Security Issue and Challenges in Wireless Sensor Networks: A Survey and Attacks

Mosiur Rahaman

Assistant Professor, Dept. of Computer Science & Engineering
Royal Institute of Technology and Science, JNTU Hyderabad, India

Abdul Aziz

RITS College Dept.Of C.S.E
Hyderabad, India

Abstract−Wireless Sensor Network processing sensitive data this are facing the risk of data manipulation, data fraud and sensor distribution or replacement, this concern application such as the gathering of data on environmental pollution around industrial installation or sensor system, replacing traditional video monitoring, large scale deployment in practice is condition by solving this kind of security problem and reducing the risk due to limited physical protection of the device and openness of wireless communication chances, while modern cryptography and computer .Confidentiality, integrity and Authentication are the most important data security treat. Security offer many ways of solving this problem, they are focused on solution of high performance devices, and not for computationally weak sensor with limited communication.

Keywords−Security, Issues, Goal, Challenges, Wireless Sensor Network (WSN)

1. INTRODUCTION

Wireless Sensor Networks (WSN) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental condition, such as temperature, sound, vibration, pressure, motion or pollutants and to co-operatively pass their data through the network to a main location or sink where the data can be observed and analyzed. The application domains of wireless sensor networks are diverse due to the availability of micro-sensor and low-power wireless communication. These sensors are densely deployed. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. The size of the sensor nodes can also range from the size of a shoe box to as small as the size of a grain of dust. Today's sensors are tiny, inexpensive to manufacture and don't need lot of power—an essential characteristic, since many sensors are expected to operate for long-term without access to line power. Most wireless objects get their power from batteries, but interesting new classes of devices are emerging that scavenge electricity directly from the environment. The more modern networks are bi-directional, also enabling control of sensor activity. These sensor nodes can communicate among themselves using radio signals. They will do local processing to reduce communication and consequently energy costs.

1.1 WSN Architecture

In a typical WSN we see following network components –

a) Sensor motes (Field devices): Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself. Each sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for.

b) Gateway or Access points: A Gateway enables communication between Host application and field devices.

c) Network manager: A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

d) Security manager: The Security Manager is responsible for the generation, storage, and management of keys.

The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, high power Wi-Fi links etc.

- ***Structure of a wireless sensor node*:** A sensor node is made up of four basic components such as sensing unit, processing unit, transceiver unit and a power unit which is shown in. It also has additional components such as a location finding system, a power generator and a mobilize. Sensing units are usually composed of two subunits: sensors and Analogue to Digital Converters (ADCs). The analogue signals produced by the sensors are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit is generally associated with a small storage unit and it can manage the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. Power units can be supported by a power scavenging unit such as solar cells. The other subunits, of the node are application dependent.

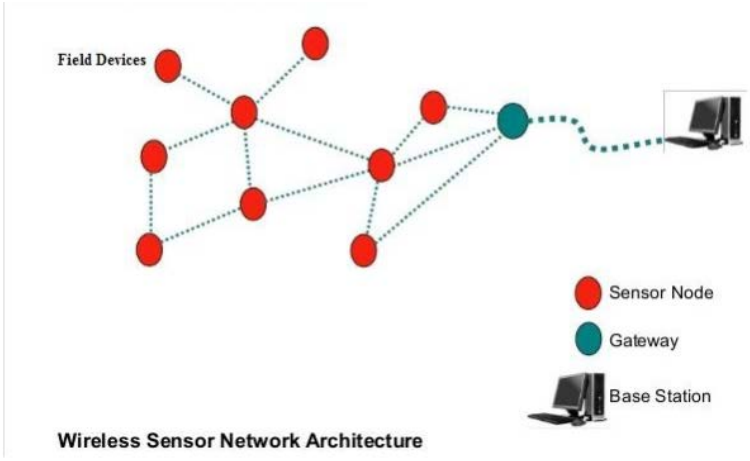


Figure:1.1 WSN Architecture

2 Security Threats and Issues in WSN

Wireless Sensor Networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Basically attacks are broadly classified in two categories i.e. active attacks and passive attacks. This paper points out both of these attacks in details.

2.1 Goal-Oriented Attacks

We distinguish passive and active attacks.

2.1.1 Passive Attacks:

These attacks are mainly against data confidentiality. An attacker monitors unencrypted traffic and looks for sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring communications, decrypting weakly encrypted traffic, and capturing authentication information. Passive interception of network operations enables adversaries to see upcoming actions. Such attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

2.1.1.1 Monitor and Eavesdropping:

This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents.

