users from accessing services or resources to which they're entitled. [10]

DoS attack is meant not just for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service.

In wireless sensor networks, many types of Denial of Service (DoS) attacks in different layers could be performed. Physical layer the DoS attacks could be jamming and tampering, at data link layer, exhaustion, collision, unfairness at network layer; neglect and greed, misdirection, homing, black holes and at transport layer this attack could be performed by malicious flooding and asynchronization.

5.2 The Wormhole attack

One node in the network (sender) sends a message to another node in the network (receiver node). Then the receiving node makes an attempt to send the message to its neighbour's. The neighbouring nodes suppose(think) the message was sent from the sender node (which is sometimes out of range), so they make an attempt to send the message to the originating node, but it ne'er arrives since it's too far away.

Wormhole attack is a significant threat to WSN, because, this kind of attack doesn't need to compromise a sensor within the network rather, it can be performed even at the initial phase when the sensors begin to find neighbouring information.

Wormhole attacks are troublesome(difficult) to counter as a result of routing information provided by a node is difficult to verify.

5.3 The Sybil attack

In this attack, a single node i.e. a malicious node will appear to be a collection of nodes and will send half truths or incorrect information to a node within the network.

The incorrect data can be a variety of things, together with signal strengths, position of nodes, making up nodes that do not exist.

Authentication and encryption (secrete writing) techniques can prevent(stop) an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating within the network, but he should only be able to do so using the identities of the nodes he has compromised.

Public key cryptography can prevent (stop) such an insider attack, but it is too high-ticket (expensive) to be used in the resource constrained sensor networks.

5.4 Selective Forwarding attack

Selective Forwarding attack is a situation (condition) when certain or particular nodes don't forward many of the messages they receive; The sensor networks depends on repeated forwarding by broadcast for messages to propagate or pass throughout the network.

5.5 Sinkhole attacks

Sinkhole attack, the adversary's final aim is to lure nearly all the traffic from a particular area (space) through a compromised node, making a metaphorical sinkhole with the adversary at the centre. sink attacks basically work by creating a compromised node look especially attractive to surrounding nodes with regard to the routing algorithm. Sinkhole attacks are not easy to counter because routing data provided by a node is difficult to verify

5.6 Passive information gathering

An intruder with an appropriately(exactly) powerful receiver and well-designed antenna will simply pick off the information stream.

Intercepting message content that possesses physical locations of sensor nodes allows an attacker to locate the nodes and

destroy them; Besides the locations of sensor nodes, a human will observe the application specific content of messages including message IDs, time-stamps and other fields.

5.7 Node Capturing

A particular sensor might be captured and data stored on it might be obtained by an adversary.

5.8 False or Malicious Node

False or Malicious Node Most of the attacks break security in WSN are caused by the insertion of false information by the compromised nodes in the to the network.

5.9 Hello flood attacks

The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power; so that a large number of nodes even far away in the network choose it as the parent. All messages(information) now need to be routed multi-hop to this parent which increases delay.

6. PREVENTION MECHANISMS

This section highlights the preventive measures of all the attacks mentioned above. It is to be noted that the list would be very vast if I try to exhaustively list all the preventive measures. So, the list is restricted to only a handful of the solutions.

6.1 DOS prevention

The mechanisms to prevent DoS attacks include payment for network resources, strong authentication, pushback and identification of traffic. One security technique uses authentication streams to secure the reprogramming process. This divides a program binary into a series of messages each of which contains a hash of the next message. This mechanism ensures that an intruder(attack) cannot hijack an ongoing program transmission, even if he knows the hashing mechanism. This is because it would be almost not possible to construct a message that matches the hash contained in the old-previous message, A digitally signed advertisement and which contains the program name, version number with hash of the first message, ensures that the process or activity is securely initiated.

We can defeat more than one threats using existing encryption and authentication mechanisms, and other techniques (such as identifying jamming attacks) can alert network administrators of ongoing attacks or trigger techniques to conserve energy on affected devices.[11]

6.2 Wormhole attack prevention

The mechanism to prevent wormhole attack include, DAWWSEN, a proactive routing protocol based on the construction of a hierarchical tree where the base station is the root node & the sensor nodes are the internal or the leaf nodes of the tree. A great benefit of DAWWSEN is that it doesn't require any geographical information about the sensor nodes & does not take the time stamp of the packet as an approach for detecting a wormhole attack, which is most important for the resource constrained nature of the sensor nodes.

