Security Attacks, Countermeasures and Solution Protocols in Wireless Sensor Network: A Review

Zeenat Amjad[1] and Sehrish Tabbasum[2],

University of Lahore ,Gujarat Campus University of Lahore ,Gujarat Campus

Abstract

There are numerous wireless sensor network (WSN) applications day to day being developed. Ranges of these applications from simple environmental monitoring such gathering temperatures in an agricultural farm to complex applications such as monitoring battle fields. Severally energy constrained are WSN since many sensor networks are designed to operate unattended for a long time and battery recharging and replacement may be in feasible or impossible. To optimize the limited capability of the sensor nodes, security requirements are generally abandoned. As the applications increase so are the attacks also. In this paper we focus on security requirements attack categorization which is based on capability of attacker, information being transmitted and origin of information. We perform analysis of Attacks on different network layers and their countermeasures in WSN. To become defensive form attacks There are several protocols of security have been introduced to be used with applications differently which have varying security requirement; this implies that the choice for the WSNs applications. The conventional techniques fail to find its way from security threats due to the limited resource availability in these types of networks.

Keywords:

Attacks, Security, security challenges, security protocols, countermeasures ,wireless Sensor Networks..

1. Introduction

Wireless sensor network is a growing faster network of sensing devices and applications in different areas e.g industry , cyber physical system, health care system and military.wsn consists of several low-price sensors that have limited resources like low processing units, low memory, low bandwidth , low battery supply[1]. Sensors have built-in capabilities along with a sensing unit. Sensors are small in sizes but can perform well with the heterogeneous sensor network. Wireless sensor network provide efficient load balancing, scalability, delay tolerant .The sensor sense the data from physical environment such as they sense the temperature, humidity, accident on the road, or in the battle field. Sensitive data transmission between node to node and the whole network, the security is the main and prior function in the WSN[3]. Because of its wired free structure the security can be compromised.

Manuscript received January 5, 2025
Manuscript revised January 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.1.11

With the advancement of technology the security threats increases rapidly. Numerous threats and attack are found in wireless sensors network. The security requirement of the WSN include:-Confidentiality, integrity, authorization and authentication [4]. Because of the distributed node system the attacker can easily have access to the sensor in the field. The WSN adopted the OSI Layer model because of its several layered protection with a specific protocol. These protocols at different layers protect the data from the different attacks by attacker and environment.

Sensor networks are basically small, low-power and low cost devices that designed for short range communication to sense environment with limited storage and processing speed.WSN is network of sink and nodes sink is a gateway that provide connection to server through internet act as access point [8]. Sensor nodes use RF band for communication to inter or outer the network the security is the main issue because protection of network get difficult when broadcasting gets done so many intruders can alter, inject into the data. These intruders can attack the network internally and externally like in the network by using nodes or can make some resource utilization attack that can ruin the battery and make processing slow. Use of some cryptography mechanism by establish some key between two sensor device can prevent some attack that algorithm must consider the limited resources of senor network like low power consumption and less complexity. [2]

OSI layer Name	Purpose
Application	Security
Transport	
Network	
Link	
Physical	

Figure 1: Layered Security model

The figure1Shows the OSI model layers which include application layer, transport layer, network layer, Link layer, physical layer. Cryptographic techniques use to improve the confidentiality, authentication improves the integrity, data encryption and decryption provide the secure transmission of data.

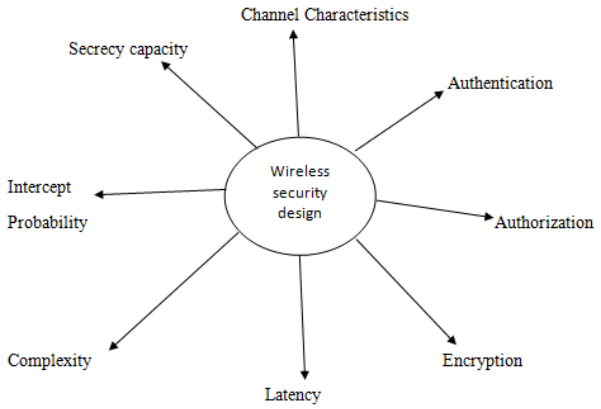

Figure 2 : wireless security methodology

The main methodology include the Authentication , authorization and encryption for which the diverse design factors e.g security level, implementation complexity and communication latency need to be balanced.
This paper focuses on different kind of attacks their description and countermeasures, security requirements, attack categorization based on capability of attacker, information being transmitted and origin of information Analysis of attacks at different layers and some important security protocols provide solution against these attacks and provide security of network.

2. Literature Review

In this paper (Thomas newe, healy 2009) wireless sensor network rapidly spreading in environment monitoring application and heterogeneous application. The WSN adopted because of its advancement feature they can monitor the field working , objects motion , the humidity level in the air , the temperature reading sensor , the road safety sensor to monitor the security of any emergency or accident happen on the road can be monitored by these sensors. Three categories of application scenarios such as: - 1) Smart building WSN, 2) environmental monitoring WSN, and 3) structural health monitoring WSN. In the environmental applications of the famous and historical spring brook rain forests of Australia is references application for its security and vulnerabilities. The responsibilities includes temperature monitoring, speed of wind, soil moisture, wetness of the leaves and direction of wind. The use of bio-acoustic technique along with videos monitoring that provides security. In the second category application which is structural monitoring use to find the damage or defect in the civil side constructions at initial levels. In the tunnel and bridges it uses to detect the damaged through vibration mechanism. For small amount of devices smart building WSN is use to perform task and perform security. Hybrid cryptographic algorithm is a solution for high and medium scale applications but not for small level applications because of their resources constraints. DES and Blowfish algorithm is feasible for less applications.[1]

In this paper (Harish,Sheng wen 2017) security attacks are more vulnerable to wireless sensor networks as compared to wired network. Protective Solutions and mechanism are required to ensure the secrecy of data transmission in the network. A protocol which authenticated node and check message integrity by applying symmetric security algorithm at link layer is Link Layer Security Protocol (LLSP).