2.1.1.2 Traffic Analysis:

Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

2.1.1.3 Camouflage Adversaries:

One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

2.1.2 Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

2.1.2.1 Routing Attacks in Sensor Networks:

The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages.

2.1.2.1.1 Attacks on Information in Transit:

In a sense or network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to Interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks.

2.1.2.1.2 Selective Forwarding:

A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.

2.1.2.1.3 Black Hole/Sinkhole Attack:

In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure 2.1.2.1.3 shows the conceptual view of a black hole/sinkhole attack.

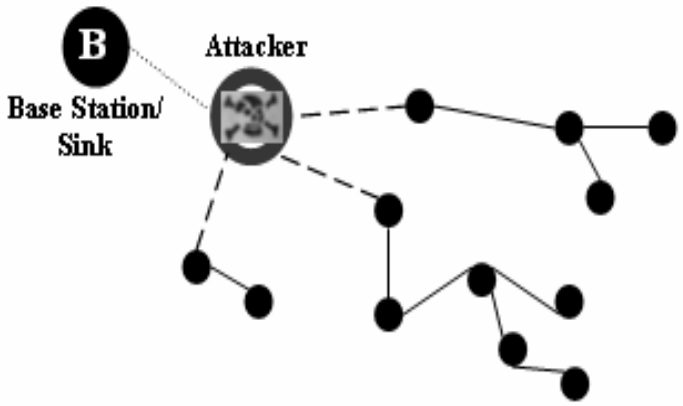
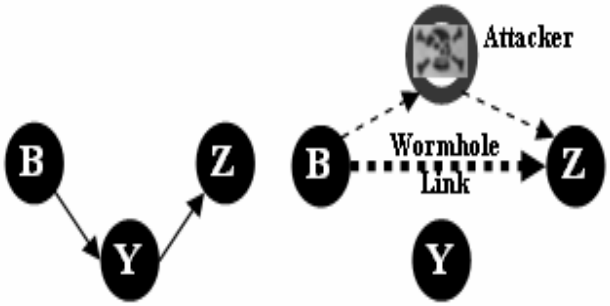


Figure: 2.1.2.1.3 Conceptual view of Black hole Attack

2.1.2.1.4 Wormholes Attacks:

Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location.



(a) (b)

Figure: 2.1.2.1.4 Wormhole Attack

Figure: 2.1.2.1.4 (a and b) shows a situation where a wormhole attack takes place.

When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as

its parent. Hence, even if the victim nodes are multi-hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

2.1.2.1.5 HELLO Flood Attacks:

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.

2.1.2.1.6 Sybil Attacks: the sensors in a wireless sensor network might need to work together to accomplish a task, hence they cause distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve.

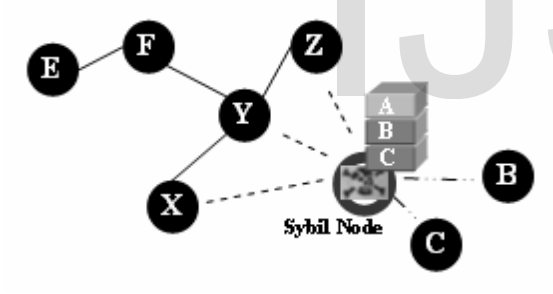


Figure: 2.1.2.1.6 Sybil Attack

2.1.2.2 Denial of Service Attack: The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevent legitimate network users from accessing services or resources to which they are entitled. At physical layer the DoS attacks could be jamming and tempering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and asynchronization. The mechanism to prevent the DoS attacks includes payment for network resources, pushback, strong authentication and identification of traffic.

2.1.2.3 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.

2.1.2.4 Node Malfunction:

A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader.

2.1.2.5 Node Outage:

Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.

2.1.2.6 Physical Attacks:

Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

2.1.2.7 Message Corruption:

Any modification of the content of a message by an attacker compromises its integrity.

2.1.2.8 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.

2.1.2.9 Node Replication Attacks:

Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID 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.

2.1.2.10 Passive Information Gathering:

An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

2.2 Performer-Oriented Attacks

Another category in attacks on WSNs can be either outside or inside attacks.

2.2.1 Outside Attacks

Outside attacks may cause passive eavesdropping on data transmissions, as well as can extend to injecting bogus data into the network to consume network resources and raise Denial of Service attacks.

2.2.2 Inside Attacks

Inside attackers can damage the network stealthily since they can avoid our authentication and authorization because they are legitimate nodes of the native network and have access to the network information, and it is not easy to expect their attack patterns. Inside attackers can launch various types of attacks, such as modification, misrouting, eavesdropping or packet drop. This last attack is tricky to counter, because for a particular packet drop, we cannot distinguish whether it is dropped by an attacker or a result from collision or noise. This attack suppresses the important information reaching the base station which significantly degrades network performance, such as packet delivery rate due to their repeated packet drops. There are several types of packet drop attacks such as black hole, gray hole and on-off attacks. This is a serious threat for many applications, such as military surveillance system that monitors the battlefield and other critical infrastructures.

