Categorized Security Threats in the Wireless Sensor Networks: Countermeasures and Security Management Schemes

Ulya Sabeel
Amity University
Noida, Uttar Pradesh
India

Saima Maqbool
Amity University
Noida, Uttar Pradesh
India

Nidhi Chandra
Amity University,
Noida, Uttar Pradesh,
India

ABSTRACT

Sensor networks have been regarded as one of the emerging technologies of the 21st century and have great future scope. They have been widely used in mission critical applications like military, health as well as civilian applications. The focus of this paper is on a security of sensor networks in various fields. Security is the major concern of a wireless sensor network especially in unattended areas. You will get a general introduction about wireless sensor networks in section I, section II explains the need for security in Wireless sensor networks, section III gives security challenges followed by section IV &V that give security and survivability requirements for a Wireless sensor network which follows attack categorization in section VI, followed by the security management schemes in section VII and finally conclusion in the last section VIII.

General Terms

Wireless sensor networks, security, security management schemes

Keywords

Attacks, security, security challenges, security protocols, Wireless Sensor Networks

1. INTRODUCTION

1.1 Background

Sensor networks are dense wireless networks of small, low-cost sensors, which collect and disseminate environmental data. Wireless sensor networks facilitate monitoring and controlling of physical environments from remote locations with better accuracy [2]. They have applications in a variety of fields such as environmental monitoring, indoor climate control, surveillance, structural monitoring, medical diagnostics, disaster management, emergency response, ambient air monitoring and gathering sensing information in inhospitable locations [3, 4, 5].A sensor network is a computer network composed of a large number of sensor nodes. The sensor nodes are densely deployed inside the phenomenon, they deploy random and have cooperative capabilities. Usually these devices are small and inexpensive, so that they can be produced and deployed in large numbers, and so their resources in terms of energy, memory, computational speed and bandwidth are severely constrained. There are different Sensors such as pressure, accelerometer, camera, thermal, microphone, etc. They monitor conditions at different locations, such as temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, the current characteristics such as speed, direction and size of an object. Normally these Sensor nodes consist there components: sensing, processing and communicating.

1.2 Architecture of Wireless Sensor Network and Sensor Node

The architectural diagram for Wireless Sensor Network and sensor node architecture are given below in fig 1 and fig 2.