In this paper (Bhasin , Kumar2018)the advancement of the technology number of applications with sensing integration capability are increasing rapidly. The structure of the network depends on the nature of the environment in which they integrate the devices. The architecture of the WSN has various constraints like energy consumption, small nodes and node life time. To provide high security within limited resources is a challenge. The use of sensing applications in area monitoring ,construction work ,environmental monitoring, Landfill Ground Well level monitoring and pump counter, Medical /Health, Vehicle Detection, Greenhouse monitoring, windrow composting, Flare Stake Monitoring, Military, Physical world. Energy issues and miniature are not yet solved.

In this paper (Paul, Delicato) the wireless sensor network is a network with multiple devices those are capable of sensing, storing, and processing and communicate wirelessly. The node is specific to a task for which it is made. The node sense data from environment, forward it to next node which perform some processing and the to the main data center for further use. Systematic literature review conclude WSN self properties (self adjustment, self protection). Different approaches to manage dynamic behavior in middle-ware system: - content based reasoning, mobile agents, code generation. Autonomy of sensor networking support by system architecture designs.

In this paper (Abdullah Al hayayeh, Ian 2020) wireless sensor network gathered sensitive data due to the limited resources traditional security solution not fulfill the security requirement of data transmission. Review of threat and attacks in the current architecture of the WSN. The threat is categories on the bases of attacker capabilities, access level and intervention of the attacker. Attack can be insider or outsider. Non-invasive attack includes power frequency based. The attacker can add new node in the current network that behave same as part of network but collect the data and transmit it to the hacker. DoS attacks, Routing attacks, non repudiation attack,

Attack on information in transit. Current security solutions are 802.15.4, zigbee, Bluetoot, TinySec, GenSec, MiniSec, Spins.But yet no solution that can perform all security requirements.

In this paper (Ritu and Yogesh et al, 2010) presents security constraints, security requirements and types of attacks ,their description and purposed solution for these attack like security protocols that provide security by security providing security mechanism. By adding in this paper discuss some threat model and description of security protocols like Sneap, µtelsa, Tinysec, Minisec, Leap, 802.15.4, Zigbee and make comparison based on encryption, CTR, overhead bytes , Mac used and ,Key agreements. These protocols also consider the power consumption, processing speed and efficacy.

In this paper (Aditi and Sanjeet et al, 2017) focuses on WSN applications which are vulnerable to different attacks due to security issues so handle these attacks this paper discuss some cryptography and stereography as security mechanism and some routing security protocol that handle attacks at network layer and all this done at node level. This paper also discus some key distribution management by some security mechanism. Security protocols are discuss in this paper(LSM) line selected multicast, Randomized efficient and distributed(RED), (LSCD), SPIN, Logical key hierarchy based model(LKHW), LEAP,CL-EKM and CRS-A.

In this paper (Tomic and Julie et al, 2017) target some potential security issues in existing protocol in WSN discuss some security requirements, mechanism, features and security vulnerability at different OSI layer discussions of some attacks on different network layers and their countermeasures. Discuss IEEE 802.15.4, B-MAC, and 6LoWpan, RPL, BCP, CTP and Caop. Also discuss security attacks and mechanism of each protocol and use cooja tools to check some security protocol performance.

3. Challenges in Security requirements for sensor networks

Prior knowledge lack in post deployment configuration: Sensor node if deployed via random scattering, protocols in the network cannot know which nodes will be in with in communication range of each other deployment beforehand. Pre determine the location of individual node in a network of large nodes makes it costly. Hence node will be the neighbors in network should not be assumed in a security protocol prior knowledge.

Limited memory resources: Key storage amount of memory in given node is highly constrained; Resources doesn't possess to establish unique keys with everyone and neighbor node in the network.

Limited Bandwidth and transmission power: Typical platform of sensor network have a very low bandwidth[23].

3.1 WSN Security Goals

Four goals of wireless sensor networks are summarizes in this section. They are data confidentiality, data integrity, message authenticity, network availability.

Data confidentiality: - Refers to the content of the message being concealed other than the destination node from every node to prevent message content disclosure by the attackers.

Data integrity:-Refers to content of message not being tempered or modified. Intentionally adversary can also alter the message content. Can occur due to falsified data injection by the attacker.

Message authenticity:-Message reliability must be ensuring by the destination node upon message reception by identification of the source. Data transmitted by attacker or the malicious nodes this prevents from acceptance.

Network availability: - Data prevent by adversary from being accepted by legitimate nodes. Access allow to legitimate users to access the network any time and any where upon request[23].

Table1: various security requirements and their objectives

Security Requirements	**Objectives**
Confidentiality	Data access limited only to legitimate users
Integrity	Prevention falsification and data accuracy transmitted guarantees
Authenticity	Authorized and unauthorized users differentiation
Availability	Make sure that the legitimate node is capable of accessing the network any time and any where upon request.