2.3 Layer-Oriented Attacks

WSNs are organized in layered form. This layered architecture makes these networks vulnerable to various kinds of attacks.

2.3.1 Physical Layer Attacks

Physical attacks on WSNs range from node capturing to the jamming of the radio channel. Physical attacks on WSNs availability are even more difficult to prevent than software attacks, because of the lack of physical control over the individual nodes. Jamming is one of the most important attacks at physical layer, aiming at interfering with normal operations. An attacker may continuously transmit radio signals on a wireless channel. An attacker can send high-energy signals in order to effectively block wireless medium and to prevent sensor nodes from communicating. This can lead to Denial-of-Service attacks at this layer.

2.3.2 Data Link Layer Attacks

The functionality of link layer protocols is to coordinate neighboring nodes to access shared wireless channels and to provide link abstraction to upper layers. Attackers can deliberately violate predefined protocol behaviors at link layer. For example, attackers may induce collisions by disrupting a packet, cause drain of sensor node energy by repeated retransmissions, or intercepting and examining messages in order to deduce information from patterns in communication. This can be performed even when the messages are encrypted and cannot be decrypted, or even cause unfairness by abusing a cooperative MAC layer priority scheme.

2.3.3 Network Layer Attacks

The network layer of WSNs is vulnerable to the different types of attacks, such as DoS attacks that are aimed at complete disruption of routing information, and therefore the whole operation of ad-hoc network. A sinkhole attack tries to lure almost all the traffic toward the compromised node,

creating a metaphorical sinkhole with the adversary at the centre. Also if an attacker captures a single node, it is sufficient for him to get hold of the entire network. Malicious or attacking nodes can however refuse to route certain messages and drop them Spoofed, Altered, or Replayed Routing Information are the most direct attacks against a routing protocol in any network, are to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network.

2.3.4 Transport Layer Attacks

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.

2.3.5 Application Layer Attacks

Different type of attacks can be carried out in this layer, such as overwhelm, repudiation, data corruption and malicious code. In overwhelm 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 nodes energy.

3. Security Challenges in WSN

WSNs have many constraints from which new challenges stand out. The extreme resource limitations of sensor nodes and unreliable communication medium in unattended environments make it very difficult to directly employ the existing security approaches on a sensor platform due to the complexity of the algorithms. Indeed, the understanding of these challenges within WSNs provides a basis for further works on sensor networks security. 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.

3.1 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 by an 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.

3.2 Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by airdrop, so nothing is known of the topology 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.

3.3 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 access to 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.

3.4 Resource Scarcity

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient.

3.5 Immense Scale

The proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

3.6 Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

• ***Unreliable Transfer:*** Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable.

• ***Conflicts:*** Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network.

• ***Latency:*** The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

3.7 Unattended Operation

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main cautions to unattended sensor nodes.

• ***Exposure to Physical Attacks:*** The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The probability that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network.

• ***Managed Remotely:*** Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues.

• ***No Central Management Point:*** A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.Perhaps most importantly, the longer that a sensor is left unattended the more likely that an adversary has compromised the node.

4. Security Goals for Sensor Networks

As the sensor networks can also operate in an adhoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of adhoc sensor networks. The security goals are classified as primary and secondary. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self- Organization, Time Synchronization and Secure Localization.

4.1 Primary Goals:

4.1.1 Data Confidentiality:

Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to the neighbors.

4.1.2 Data Authentication:

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. Data authentication verifies the identity of the senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication.

4.1.3 Data Integrity:

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. The integrity of the network will be in trouble when:

• A malicious node present in the network injects false data.

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

4.1.4 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. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

4.2 Secondary Goals:

4.2.1 Data Freshness:

Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To solve this problem a nonce, or another time related counter, can be added into the packet to ensure data freshness.

4.2.2 Self-Organization:

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.

4.2.3 Time Synchronization:

Most sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications.

4.2.4 Secure Localization:

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate in secured location information by reporting false signal strengths, replaying signals. This Section has discussed about the security goals that are widely available for wireless sensor networks and the next section explains about the attacks that commonly occur on wireless sensor networks.

5 Security Mechanisms in WSN

The security mechanisms are actually used to detect, prevent and recover from the security attacks. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high level and low-level.

Figure shows the order of security mechanisms.