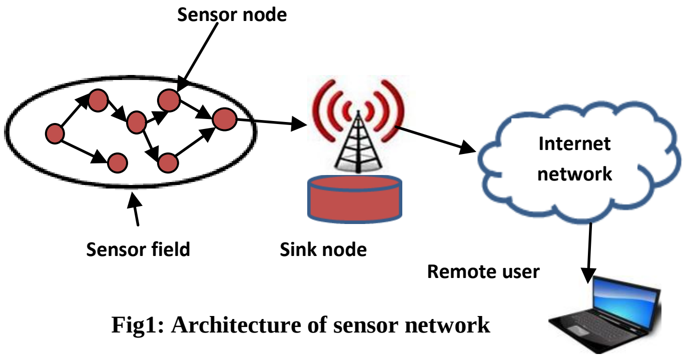

Fig1: Architecture of sensor network

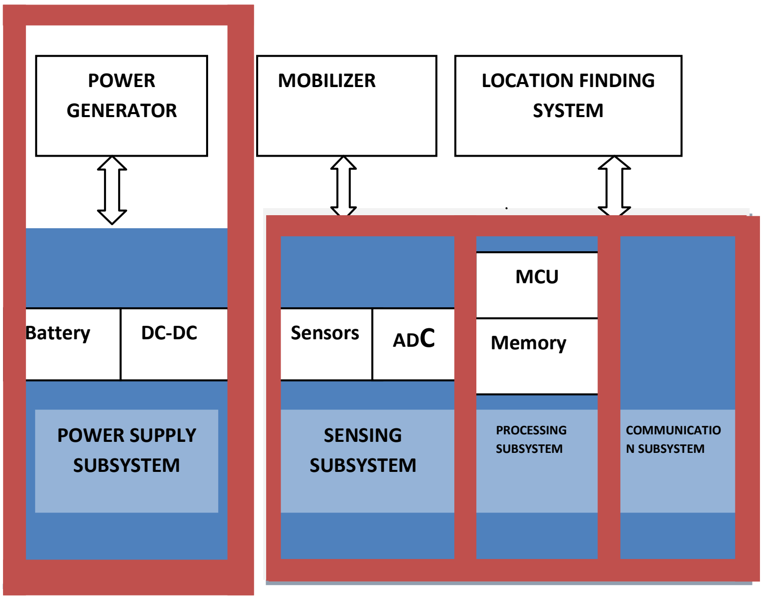

Fig 2: Diagram depicting a Wireless sensor architecture

2. SECURITY IN WSN

Security is an essential characteristic of a wireless sensor network especially in case of military applications that carry highly sensitive information as well as most of the civilian applications. More common attacks are when a node drops a packet and doesn’t forward it. Such attacks cannot be easily detected by checksum. A key requirement from both the technological and commercial point of view is to provide adequate security capabilities. Fulfilling privacy and security requirements in an appropriate architecture for WSNs offering pervasive services is essential for user acceptance and satisfaction [9]. Caused by resource restriction some of WSN applications work without security which decreased Quality of Service (QoS). [8] In order to achieve security and privacy in Wireless Sensor Networks (WSNs), it is necessary to implement and deploy a certain number of mechanisms. Due to the sensitivity of sensor data in many applications the mechanisms for attack detection, prevention of data corruption and vulnerability assessment play an important role. However, the security increases the delay and overhead in operation, higher energy consumption and reduced network lifetime. There is an adaptation of security to the changes in application requirements, context and power consumption in diverse type of application scenarios. In the security context the nodes may be having different security functionalities: (1) the nodes implementing management security functions (for example a coordinator node) and (2) end sensor nodes, performing reduced or even minimum security services. [10]

3. SECURITY CHALLENGES

WSNs have many characteristics that make them very susceptible to malicious attacks in hostile environments such as a military battlefield as well as civilian applications:-

- A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs.
- Most protocols for WSNs do not include potential security considerations at the design stage and are known publicly. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols.
- The constrained resources make it very difficult to implement strong security algorithms on a sensor platform due to the complexity of the algorithms.
- A WSN can scale up to thousands of sensor nodes. These pose the demand for simple, flexible, and scalable security protocols.
- The design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications.
- Weak security protocols can be broken easily by attackers and thus pose a great threat to the sensor networks.
- A WSN is usually deployed in hostile areas without any fixed infrastructure. Thus, difficult to perform continuous surveillance after network deployment. So, it may be susceptible to various kinds of attacks.

4. DATA SECURITY REQUIREMENTS IN WSNs

The harsh environments and existence of threats demand certain security considerations in WSN. These are same as that of the traditional networks .The following services should be provided.

Confidentiality: This is the basic security service in case of WSN. Here we have to maintain the secrecy of the data transmitted between the sensor nodes. As long as the event sensing nodes are not compromised, the confidentiality of the corresponding data report should not be compromised due to any other nodes’ compromise including the intermediate nodes along the report forwarding route. Both the data as well as the header part may be encrypted.

Authenticity: Data reports collected by WSNs are usually sensitive and highly critical, such as in military applications as well as in case of some civilian applications, and hence, it is critical to ensure the identity of the sensor nodes by authenticating them. The compromised node can always send the false / modified messages; the encryption can’t play a vital role here. Every node should check whether the message has come from a real sender. A message authentication code (MAC) can be used to authenticate the origin of the message.

Integrity: Integrity is provided to check that the send message has not been modified by an intruder. The contents of the message can be deleted or modified by the attacker. This may be prevented by providing a message authentication code.

Data Freshness: Data freshness means the recent data that is up-to-date and ensures that no old messages have been repeated and then relayed by the attacker. To solve this problem a nonce, or another time related counter, can be added into the packet to ensure data freshness.

Self-Organization: A wireless sensor network is ad hoc in nature and each node should be independent and flexible enough to organize itself according to the environment. Due to the Infrastructure less feature, there are many challenges imposed on the network security in WSN. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be devastating.

Time Synchronization: Time synchronization is an important feature of most of the sensor network applications. Furthermore, sensors may wish to compute the end-to-end delay of a packet transmitted between two sensors. A more collaborative Sensor network may require group synchronization for tracking applications.

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 locate the exact location of a fault. Unfortunately, an attacker can easily manipulate no secured location information by reporting false signal strengths, replaying signals.

5. SURVIVABILITY REQUIREMENTS FOR WSNS

Reliability: In addition to the security concerns, the reliability of the network is also of special interest because many applications require the WSN to operate in uncontrolled environments. In such cases, some wireless sensor nodes may fail, thus affecting the operation of the whole network. Reliability is the capability to keep the functionality of the WSN even if some sensor nodes fail.