4. Threats and Attacks on wireless sensor networks

Active attacks and passive attacks:-Data modified in active attacks and are Black hole, Sybil, HELLO, Denial of services, Flood attacks, worm hole attack. In passive attacks are such as; against privacy attack, traffic analysis, eavesdropping (Padmavathi & Shanmugapriya 2009)
WSN attacks are categories in following three

Authentication and Secrecy attacks: such as eaves dropping, spoofing, and replay packet attacks.
***Network availability attacks*:** DoS Stealthy attack against service.
Integrity: WSN acknowledge a false data value makes by attacker e.g injection through of false value data.
Attacks against routing mechanisms and security mechanism (pathan, Lee & Hong, 2006)

4.1 Major WSN Attacks

Hello flood attack: Attack is happen when assumption is made HELLO packets broad casting by the node that is genuine neighbor.
Wormhole attacks: Tunneling of messages over alternatives low-latency links, to confuse the routing protocols, creating sink holes etc.
Sink hole Attacks*:* Attracting traffic to a specific nodes, e.g to prepare selective forwarding[26].
Sybil Attack: A single node can present itself in multiple ways/identities to the other entire node in WSN network.
Spoofed Altered*:* Some packets are transmitted but some are dropped in network transmission.
Attacks on information in transit: A big problem in WSN is traffic analyses can potentially allowing the attacker to map the routing layout of a network.
Node Replication attack*:* The attack replace the network node with new node or can add the new node with the current network which can act as similar to old node are behave different by performing some extra task[23].

5. Attacks Categorization

Several types of attacks are susceptible to sensor devices. In a variety of types attacker can attack on network such as DoS, traffic analysis and so many internal and external attacks. Due to broadcast nature of WSN it is more vulnerable to different kind of attacks we describe its classification in this section [23].

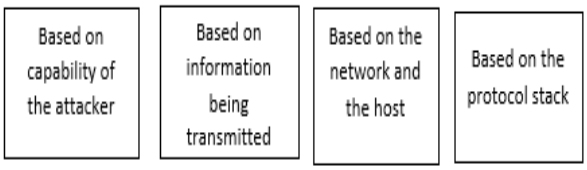

Figure 3: Attack Categories in WSN

Figure 2 show the categorization of attacks base upon attacker, information, origin of network and protocol stack now we will provide the description of each one[13].

5.1 Based on the capability of the Attacker

Insider vs outsider attacks:- Attacker that has no specific access to the network node are outsider while insider is when some of the specific node security is compromised by applying some malicious code. Robustness require as a countermeasure against outsider attack and for insider level of security at real level is required [13].
***Active vs passive attacks*:** - Idle listening and monitoring the channel communication without harm to any network device is passive. To add, change, or remove data from a communication channel is active attack.
Laptop-class vs Mote-class attacks*:*- Access to the legal and powerful devices of the network like cable processor or battery is laptop class attack. Mote-class attacks have access to the small devices with the same capabilities.

5.2 Based on the information being transmitted

Sensor devices are used to sense the data from the environment on specific values or parameters changes report forward to the sink as per requirement .In between the transmission of report the false data can be replace with the original report. The attacks are as following:-
***Interception*:-**Un-authorized access gain by the third party and also to the node with the data it holds.e.g node capturing attacks [18].

***Modification*:-**Data not only accessible but can be changed or delete by the third party that is un-authorized e.g. message integrity can be compromised.
Interruption: - Communication channel link become unavailable e-g node capturing attack. Protocol stack at all WSN layer is aimed [23].

5.3 Based upon the origin of information

Host base Attack
User compromise:- Revealing information about the user-end e.g password crack
Hardware compromise:-Attack on the hardware to crack and trying to run the code on the node.

Table 2: Layer base Attacks and countermeasures

OSI Layer	Attack	Counter measure
Physical layer	Jamming	• Black listing • Channel hopping
Physical layer	Sybil	• Physically protect the devices
Physical layer	Radio Interference	• Black listing • Channel hopping
Physical layer	Tampering	• Key management • Frequently changing the key
Data-Link Layer	Sybil	• Regularly change the key
Data-Link Layer	Collision	• Diversity of time • Check cyclic redundancy
Data-Link Layer	Spoofing	• Alternate paths used for message resend
Data-Link Layer	Eaves dropping	• Proper key management for Data link protocol data unit(DLPDU)
Data-Link Layer	Traffic analysis	• Monitor the network regularly • At regular interval of time send dummy packets
Data-Link Layer	De-synchronization	• For time synchronization use different neighbors
Data-Link Layer	Denial of the sleep	• Check battery power and monitoring the network at regular interval of time
Data-Link Layer	Exhaustion	• Protect the network ID use to connect the device
Network Layer	Worm hole	• Field devices monitoring physically • Use source routing for regular monitoring • LEACH techniques use to monitor
Network Layer	DoS	• Protect Network ID • Network inspection
Network Layer	Sybil	• Change and resetting the device regularly
Network Layer	Traffic analysis	• Monitor the network regularly • At regular interval of time send dummy packets
Network Layer	Eavesdropping	• Proper key management for Data link protocol data unit(DLPDU)
Network Layer	Selective forwarding	• Source routing to check network at daily interval
Network Layer	Black hole	• Routing through multipath • Path selection randomly
Network Layer	Node capture	• Monitor Physically • Groundbreaking
Network Layer	Sink hole	• Topology with localized information • Use-geo routing
Network Layer	Hello Flood	• Message authentication over bi-directional link
Network Layer	Homing	• Use header encryption technique
Network Layer	Mix direction	• Use sleep mode for affected node
Network Layer	Internet surfing	• Affected node switched to SLEEP mode
Transport Layer	De-Synchronization	• Authenticate header or full packet data
Transport Layer	Flooding	• No of connections limited for a node
Application Layer	Deluge (reprogram)	• Authentication
Application Layer	Path based Dos	• Anti replay Protection • Authentication
Application Layer	Overwhelm	• Limiting rate • Efficient data aggregation algorithms

Software compromise: - Attack on the software that is running on the node of the network [21].

Network base attack

Two types of attacks and are

Layer specific: - Attack on information while transmission from protocol its purpose is to get the access in the network

Protocol specific: - Attack on the actual protocols to deviate its function [23].