6.3 Sybil prevention

To prevent against Sybil attacks, use identity certificates. The basic idea is very simple. The setup server, before deployment, assigns each sensor node some unique data. Then servers create an identity certificate binding this node's identity to the assigned unique data, and downloads this data into the node. To securely demonstrate its identification, a node first presents its identity certificate and then proves that it possesses or matches the associated unique data. This process needs the exchange of several or related some messages. Merkle hash tree can be used as basic means of computing identity certificates. The Merkle hash tree is a vertex-labelled binary tree, where the label of each non-leaf vertex is a hash of the concatenation of the labels of its two child vertexes. The primary path of a leaf vertex is the set of vertexes on the path from the leaf to the root of the tree. The authentication path contains siblings of the vertexes on this primary path. Given a vertex, its authentication path and hash function, the primary path can then be calculated, up to and including the root of the tree. This generated value or computed of the root can then be compared with a stored value, to verify the authentication of the label of the leaf vertex. [12]

6.4 Passive informational gathering prevention

To minimize or small effect of the threats of passive information gathering, strong encryption techniques need to be used.

6.5 Node capture prevention

If a node has been compromised then how to exclude that node and that node only from the sensor network is at issue and This issue is solved with the help of Localized Encryption and Authentication protocol (LEAP). LEAP (localized encryption and authentication protocol) is an efficient protocol for inter-node traffic authentication. This protocol relies on a key sharing approach that authorizes into network processing and at the same time mitigates several possible attacks.

6.6 False or Malicious Node prevention

This attack needs to be checked in the Routing layer itself. Details pertaining to the preventive measures for "false node" attack are out of the scope of this paper.

6.7 Hello flood attacks prevention

This can be prevented by checking bidirectional of a link, so that the nodes ensure that they reach their parent within one hop.

6.8 Selective Forwarding attack prevention

Multipath routing can prevent these types of selective forwarding attacks. The messages routed over the paths where the nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates which can further reduce the chances of an adversary gaining complete control of a data flow.

6.9 Sinkhole attacks prevention

These types of attacks are very difficult to defend against one class of protocols resistant to these attacks is geographic routing protocols. On demand, geographic protocols construct a topology using only localized interactions and without initiation from the base station. [13]

7. SUMMARY

All the previously mentioned security threats like Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, serve one common purpose that is to compromise the integrity of the network they attack. Also In the past, focus has not been on the security of WSNs, but with the various threats arising and the importance of data confidentiality, security has

become a major issue. Although there are some solutions which has been already proposed, but there is no single solution to protect against every threat. Here, we mainly focus on the security threats in WSN. We have presented the summary of the WSNs threats affecting different layers along with their defence mechanism. We can see that the defence mechanism presented just gives guidelines about the WSN security threats; the exact solution depends on the type of application the WSN is deployed for. There are many security mechanisms which are used in "layer-by-layer" basis as a security tool. People are now going for integrated system for security mechanism rather than concentrating on different layers independently. Through this paper, we tried to showcase the most common security threats in various layers and their most possible solution.

8. ACKNOWLEDGEMENT

We are gratefully and sincerely appreciate the efforts of people who have worked towards Wireless Sensor Networks security and making it difficult for hackers to penetrate into the system. Thus making WSN more secure.

9. REFERENCES

[1] Gaurav Jolly, Mustafa C. KuşÁu, Pallavi Kokate, and Mohamed Younis, Computer Science and Electrical Engineering, University of Maryland- "A Low-Energy Key Management Protocol for Wireless Sensor Networks".

[2] C. Anuradha, "Stochastic Analysis of Various Security Protocols in Wireless Sensor Networks" Volume 3, Issue 2, February 2013 .

[3] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges" ISBN 89-5519-129-4, Feb. 20-22, 2006.

[4] Antonio dc la picdra, "Wireless Sensor Networks for Environmental Research: A Survey on Limitations and Challenges" 978-1-4673-2232-4/13.

[5] Chris Karlof, David Wagner- "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" Adhoc Networks 1,293-315.

[6] Feng Zhao Wireless Sensor Networks Morgan Kaufmann Publications.

[7] Security in wireless sensor networks (book)

[8] Anthony D. Wood," Denial of Service in Sensor Networks" http://www.cs.virginia.edu/~adw5p/pubs.html

[9] Ann Holms , Ethan Culler-Mayeno, "A Technical Report: Wireless Sensor Networks and How They Work"

[10] C. Siva Ram Murthy and B.S. Manoj "Building wireless M2M & IoT sensor networks: issues and challenges"

[11] http://www.cs.cmu.edu (Refered for Sybil attack)

[12] https://www.techopedia.com (Refered for DOS attack)

[13] Wireless Sensor Networks and Applications (Book) edited by Ibrahiem M. M. El Emary, S.Ramakrishhnan.