Availability: This indicates to provide all the services whenever they are required. As compromised nodes are assumed to exist in the WSNs, it is important to prevent or be tolerant to their interference as much as possible to protect data availability. In this regard, security designs should be as robust as possible in the presence of compromised nodes. However, attackers can launch attacks to degrade the network performance or even destroy the entire network. A denial of service (DoS) attack [10] is the most detrimental threat to network availability; this occurs when attackers cause the network to lose the capability to provide services by sending radio interference, disrupting network protocols, or depleting the power of nodes through various tricky methods.

Energy efficiency: A WSN consists of battery-operated sensor devices with computing, data processing, and the communicating components. Energy conservation is a critical issue in a WSN, because batteries are the only energy source available to power the sensor nodes. Apparently, the battery life affects the reliability and availability of the WSN. Protocols, including security mechanisms designed for the WSN, should be energy aware and efficient. Evidently, there is a coupling between security, reliability, availability, and energy efficiency of a WSN. [12]

6.ATTACK CATEGORIZATION IN WSN

Sensor networks are susceptible to several types of attacks. Attacks can be performed in a variety of ways, such as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Figure shows the classification of attacks. It is impractical to monitor and protect each individual sensor from physical or logical attack. Here in this section we present a categorization of WSN security threats. The diagram depicting various categories of attacks is given below.

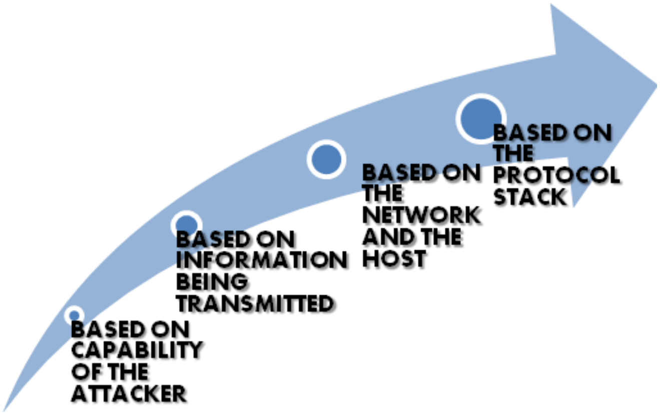
BASED ON CAPABILITY OF THE ATTACKER
BASED ON INFORMATION BEING TRANSMITTED
BASED ON THE NETWORK AND THE HOST
BASED ON THE PROTOCOL STACK

Figure 3: Categorization of Attacks in WSN

6.1 Based On the Capability of the Attacker

6.1.1 Outsider versus insider attacks

Outsider attacks are the attacks from nodes outside a WSN while insider attacks occur when legitimate inner nodes of a WSN pertain to unauthorized ways. To overcome these attacks, we require robustness against Outsider Attacks, Resilience to Insider Attacks, Graceful Degradation with Respect to Node Compromise and Realistic Levels of Security. [13]

6.1.2. Passive versus active attacks

The monitoring and listening of the communication channel by unauthorized parties is known as a passive attack. This involves eavesdropping on or monitoring activities whereas the active attacks involve some modifications of the data packets or sending the packets that are not legitimate.

6.1.3. Mote-class versus laptop-class attacks

The former consists of an attacker attacking a WSN by using a few nodes with similar capabilities to the network nodes; whereas the latter consists of an adversary that can use more powerful devices (e.g., a laptop) to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes. [13]

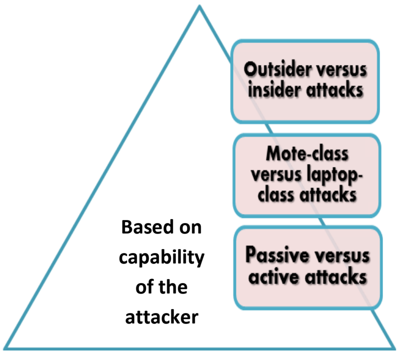
Outsider versus insider attacks
Mote-class versus laptop-class attacks
Passive versus active attacks
Based on capability of the attacker

Figure 4: Attacks in WSN based on the capability of the attacker

5.2 Based on the information being transmitted

In a sensor 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 attacked to provide wrong information to the base stations or sinks. The attacks are:

1. Interruption

Communication link in sensor networks becomes lost or unavailable. This causes the mal functioning of the service. The main purpose is to launch denial-of service (DoS) attacks. This is aimed at all layers of WSN protocol stack.

2. Interception

An interception means that some unauthorized party has gained access to the network ant to its nodes along with the data. An Example of this type of attacks is node capture attacks. This threatens message confidentiality. The main purpose is to eavesdrop on the information carried in the messages. This operation is usually aimed at the application layer of WSN protocol stack.

3. Modification

An unauthorized party not only accesses the data but also tampers it. This threatens message integrity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer of WSN protocol stack, because of the richer semantics of these layers.