5.4 Based on protocol Stack

Protocol architecture consist of protocol stack that contain different layers of network ,physical layer, data link layer, routing or network layer, transport layer and application layer[19]. Table 2 shows that each layer specifies different kind of attacks related to that layer only and their corresponding countermeasure are discussed [23].

6. Security Attacks in Wireless sensor network

Here are different kinds of attacks we make classify in different categories we discussed layer wise Attack and their countermeasure .this picture show the summary of performer oriented Attacks and goal oriented attacks

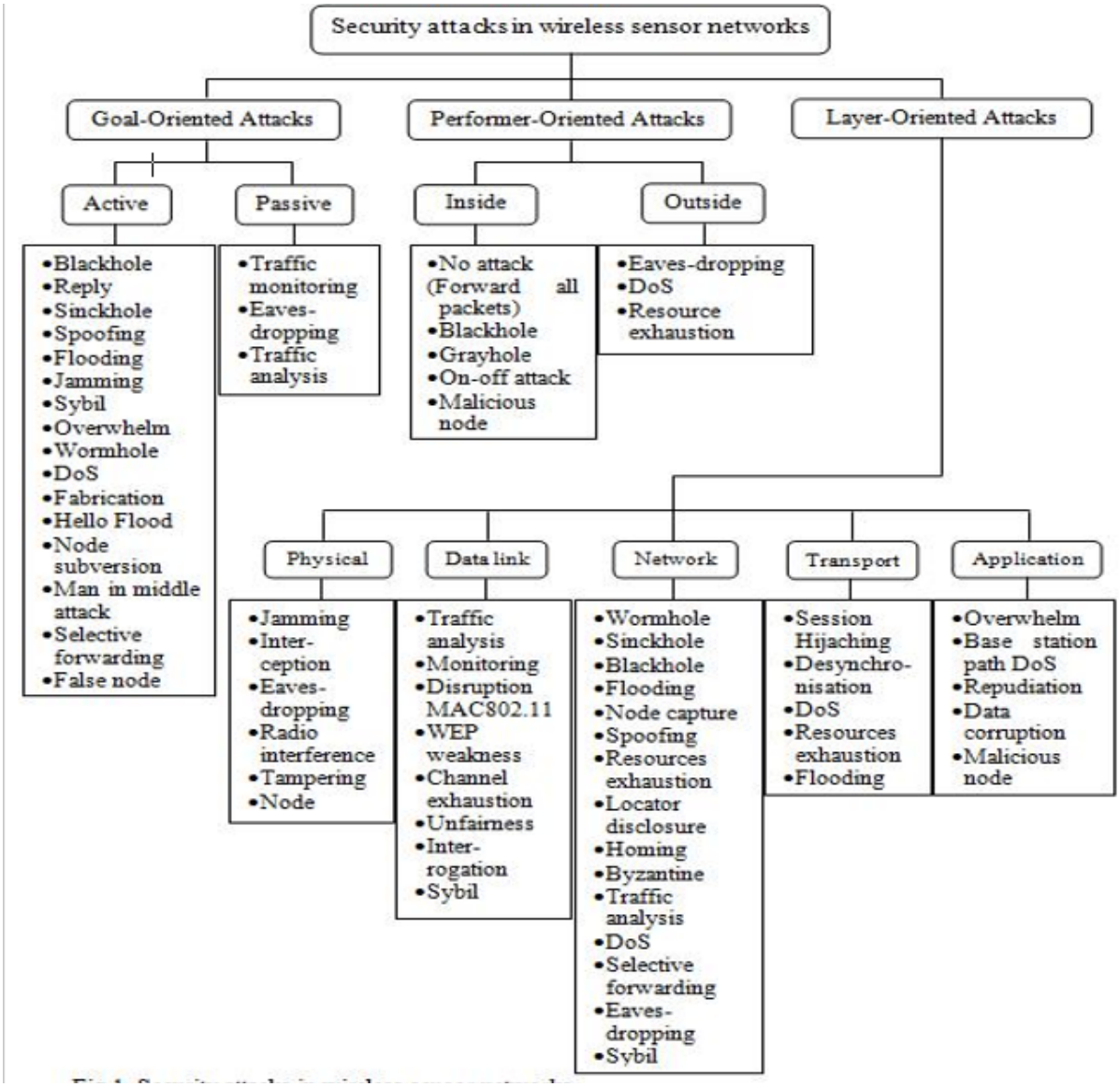

Figure 4: security attacks in WSN

Although we just give detail description on layer base attack and counter measures in the next section we will analyze the attacks and how these fulfill the security requirements. First we categorize the attacks based on some content then divide that attacks layer wise in protocol stack.

Manuscript received January 5, 2025
Manuscript revised January 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.1.11

6.1Analysis of possible attacks and threats

The attackers made unauthorized effort for gaining the data access in the availability of the data. As the WSNs can be exposed to several numbers of attacks which are briefly discussed, classify and explain in this papers and a related table is given below with their description.

Table 3: Analysis of security Attacks

Security Requirements	**category**	**Possible attacks**		**Description**
Confidentiality and Authentication	Attacks on privacy	Passive monitoring attack and eavesdropping		The data that is communicated can be listening and realize its content easily to adversary.
		Camouflage attack		Malicious new node is attach in the current network that act similar as other node but forward the data to the attacker
		Traffic analysis		Some node can be detected by attacker with the added functionality of providing information about communication.
		Node replication attack		Entire network communication can be replicate
Service integrity		Stealthy Attacks		Attacks against service integrity than can forced wsn node for accepted communicate false value.
Service integrity	Denial of services attacks	Physical Layer	Tampering attack	Accessing the WSN node physically and data is extracting.
			Jamming attack	Attacker interfere on the authorize radio frequencies
		The data link layer	Exhaustion attack	Non-stop collision attack on the resource's of the network to consume all its energy until all the node are dead.
Service integrity	Denial of services attacks	The data link layer	Collision attack	Different node transmission running on the same frequencies range then collision arises.
Service integrity		The data link layer	Unfairness attack	Trying to acces the data link layer through unauthorized ways .
		Network and routing layer	Selective Forwarding attack	Select the specific path and a node which drop the data packets during transmission