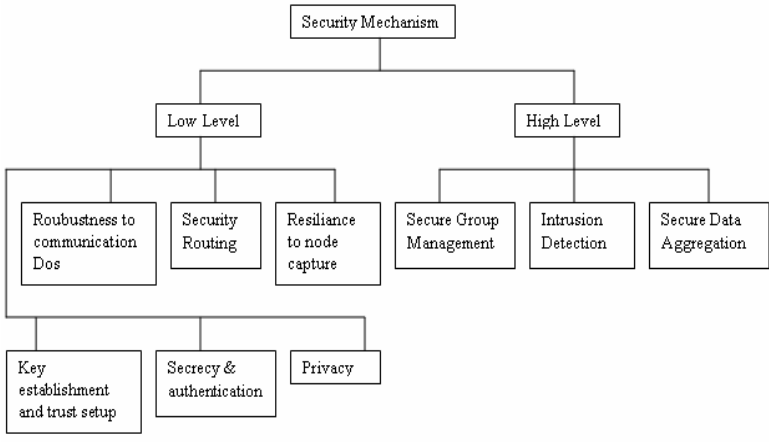


Figure: Security mechanisms

5.1 Low-Level Mechanism

Low-level security primitives for securing sensor networks includes,

5.1.1 Key establishment and Trust setup:

The primary requirement of setting up the sensor network is the establishment of cryptographic keys. Generally the sensor devices have limited computational power and the public key cryptographic primitives are too expensive to follow. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes. In addition, the communication patterns of sensor networks differ from traditional networks; sensor nodes may need to set up keys with their neighbors and with data aggregation nodes. The disadvantage of this approach is that attackers who compromised sufficiently and many nodes could also reconstruct the complete key pool and break the scheme.

5.1.2 Secrecy and Authentication:

Most of the sensor network applications require protection against eavesdropping, injection, and modification of packets. Cryptography is the standard defense. Remarkable system trade-offs arise when incorporating cryptography into sensor networks. For point-to-point communication, end-to-end cryptography achieves a high level of security but requires that keys be set up among all end points and be incompatible with passive participation and local broadcast. Link-layer cryptography with a network wide shared key simplifies key setup and supports passive participation and local broadcast, but intermediate nodes might eavesdrop or alter messages. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network cryptographic approaches.

5.1.3 Privacy:

Like other traditional networks, the sensor networks have also force privacy concerns. Initially the sensor networks 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.

5.1.4 Robustness to communication denial of service:

An adversary attempts to disrupt the network's operation by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed. More sophisticated attacks are also possible; the adversary might inhibit communication by violating the 802.11 medium access control (MAC) protocol by, say, transmitting while a neighbor is also transmitting or by continuously requesting channel access with a request-to send signal.

5.1.5 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. For example, an attacker might launch denial of- service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages.

5.1.6 Resilience to node capture:

One of the most challenging issues in sensor networks is resiliency against node capture attacks. In most applications, sensor nodes are likely to be placed in locations easily accessible to attackers. Such exposure raises the possibility that an attacker might capture sensor nodes, extract cryptographic secrets, modify their programming, or replace them with malicious nodes under the control of the attacker. Tamper-resistant packaging may be one defense, but it's expensive, since current technology does not provide a high level of security. Algorithmic solutions to the problem of node capture are preferable.

5.2 High-Level Mechanism:

High-level security mechanisms for securing sensor networks,

5.2.1 Secure group management:

Each and every node in a wireless sensor network is limited in its computing and communication capabilities. However, interesting in-network data aggregation and analysis can be performed by groups of nodes. For example, a group of nodes might be responsible for jointly tracking a vehicle through the network. The actual nodes comprising the group may change continuously and quickly. Many other key services in wireless sensor networks are also performed by groups. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. The outcome of the group key computation is normally transmitted to a base station. The output must be authenticated to ensure it comes from a valid group.

5.2.2 Intrusion detection:

Wireless sensor networks are susceptible to many forms of intrusion. Wireless sensor networks require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. The use of secure groups may be a promising approach for decentralized intrusion detection.

5.2.3 Secure data aggregation:

One advantage of a wireless sensor network is the fine grain sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. All aggregation locations must be secured.

CONCLUSION

The Wireless Sensor Network suffers from many constraints such as limited energy, processing capability, and storage capacity, as well as unreliable communication and unattended operation etc.Security in Wireless Sensor Network is requisite to the acceptance and use of Sensor networks. Wireless sensor network product in industry will not get embrace unless there is a full corroboration security to the network. We also condense our integrated Wireless security scheme that considered the specific routing characteristics of sensor networks like large scale, Dynamic topology and low energy.