4. Fabrication

An unauthorized party inserts spurious data and compromises the trustworthiness of information. This threatens message authenticity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This operation can also facilitate DOS attacks, by flooding the network.

5. Replaying existing messages

This operation threatens message freshness. The main purpose of this operation is to send the same messages again and again or send the old messages on the communication link, in order to confuse or mislead the parties involved in the communication protocol that is not time- aware.

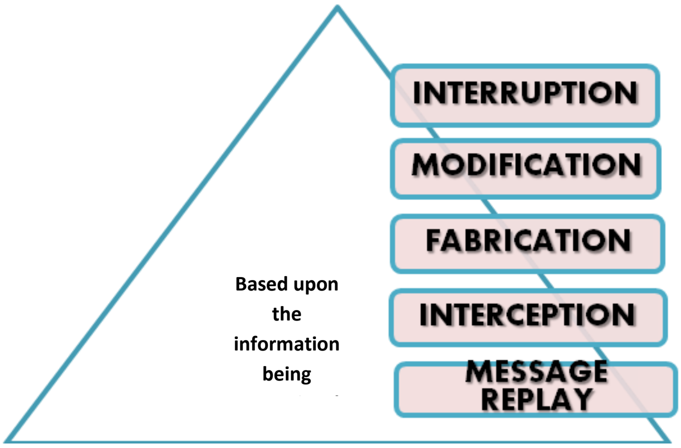

Figure 5: Attacks in WSN based on the information being transmitted

5.3 Based upon the origin of information

6.3.1. Host-based attacks

It is further broken down into the following based upon the type of host involved:-

- User compromise: This involves compromising the users of a WSN, e.g. by cheating the users into revealing information such as passwords or keys about the sensor nodes.
- Hardware compromise: This involves tampering with the hardware to extract the program code, data and keys stored within a sensor node. The attacker might also attempt to load its program in the compromised node.
- Software compromise: This involves breaking the software 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.

6.3.2. Network-based attacks

This consists of two types of attacks: layer-specific attacks, and protocol-specific attacks. It includes the attacks such as attack on information in transit and deviating from protocol: when the attacker becomes an insider of the network, and the his purpose is not to threaten the service availability, message confidentiality, integrity and authenticity of the network, but to gain an illegitimate access for itself in the usage of the network, the attacker adopts selfish behaviors that deviate from the intended functioning of the actual protocol used.

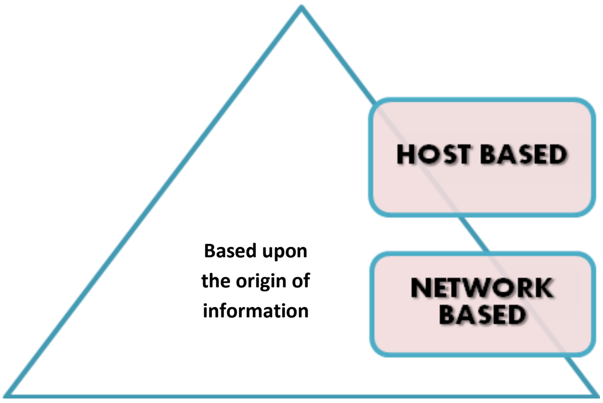

Figure 6: Attacks in WSN based upon the origin of information

6.4 Based Upon the Protocol Stack

Given below is the protocol architecture. In layered approach the protocol stacks consists of the physical layer, data link layer, network layer, transport layer and application layer. These five layers and the three planes, i.e., the security management plane, mobility management plane and power management plane (not shown here) jointly forms the wireless layered architecture.

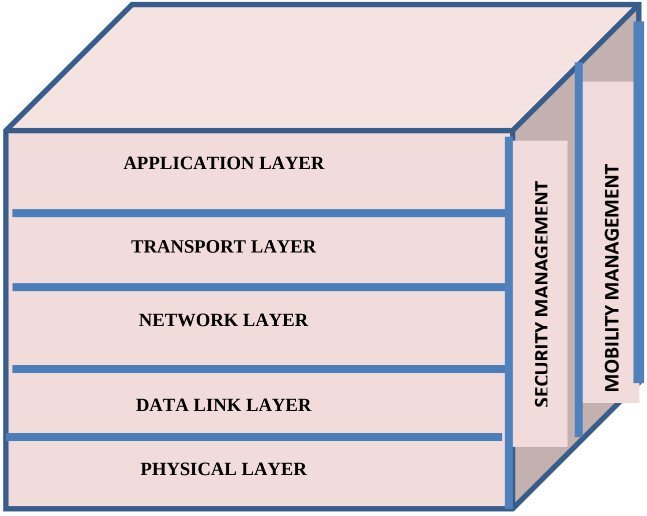

Figure 7: Protocol stack architecture for WSN

6.4.1 Physical layer

The physical layer is the lowest layer in the protocol stack for WSN. The responsibilities of the Physical Layer are frequency selection, carrier frequency generation, signal detection, modulation, and encryption. Its main priority is energy minimization and secondary concerns are the same as those of other wireless networks. [14]