	Denial of services attacks		Replayed routing information attack, Spoofed	WSN's traffic block or attack by altered during sensor exchanged information
	Denial of services attacks	Network and routing layer	Black Hole attack	Specific selective route to attack in the form of malicious or compromised node where they can drop data packets
Availability	Denial of services attacks	Network and routing layer	Sybil attack	A node change itself to different identities of the network node to behave like them for gaining the data access for the attacker
Availability		Network and routing layer	Acknowledgement Spoofing attack	False information spreading through the acknowledgement of message between the attacking node and the node in neighbor.
Availability		Transport layer	Desynchronization attack	Direction set to end host for spoofing message frequently yet the request is send for retransmission of loss data packets

This table 3 summarized the possible attacks and their description related to different layer attacks and what kind of security requirements they don't fulfill.

7. Security Solutions in Wireless sensor network

To achieve security at various layers in wireless sensor network we can apply security mechanism, but due to heterogeneous nature of WSN it's difficult to achieve. Some researchers are doing improvements in WSN protocols in node design but others are interested in resolving security issues. Security mechanism requires high computation power and memory that are limitation in WSN. Protocols are defined as set of rules followed during interaction between peer processor. Some of important security protocols are discussed below which provide solution against threats and attacks that will fulfill the security requirements in WSN[3].

7.1 SPINS: Sensor protocol for information via Negotiation

Optimized security protocol for sensor network and it has two secure structure blocks: SNEAP and µTESLA.SNEAP provide data confidentiality, authentication for two parties and details of data freshness while µTELSA Include authenticated broadcast of resource controlled environments [4].

SNEAP: Sensor network encryption protocol
It uses counter mode CTR like other cryptographic algorithm but neglect counter value when transmitting packet at both ends. it use only 8 bit added per message and has low communication transparency .SNEAP attain

Semantic security that prevents from different security attacks like eavesdropping. It provides replay protection, Data authentication and weak message freshness[9]. But when we send data over radio frequency channel it need more energy for transmission, but SNEAP use cryptographic schemes that help to achieve semantic security by reducing the transmission energy. It also uses message authentication code (MAC) and CTR for data authentication and integrity [4].

µTELSA: Authentication Broadcast
TELSA (time efficient Stream Loss-Tolerant authentication) was used for data authentication and it uses Asymmetric digital signature that is not practical for wireless sensor network because it require high communication power about 50-1000 which violate the limitation in WSN. Adrian Perrig et al, proposed UTELSA micro and earlier version of TELSA to handle these limitations in sensor network [7]. It uses only symmetric key mechanism, provide authentication with digital signature of first data packet which get expensive for WSN. It get expensive to accumulate one way key used in sensor node this node store the packet in buffer and known to be that MAC key is open or known by base station that's the reason UTELSA limit the user for authentication and has synchronization problem. There is one limitation in UTELSA is that before sending the broadcast some early information must be send to every node before authentication and much node synchronization is a challenge [8].

7.2 TINYSEC

It is a link layer security protocol for WSN and it is replacement with SNEAP protocol main difference is its doesn't use counter in their encryption schemes, hence it doesn't guarantee the data freshness and by rejecting counter mode it use block cipher with particular operations.[2] .it provides security services like confidentiality, authentication, Integrity and access control. It is very lightweight protocol. For confidentiality, encryption is made by using CBC (cipher block chaining) with cipher text stealing mode (CTS) that means cipher text and plain text are of same size and for authentication, it uses CBC-MAC.for variable message size message tinysec XOR the first plaintext block with encryption of message length to achieve more security.[10] It follows symmetric key mechanism as sender and receiver both share the same key to calculate MAC. It has two security options or packet formats which is Tinysec-Auth for authenticated message and Tinysec-AE for encrypted message. For Tinysec-AE, uses packet header of 8 bit with combination of 29 bytes payload.MAC is calculated on both payload and header that provide encryption of packet. In tinysec-Auth packet header is 4 byte long and packet payload is also 29 bytes.MAC computations apply on payload and header but data payload is not encrypted. Hence security of CBS-MAC is depends on length of MAC[30].

In CBC initialization vector (IV) used for get semantic security in which some variation occurs in message during encryption process. Same IV must be used by receiver to decrypt the message that is not covert as well like private key.

7.3 MINISEC

It is a network layer security protocol and consumes low energy than Tinysec. Security level almost equal to the zigbee security protocol .most important about this protocol is it use offset codebook (OCB) mode with block cipher mode of operations that offer authenticated encryption, with one pass over message. advantage by using OCB is that plaintext and cipher both has same length and adding of 4 bits in Tinysec case get discarded so CTS cipher text stealing is not necessary in this case. It has less synchronization problem and provides a security against reply attack. It has two modes of operations one is Unicast and other is for broadcast. Which one will be used depends on scenario.

7.4 LEAP

Localized Encryption and Authentication Protocol is management protocol for SN that provide strong and efficient security mechanism, after observing different kind of message transmission which require different security. It has important a point like it is lightweight, robustness, energy efficient and survivability operations and as well as provide confidentiality and authentication. It supports data aggregation that's uses inside networking that result in low energy consumption. LEAP provide establishment of (4) four different types of keys for each node recognized as individual, pair wise ,cluster and group key. All these 4 keys are symmetric shows as given[3]:

Individual key: this is special key shared by both base station and node for secure communication that basically provide confidentiality.