In this article, we focused to dispense a general outline of the major aspects of wireless sensor network security, challenges and attacks, as well as some of some of frequently used shielding approaches.

REFERENCES

[1] Kuthadi Venu Madhav, Rajendra.C and Raja Lakshmi Selvaraj -A Study of Security Challenges In Wireless Sensor Networks, Journal of Theoretical and Applied Information Technology, 2005-2010.

[2] Luis E. Palafox, J. Antonio Garcia-Macias, -Security In Wireless Sensor Networks,‖ IGI Global, 2008.

[3] Hemanta Kumar Kalita and Avijit Kar, -Wireless Sensor Network Security Analysis,‖ International Journal of Next-Generation Networks (IJNGN), December 2009.

[4] Vikash Kumar, Anshu Jain and P N Barwal, -Wireless Sensor Networks: Security Issues, Challenges And Solutions, International Journal Of Information & Computation Technology, Volume 4, Number 8 (2014), pp. 859-868.

[5] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah And Kashif Naseer Qureshi, -Security Issues And Attacks In Wireless Sensor Network, World Applied Sciences Journal 30 (10): 1224-1227, 2014, Idosi Publications, 2014.

[6] Divya Singla, Chander Diwaker, ―Analysis Of Security Attacks In Wireless Sensor Networks, International Journal Of Software And Web Sciences (IJSWS), 14-233; 2014.

[7] Dr. Manoj Kumar Jain, -Wireless Sensor Networks: Security Issues and Challenges, Volume 02, Issue 01, Manuscript Code: 110746, IJCIT, 2011.

[8] Yong Wang, Garhan Attebury, and Byrav Ramamurthy, -A Survey Of Security Issues In Wireless Sensor Networks, IEEE Communications

Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.

[9] Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, and Tanveer A. Zia, ―Threat Models And Security Issues In Wireless Sensor Networks, International Journal Of Computer Theory And Engineering, Vol. 5, No. 5, October 2013.

[10] Jyoti Shukla, Babli Kumari, -Security Threats and Defense Approaches In Wireless Sensor Networks: An Overview, International Journal Of Application Or Innovation In Engineering & Management (IJAIEM), Volume 2, Issue 3, March 2013.

[11] Vishal Rathod, Mrudang Mehta, -Security in Wireless Sensor Network: A Survey, Ganpat University Journal of Engineering & Technology, Vol.-1, Issue-1, Jan-Jun-2011.

[12] Adrian Perrig, John Stankovic, David Wagner, -Security in Wireless Sensor Networks, Communications of the ACM, Page53-57, year 2004.

[13] Chris Karlof, David Wagner, -Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, AdHoc Networks (Elsevier),Page: 299-302, year 2003.

[14] Poonam Khare, Sara Ali, -Survey of Wireless Sensor Network Vulnerabilities and its Solution, International Journal of Recent Development in Engineering and Technology, Volume 2, Issue 6, June 2014.

[15] Hiren Kumar Deva Sarma and Avijit Kar, -Security Threats in Wireless Sensor Networks, IEEE A&E SYSTEMS MAGAZINE, June 2008.

[16] Mahfuzulhoq Chowdhury, Md Fazlul Kader and Asaduzzaman, -Security Issues in Wireless Sensor Networks: A Survey, International Journal of Future Generation Communication and Networking Vol.6, No.5 (2013), pp.97-116.

[17] Vinod Kumar Jatav, Meenakshi Tripathi, M S Gaur and Vijay Laxmi, -Wireless Sensor Networks: Attack Models and Detection, IACSIT Hong Kong Conferences IPCSIT vol. 30, 2012.

[18] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong, -Security in Wireless Sensor Networks: Issues and Challenges, Feb. 20-22, 2006 ICACT2006.

[19] Xiaojiang Du and Hsiao-Hwa Chen, -Security in Wireless Sensor Networks, IEEE Wireless Communications, August 2008.

[20] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, -Security Issues in Wireless Sensor Networks, International Journal of Communications, Issue 1, Volume 2, 2008.

[21] Ranjit Panigrahi, Kalpana Sharma, M.K. Ghose, -Wireless Sensor Networks –Architecture, Security Requirements, Security Threats And
Its countermeasures, Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA – 2013, pp. 107–115, 2013. CS & IT-CSCP 2013.

[22] David Boyle and Thomas Newe, -Securing Wireless Sensor Networks: Security Architectures, Journal of Networks, Vol. 3, No. 1, January2008.

[23] Fei Hu, Jim Ziobro, Jason Tillett and Neeraj K. Sharma, -Secure Wireless Sensor Networks: Problems and Solutions, Systemics, Cybernetics
And Informatics Volume 1 - Number 4.