The various types of attacks possible are radio interference, jamming, tampering and Sybil. Most wireless communications use the RF spectrum as a broadcast medium. These messages can be easily intercepted by the intruders and modified or new messages created and injected into the network. **Radio signals** can be **jammed** or **interfered**, which causes the message to be corrupted or lost. The most common types of attacks in in physical layer in WSN are jamming attacks. **Jamming** interrupts the network if a single frequency is used throughout. It also causes excessive energy consumption by addition of infected packets. Examples of jamming attacks include sinkhole and wormhole attack.

Xu, Trappe, Zhang and Wood in 2005 proposed [15] four different type of jamming attack that can be used by an attacker to stop the operation of a wireless network. How each model effects on the sending and receiving capability of a wireless node and its impressiveness was evaluated. It was remarked that no single system of measures such as carrier sensing time and signal strength is adequate for reliably detecting the conduct of a jammer, and that using packet delivery cannot recognize whether poor link service was due to the mobility of nodes or jamming while it may be efficacious in mark as different between jammed scenarios and congested.

Tampering is another attack on physical layer. In this attack, nodes are vulnerable to tampering or physical harm. In case of a **Sybil attack**, a single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network [17]. The table 1 given below describes Physical Layer Attack and Countermeasures in WSN.

Table 1: Physical layer attacks and countermeasures

ATTACK	COUNTERMEASURE
Jamming	Channel hopping, Blacklisting
Radio Interference	Channel hopping, Blacklisting
Sybil	Physical protection of devices
Tampering	Changing the key frequently, Proper Key management Schemes

6.4.2 Data Link layer

The responsibilities of the Data Link Layer are the multiplexing of data streams, data frame detection, medium access and error control. A wireless sensor network must have a specialized MAC protocol to address the issues of power conservation and data-centric routing. Some of the MAC protocols are sensor-MAC (SMAC), Etiquette Protocol, and CSMA for Sensor Networks. [14] Attacks can also be made on the link layer. The various types of the possible attacks here are eavesdropping, Sybil, spoofing, collision, unfairness, exhaustion, denial-of-sleep and de-synchronization. An attacker may violate the communication protocol causing **de-synchronization**, and continuously send messages in an attempt to cause **collisions**. An attacker may consume easily a sensor node's power supply by forcing oversupply retransmissions and thus cause **exhaustion** of the battery power. WSN is susceptible to **denial-of-sleep attacks**, which reduce the network life span from years to days. The attack imposes large amount of energy consumption on the sensor nodes that the entire charge is consumed by the load levied upon the network, and the nodes stop working. In a **Sybil attack**, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. [17] In case of **Eavesdropping**, the adversary (eavesdropper) aims to determine the aggregate data that is being output by the sensor network: it is attempting to see what the system is observing, e.g., to predict how the owner of the sensor network will react. [16] By **spoofing, altering, or replaying** routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc. [13]. Table 2 given below describes Data Link Layer attacks and Countermeasures in WSN.

Table 2: Data Link layer attacks and countermeasures

ATTACK	COUNTERMEASURE
Collision	Cyclic redundancy check, Time diversity
Eavesdropping	Proper key management for Data Link Protocol Data Unit (DLPDU)
De-synchronization	Use different neighbors for time synchronization
Sybil	Regular changing of the key
Spoofing	Different paths to be used for message resend
Traffic analysis	Regular monitoring of the network, Send dummy packets at regular intervals
Exhaustion	Protection of Network ID and other Information that is required to joining device
Denial of the sleep	Regular monitoring of the network, checking the battery power at regular intervals

6.4.3 Network Layer

The network layer [14] in a WSN must be designed with the following considerations in mind: power efficiency, WSNs are data-centric networks, and WSNs have attribute-based addressing and location awareness. The Link layer handles how two nodes talk to each other, the network layer is responsible for deciding which node to talk to. Network layer is susceptible to various attacks. These may include eavesdropping, DoS, Selective forwarding, Sybil, Traffic analysis, wormhole, sinkhole, hello flood, node capture, black hole, spoofing, acknowledgment spoofing, misdirection, internet smurf attack and homing.