Pair wise key: this key is shared by other sensor nodes or between nodes.

Cluster Key: this key used for locally broadcast communication in very secure manner and it is mutual between node and all surrounding neighbor's nodes.

Group Key: it is joint by all base station and whole sensor nodes in the network globally. Provides confidentiality and used for mostly query base events.

LEAP is profoundly used to protect against security attacks like Wormhole Attack ,HELLO Floods Attack, Sybil Attack and. it provide authentication between nodes and packets are authenticated hop by hop[7].

7.5 ZIGBEE

Zigbee is wireless communication technology works on network layer just above PHY and MAC layer operate on IEEE802.15.4 standard. It is used in different application such as home automation, military security and environment monitoring. It used to provide data integration and data confidentiality and it uses 128 bit key for security mechanism. It is just like "trust center" provide authentication for requesting nodes to join the network and distribute the key.[7] It uses (3) three network devices; 1.Zigbee coordinator which start the communication, 2 stores information and different networks bridges, 3. Zigbee router provide link between different device and multi hop communication. zigbee mostly uses in end devices to collect data from one component and communicate with other component or node. Zigbee coordinator as a trust center performs different roles:

Trust Manager: it authenticates the request of nodes/devices to join the network.

Network Manager: it distributes the key to other devices in the network and maintains its secure connection.

Configure Manager: it assure end to end secure connection and organize security mechanism.

It works in commercial and residential mode. Commercial mode is used for commercial application which requires high security require high cost and operational mode is used for normal real life residential applications which require less security this is less expensive to implement. It uses different types of keys employees, master key, Link key and Master key [11].

Master key: As name show it installed first in the base or out of the group. It provides long term security between two devices and this key sent by trust center.
Link Key: provide the security between two devices
Network key: it gives security across the entire NS both network and link key implement (SKKE) symmetrical key, key swap handshake between devices or nodes. This key is derived from trust center [14] .
These operations done in commercial mode are not suitable for residential mode, because it doesn't allow authentication. Open source zigbee security features not implemented completely but commercially its implemented and provide full security features. In commercial mode, security added easily by inserting 3 bits in security layer subfields is set. The security level identifies '111' for encryption with 16 bytes MAC and '000' for no security. Latency and power control of zigbee is under investigation. [9]

7.6 IEEE 802.15.4

IEEE 802.15.2 is a standard protocol implemented on MAC/link layer by providing security mechanism. It has three mode for operations secured, unsecured and Access control list. Secured mode fulfills four security requirements 1) Access control 2) frame integrity 3) sequential freshness 4) data encryption. And name shows unsecured mode doesn't implement any security mechanism.ACL mode hold the list of devices that try to communicate and this also doesn't contain cryptography security so the message address can be spoofed. [4]Secured mode implements different security suits that are using AES advanced encryption standards and symmetric cryptography, operate in different mode 1) counter mode CTR 2) (CBC-MAC) with message authentication mode 3) Authenticate and encrypt block cipher mode almost all handle data integrity with different length (32, 64, 128). All security suits implement on radio chip because all cryptographic computation done on hardware that reduce energy consumption. Almost all security implementation done at upper levels that support type of key and authentication policies.[3] Despite all these securities some attacks also occurred that are tampering and jamming attacks which cause DOS and man in the middle attack. Additional security mechanism can be provided against jamming attack at IEEE 802.15.4e with channel hopping. Encryption done only MAC payload, an intruder can attack in IEEE 802.15.4 packet header that can affect the whole network. If any change in the packet for example if there any change in frame counter , security mechanism find the frame integrity broken then frame will be rejected but it consume energy[12]. If these security suits implement successfully provide strong basics for high and fully featured security [11][27].

7.7 LLSP: Link Layer Security Protocol

This protocol implement on link layer that is energy efficient and can minimize the energy consumption by considering the security requirements. It consumes less energy as compared to Tinysec. LLSP provides message confidentiality, replay protection, message authentication and access control. It has low performance transparency that's supports early rejection of attacks. It has disadvantage that provide low scalability so adding new node in large network or maintaining node get difficult. LLSP uses two schemes AES and CBC (cipher block chaining).[9] To get the authentication and access control message get encrypt with MAC and CBC which ensures that coming or receiving message is error free. LLSP preserve 4 byte synchronous counter between user and receiver that always get updated by FSR (feedback shift register). By using the FSR user can get records of all message then receiver can detect any attack and discard it and FSR also help in energy consumption by adding counter with each packet message. Security in LLSP depends on MAC length its 4 bytes its mean intruder need to attempt 2^{32} options to get the original MAC code.[13] Tinysec require more time to transmit the data than LLSP has low overhead and less energy consumption than Tinysec by using security mechanism to fulfill security requirements[27].

7.8 LISP: Light weight Security protocol

It name shows that it balance the consumption of power, energy and also implement light weight security mechanism that provide strong support key renewability. It enhances the scalability, energy efficiency and security by reuse the shared key stream reuse. It supports key distribution in WSN that make it reliable. [2]It doesn't involve in retransmission of packets that's the reason it is vigorous against DOS attack. It supports transmission of new key, that change time to time which is managed by (KS) key server provides encryption and decryption after broadcast of every new key. When key get received by client it authenticated, recover list all missing keys also. It is useful for those large scale network where resource are major concern because it is light weight, work at low processing speed, require low energy for computation and use less resources[27]. It works best in distributed SN that divide the whole network into cluster and group head (GH) that mange the whole network that GH hold server key [3].