Out of these attacks, eavesdropping, spoofing, Sybil and Traffic analysis have already been explained in the attacks on Data link layer section. A **sinkhole attack** tries to lure almost all the traffic toward the compromised node, creating a metaphorical sinkhole with the adversary at the center. 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. If they drop all the packets through them, then it is called a **Black Hole Attack**. However if they **selectively forward** the packets, then it is called selective forwarding. **Hello Flood attack** exploits Hello packets that are required in many protocols to announce nodes to their neighbors. A node receiving such packets may assume that it is in radio range of the sender. A laptop class adversary can send this kind of packet to all sensor nodes in the network so that they believe the compromised node belongs to their neighbors. This causes a large number of nodes sending packets to this imaginary neighbor and thus into oblivion**.** In the **Wormhole Attacks**, an adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. This is usually done with the coordination of two adversary nodes, where the nodes try to understate their distance from each other, by broadcasting packets along an out-of-bound channel available only to the attacker. **Spoofed, Altered, or Replayed Routing Information** is the most direct attack against a routing protocol in any network is 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. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency. An attacking node can spoof the Acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes. **Homing** uses traffic pattern analysis to identify and target nodes that have special responsibilities, such as cluster heads or cryptographic- key managers. An attacker then achieves **DoS** by jamming or destroying these key network nodes. **Misdirection** is a more active attack in which a malicious node present in the routing path can send the packets in wrong direction through which the destination is unreachable. In the **Internet Smurf Attack,** the adversary can flood the victim node's network link. The attacker forges the victim's address and broadcasts echoes in the network and also routes all the replies to the victim node. This way the attacker can flood the network link of the victim. If it gets observed that a node's network link is getting flooded without any useful information then the victim node can be scheduled into sleep mode for some time to overcome this.[13] Various attacks and their countermeasures are given below:-

ATTACK	COUNTERMEASURE
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing, Monitoring system may use packet LEACH techniques
Traffic Analysis	Regular monitoring of the network, Send dummy packets at regular intervals
Eavesdropping	Proper key management for Data Link Protocol Data Unit (DLPDU)
DoS	Physical protection & inspection of network, protection of network specific ID
Selective forwarding	Regular network monitoring using source routing
Sybil	Regular changing of the key and resetting the device
Sinkhole	Use Geo-Routing protocols, Topology with localized information
Blackhole	Multi path Routing with random selection of paths
Spoofing	Efficient encryption and authentication techniques, Use MAC with each message
Acknowledgement Spoofing	Authentication via encryption
Node capture	Groundbreaking, Physical monitoring
Homing	Header Encryption technique
Hello Flood	Authentication of the message over bi-directional link
Internet Smurfing	Affected node switched to SLEEP mode
Misdirection	Affected node switched to SLEEP mode

6.4.4 Transport Layer

The transport layer comes into play when the system needs to communicate with the outside world. Communication from the sink to the user is a problem because the Wireless Sensor Network is not based on global addressing and attribute-based naming is used to indicate the destinations of DATA packets.[14]

The Transport layer is also vulnerable to some attacks as Flooding attack and de-synchronization attack. In case of **Flooding**, many connection requests are sent until the resources required by each connection are exhausted or reach a maximum limit. Eventually the node's resources are exhausted and render it useless. In the **de-synchronization attack**, the attacker repeatedly forges the messages to one or both end points which request transmission of missed frames. Hence, these messages are again transmitted and if the attacker maintains a proper timing, it can prevent the end points from exchanging any useful information. This causes a considerable drainage of energy for recovering the compromised nodes. Given below is the table for transport layer attacks and countermeasures.

Table 4: Transport layer attacks and countermeasures

ATTACK	COUNTERMEASURE
Flooding	Limit the number of connections for a node
De-synchronization	Header or full packet authentication

6.4.5 Application Layer

This is the topmost layer of the sensor network protocol stack. A Sensor Management Protocol, SMP, [14] at the application layer is used to make the hardware and software of lower layers transparent to the Sensor Network Management Applications. The system administrators and programmers with interact with the Sensor Network using SMP. Again the lack of global identification and infrastructure less nature of sensor networks must be taken into consideration.

Three types of attacks are common on this layer. These include: path based DoS, Overwhelm attack, Deluge or reprogram attack. The **path based DoS attack** involves sending extra or replayed packets into the network on the leaf nodes. This occupies the resources of the entire network and starves the legitimate traffic. In **Overwhelm attack**, an attacker might attempt to overwhelm network nodes with sensor stimuli, causing the network to forward large volumes of traffic to a base station. This attack also consumes network bandwidth and drains node energy. The third attack is **Deluge (reprogram) attack** where [13] Network programming system lets you remotely reprogram nodes in deployed networks. If the reprogramming process isn't secure, an intruder can hijack this process and take control of large portions of a network. These attacks with their countermeasures can be shown in the table below.

Table 5: Application layer attacks and countermeasures

ATTACK	COUNTERMEASURE
Path based DoS attack	Authentication, Anti-replay protection
Overwhelm attack	Efficient data aggregation algorithms, Rate limiting
Deluge (reprogram) attack	Authentication

6. SECURITY MANAGEMENT SCHEMES

The major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. This, combined with a large number of threats, makes it unusually hard to build security solutions for WSN. The proposed security management schemes are very useful for detecting and mitigating the security attacks on the wireless sensor network. These may be categorized as low level and high level [20] as shown in the figure.

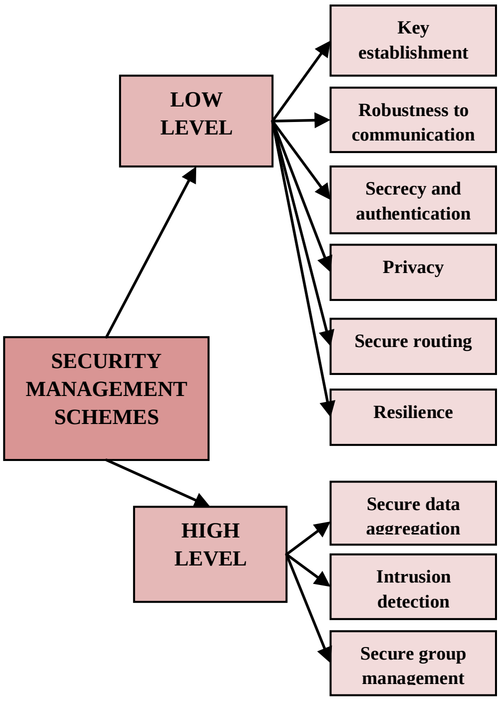

Figure 8: Security Mechanism in WSNs

7.1 Low-Level Mechanism

Low-level security primitives for securing sensor networks includes:-

1. Key establishment and trust setup

2. Secrecy and authentication

3. Privacy

4. Robustness to communication denial of service

5. Secure routing

6. Resilience to node capture

7.1.1 Key establishment and trust setup

Due to the resource constraints especially limited battery power, asymmetric key cryptography should be should be avoided in the sensor networks. Thus our aim should be setting up of the symmetric keys. Various communication patterns can be adopted unicast, local broadcast and global broadcast. Key-establishment techniques need to be used in the networks with hundreds or thousands of nodes. Various types of keys can be used node keys, cluster keys and network keys. The disadvantage of this approach is that there is no tamper resistance and the attackers can generate all the keys and break the privacy of the network.

7.1.2 Secrecy and authentication.

Just like the other traditional networks, the sensor network applications require protection against eavesdropping, attack injection, dropping and modification of packets. Cryptography is the standard technique for defense. 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.[19] Cryptography not only increases efficiency but also increases the cost of implementing a network. 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.

7.1.3 Privacy

Like other traditional networks, the sensor networks have also to enforce privacy concerns. There are many risks to sensor networks like the illegitimate users accessing the network for unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is particularly important. A lot of research needs to be done in this area so as to provide valid security schemes for protecting the sensor networks.

7.1.4 Robustness to communication denial of service

A DoS attack reduces the network's capacity to perform its intended function. There are many reasons behind this kind of attack such as hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors. An attacker attempts to disrupt the network's operation by broadcasting a high-energy signal so that the entire system's communication could be jammed and also by transmitting while a neighbor is also transmitting or by continuously requesting channel access with a request-to-send signal. The spread spectrum technique is effective to mitigate this kind of attack. Sensor networks should already be designed to continue functioning even in the presence of faults. This robustness against physical challenges may prevent some classes of DoS attacks.

7.1.5 Secure routing

In order to enable communication in sensor networks, routing and data forwarding is a crucial service. But, the current sensor routing protocols suffer from many security vulnerabilities such as jamming of the network. Sensor networks are particularly susceptible to node-capture attacks. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Devising simple authentication schemes and secure routing protocols might guard against such attacks.

7.1.6 Resilience to node capture

Node capture is a severe threat to data security in Wireless Sensor Networks. Most applications deploy sensors in the locations that are easily accessible to attackers. An attacker can have illegal access to the network and might capture sensor nodes, extract cryptographic secrets, modify their programming, or replace them with malicious nodes under the control of the attacker. Some of the defense techniques are Tamper-resistant packaging, Algorithmic solutions, Hashing technique, and gathering of multiple redundant views of the environment to cross check them for consistency.