7.9 LEDS: Location Aware end-to-end Security

This protocol provides location awareness by implementing security mechanism as addition and encryption done by unique key which is shared by event sensing node and base station. It provide end to end authentication inter routing capability to handle different kind of attacks for insertion of data.[5] It support location alert key management and it can use in both type of

network small and large as number of cells increases key numbers also increases respectively. It doesn't support multiple topologies, divide the whole network into different cell regions to sense the event of corresponding region, that event should be sensed by different sensor node in that regions. LEDS handle selective forwarding attack; node capturing attack and report disrupting attack behalf of this it assure data availability. [6]It provide report generating mechanism as we know wireless devices uses for broadcast communication so it assured report authentication process by send data between different node in next hope separately[27]. No chances of report disappearance due to single node. LEDS provide very high security authentication, data confidentiality without taking into consideration cost for communication and computation [10].

7.10 RPL: - Routing Protocol for Low power and Lossy network

RPL is a distance vector routing protocol that supports different technologies work on data link layer (IEEE 802.15.4, ISA100).RPL implement on routing or network layer in WSN which provide integrity, confidentiality, availability and non repudiation. It has 3 security modes of operations

Unsecured mode: name shows it provides no security mechanism for routing but supports other different mechanism and support link layer security.

Preinstalled mode: it use preconfigured symmetric key by providing integrity data confidentiality and authentication that bases on encrypted message. Any node may connect RPL network by a node which can be a host or a router.

Authenticated mode: those nodes who has predefined symmetric key may link the network as a host only. Node fist take key from authority node then use this key for authentication and authorization by passing message between two various adjacent nodes[11].

Beyond the measurement any one of RPL mode is not implemented till now this makes RPL make viral for security attacks. wallgren et al. introduces light weight heartbeat protocol this is combine with IPSec to sense selective forwarding attack. This attack also tackled by other techniques such as data replication and random routes[12]. Hello Food not remains for longer time inside RPL network because of its self curing mechanism. Other different combination of security mechanism can be used to prevent different attack at network layer or routing layer like clone ID and Sybil attack can be prevented by knowing the geographical location of nodes.

7.11 COAP: Constrained Application Protocol

It implements on application layer in WSN and developed for web transfer used in IOT same like HTTP used in different applications. Directly it has no security features itself but researchers adds (DTLS) datagram transport layer security to secure CAOP messages and also handle unpredictable nature of UDP. DTLS assure confidentiality, integrity, authentication and nonrepudation and it provides 4 modes of security operations.

NoSEc: mean no security DTLS doesn't use at this mode.

***PreSharedKey*:-** DTLS provide list of pre distributed symmetric keys and those nodes have same keys knows as part of group

***RawPublicKey*:-**DTLS uses pair of Asymmetric keys in this mode that is installed on node during making phase give high security mechanism.

Certificate: it is enhanced form of rawpublickey mode. It provides the combination of symmetric and asymmetric key and provides certification authority. Only those nodes can send data who verify the certificate[12].

DTLS has 2 layers one is bottom layer which support "symmetric key encryption" and upper layer provide "hand shake" mechanism that establish secure setting and session key. Main disadvantage is this doesn't provide multicast communication which is necessary in WSN environment. Handshake is not also reliable due to its message exchange complexity and it achieves high cost. It provides protection against reply attack[12]. We use DTLS as a COAP which has many lacking with rest to security requirements

Table 4: comaprison of different security protocl

Security Protocol	Security Requirements	Security Attacks Protected	Strengths	Overhead bytes	MAC used	Key Arrangements	Limitations
SPINS	• confidentiality • Authentication • Integrity • Freshness	• Eavesdropping • Spoofing • Message replay attack	Semantic security and Low communication overhead	8	yes	Symmetric Delayed	Data inaccessible cannot guard against OS

TINY SEC	• confidentiality • Authentication • Integrity • Freshness	• Spoofing • Message replay attack	Energy efficient and low memory usage	4	Yes	any	Resource consumption on attack node
MINI SEC	• confidentiality • Authentication • Freshness	• Spoofing message replay attack	High security at low consumption	4,3	Yes	any	Lack of data integrity
LEAP	• confidentiality • Authentication	• Hello Flood attack • Sybil Attack • Wormhole attack • Reduce Selective • Sink hole • Forward attack	Supports communication patterns, in-networking processing	variable	Yes	Pre_developed	Sink node doesn't compromise
Zigbee	• Authentication • Integrity • Freshness	• Sybil attack • Wormhole attack • Sink hole	Scalable and energy efficient	4,8,16	Yes	Trust center	High security at high power consumption
IEE 802.15.4	• Access control • Authentication. • Frame integrity. • Sequential. • freshness	• Reactive Jamming • Tempering • Eavesdropping	Have high security suits CTR,CCM and ,CBC-MAC.	4,8,16	yes	any	Jamming technique offered DOS attack. Use limited channels for communication.
LLSP	• Authentication • Confidentiality • Access control	• Protection against replay attack	Semantic security, less transmission time and energy consumption	4	Yes	NO	Low scalability so don't support data availability
LISP	• confidentiality • Authentication • Integrity • Access control • Availability	• Dos Attack • Malicious node attack • Replay attack	Used for large scale and energy efficient	8	Yes	Key server (reuse every time)	Require IDS for better security
LEDS	• confidentiality • Authentication • Availability	• Prevent node capture • DOS Attack • Selective forwarding attack	Location aware end to end and provide security Highly robust Dos against	variable	yes	Location alert (any)	Doesn't support multi technology
RPL	• Confidentiality	• Sinkhole • Selective	Support multiple	4	Yes	Any	No practical implementation

	• Integrity • Authentication • Nonrepudation	forwarding • Spoofing • Sybil Attack • Wormhole, rank Attack	topologies(point to point, multipoint to point) maintenance .Self healing nature				took places, more prone to internal attacks
COAP	• Confidentiality • Integrity • Authentication • Nonrepudation	• Dos attack replay attack • Exhaustion attack	Work with DTLS provide high security	4,8	Yes	Any	Multicast communication

8. Conclusion:

WSN facing challenges for designing the WSN security architecture concerned about security threats and security protocol implementation. This paper purposes different security requirements, security threats at each layer and theirs countermeasures attack categorization with information of network and attackers at different layer. Give description of some security protocols that fulfill which security requirements, their strengths, weakness, MAC used and key arrangements. Provide protection against some relevant attack at different layers. This research will help to choose which security protocol implement in what application.