High-Level Mechanism

High-level security mechanisms for securing sensor networks, includes secure group management, intrusion detection, and secure data aggregation.

7.2.1 Secure group management

Due to the nature of communication, limited computing power and the kind of data the sensors are going to handle, it is important to have the capability in the network to establish trusted communication. For this purpose, the formation of secure groups in sensor network with a low communication complexity and provide an efficient solution to maintain such multicast group is important. 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. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. [18]

7.2.2 Intrusion detection

An intrusion can be defined as a set of activities that can lead to an illegitimate access or alteration of information in a certain system. Wireless sensor networks are susceptible to many forms of intrusion. The task of Intrusion Detection Systems is to monitor the sensor networks, detect any possible intrusions and send the alert message to the user. Wireless sensor networks require an inexpensive solution in terms of communication, energy, and memory requirements. For decentralized intrusion detection, use of secure groups may be a promising approach.

7.2.3 Secure data aggregation

The data collected from the individual nodes is aggregated at the base station. Due to the various constraints on the wireless sensor networks, they are vulnerable to a large number security attacks. The compromised nodes can be used to inject false data that leads to incorrect aggregates being computed at the base station. Thus, all aggregation locations must be secured. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. Secure routing protocols and authentication schemes are useful to prevent the attackers to inject false data into the system.

8. CONCLUSION

This paper gives an overview of the general concept of wireless sensor networks. In case of unattended areas, especially mission critical areas like Military, Health and in other civilian applications, WSNs play a major role. In highly unattended areas, WSNs become vulnerable. Security is an important feature for deploying the sensors. This paper summarizes various requirements and security challenges of sensor networks and also categorizes various security attacks and their countermeasures, finally various security management schemes to increase the level of security for WSNs. In future, we would like to propose an optimized secure framework for WSNs along with some robust security protocols for maintaining security requirements in WSNs.

9. REFERENCES

[1] "21 ideas for the 21st century," Business Week, pp. 78-167, Aug.39, 1999.

[2] H. Karl and A. Willig, "Protocols and Architectures for Wireless Sensor Networks", John Wiley and Sons Ltd, the Atrium, Southern Gate, Chichester, West Sussex, England, 2005.

[3] D. Culler, D. Estrin, and M. Srivastava, "Overview of Sensor Networks", *IEEE Computer*, August 2004.

[4] K. Martinez, J. K. Hart, and R. Ong, "Environmental sensor networks", *IEEE Computer Journal*, Vol. 37 (8), 50-56, August 2004.

[5] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk , and J. Anderson, "Wireless sensor networks for habitat monitoring", Proceedings of the 1st ACM International workshop on Wireless sensor networks and applications, Atlanta, Georgia, USA, 88-97, 2002.

[6] http://en.wikipedia.org/wiki/Sensor_Networks

[7] Akyildiz, I.F., W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, August, 102-114(2002).

[8] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh , "Overview of Security Issues in Wireless Sensor Networks" , 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, , © 2011 IEEE

[9] Dirk Westhoff, Joao Girao, Amardeo Sarma , "Security Solutions for Wireless Sensor Networks"

[10] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, "A Security, Privacy and Trust Architecture for Wireless Sensor Networks", 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia

[11] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer Mag., vol. 35, no. 10, Oct. 2002, pp.54–62

[12] Yi Qian and Kejie Lu, David Tipper, "A Design for secure and survivable wireless sensor networks", IEEE Wireless Communications • October 2007 © 2007 IEEE

[13] Chaudhari H.C. and Kadam L.U., "Wireless Sensor Networks: Security, Attacks and Challenges", International Journal of Networking Volume 1, Issue 1, 2011

[14]http://www.thecourse.us/Students/Wireless_Sensor_Networks.htm

[15] W. Xu, *et al.*, "The feasibility of launching and detecting jamming attacks in wireless networks," 2005, pp. 46 57

[16] Madhukar Anand, Zachary Ives, Insup Lee, "Quantifying Eavesdropping Vulnerability in Sensor Networks" , *Proceedings of the 2nd International VLDB Workshop on Data Management for Sensor Networks 2005 (DMSN 2005)*, pages 3-9. Copyright ACM, 2005

[17] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International conference on Advanced Computing Technologies, Page1043-1045, year 2006

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

[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] "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", Dr. G. Padmavathi, Mrs. D. Shanmugapriya, *(IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2*