9. References:

[1] Sharma, Ritu, Yogesh Chaba, and Yudhvir Singh. "Analysis of security protocols in wireless sensor network." *Int. J. Advanced Networking and Applications* 2.03 (2010): 707-713.

[2] Salehi, S. Ahmad, et al. "Security in wireless sensor networks: Issues and challanges." *2013 IEEE International Conference on Space Science and Communication (IconSpace)*. IEEE, 2013.

[3] Ndia, John G. "A Survey of Security Protocols for Wireless Sensor Networks." (2017).

[4] Zhou, Yun, Yuguang Fang, and Yanchao Zhang. "Securing wireless sensor networks: a survey." *IEEE Communications Surveys & Tutorials* 10.3 (2008): 6-28.

[5] Boyle, David, and Thomas Newe. "Securing Wireless Sensor Networks: Security Architectures." *J. Networks* 3.1 (2008): 65-77.

[6] Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." *2006 8th International Conference Advanced Communication Technology*. Vol. 2. IEEE, 2006.

[7] Grover, Jitender, and Shikha Sharma. "Security issues in wireless sensor network—a review." *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. IEEE, 2016.

[8] Sinha, Preeti, et al. "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey." *2017 International Conference on Signal Processing and Communication (ICSPC)*. IEEE, 2017.

[9] Zia, Tanveer, and Albert Zomaya. "Security issues in wireless sensor networks." *2006 International Conference on Systems and Networks Communications (ICSNC'06)*. IEEE, 2006.

[10] Bhasin, Vandana, et al. "Security architectures in wireless sensor network." *International Journal of Information Technology* 12.1 (2020): 261-272.

[11] Patel, Punyaban, Bibekananda Jena, and Sateesh Nagavarapu. "Wireless Sensor Networks: Architecture, Issues and Research Challenges."

[12] Tomić, Ivana, and Julie A. McCann. "A survey of potential security issues in existing wireless sensor network protocols." *IEEE Internet of Things Journal* 4.6 (2017): 1910-1923.

[13] Modares, Hero, Rosli Salleh, and Amirhossein Moravejosharieh. "Overview of security issues in wireless sensor networks." *2011 Third International Conference on Computational Intelligence, Modelling & Simulation*. IEEE, 2011.

[14] Chelli K. Security issues in wireless sensor networks: Attacks and countermeasures. InProceedings of the World Congress on Engineering 2015 Jul 1 (Vol. 1, No. 20).

[15] Sharma K, Ghose MK. Wireless sensor networks: An overview on its security threats. IJCA, Special

Issue on “Mobile Ad-hoc Networks” MANETs. 2010:42-5.

[16] Sarma HK, Kar A. Security threats in wireless sensor networks. InProceedings 40th Annual 2006 International Carnahan Conference on Security Technology 2006 Oct 16 (pp. 243-251). IEEE.

[19] *Telecommunication, Electronic and Computer Engineering (JTEC)* 10.1-7 (2018): 17-21.

[20] Boyle, David, and Thomas Newe. "Securing Wireless Sensor Networks: Security Architectures." *J. Networks* 3.1 (2008): 65-77.

[21] Bhushan, Bharat, and Gadadhar Sahoo. "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks." *WirelessPersonal Communications* 98.2 (2018): 2037-2077.

[22] Zou, Yulong, et al. "A survey on wireless security: Technical challenges, recent advances, and future trends." *Proceedings of the IEEE* 104.9 (2016): 1727-176.

[23] Sabeel, Ulya, and Saima Maqbool. "Categorized security threats in the wireless sensor networks: Countermeasures and security management schemes." *International Journal of Computer Applications* 64.16 (2013).

[24] Radhappa, Harish, et al. "Practical overview of security issues in wireless sensor network applications." *International journal of computers and applications* 40.4 (2018): 202-213.

[25] Sinha, Preeti, et al. "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model:

[17] Sastry AS, Sulthana S, Vagdevi S. Security threats in wireless sensor networks in each layer. International Journal of Advanced Networking and Applications. 2013;4(4):1657.

[18] M. A., et al. "A review on security challenges and features in wireless sensor networks: IoTBurhanuddin perspective." *Journal of* A survey." *2017 International Conference on Signal Processing and Communication (ICSPC)*. IEEE, 2017.

[26] Portocarrero, Jesús MT, et al. "Autonomic wireless sensor networks: a systematic literature review." *Journal of Sensors* 2014 (2014).

[27] Ahmed, Abu Shohel. "An evaluation of security protocols on wireless sensor network." *TKK T-110.5190 Seminar on Internetworking*. 2009.

[28] Zhu, Sencun, Sanjeev Setia, and Sushil Jajodia. "LEAP+ Efficient security mechanisms for large-scale distributed sensor networks." *ACM Transactions on Sensor Networks (TOSN)* 2.4 (2006): 500-528.

[29] Park, Taejoon, and Kang G. Shin. "LiSP: A lightweight security protocol for wireless sensor networks." *ACM Transactions on Embedded Computing Systems (TECS)* 3.3 (2004): 634-660.

[30] Karlof, Chris, Naveen Sastry, and David Wagner. "TinySec: a link layer security architecture for wireless sensor networks." *Proceedings of the 2nd international conference on Embedded networked sensor systems*. 2004.