A Survey on Wireless Sensor Network Security

Dhruv Haribhakti
Information Systems Engineering
Concordia University
Montreal, Canada
dhruvharibhakti7@gmail.com

Mahima Shukla
Information Systems Engineering
Concordia University
Montreal, Canada
mahimashukla.0707@gmail.com

Aashika Lakhani
Information Systems Engineering
Concordia University
Montreal, Canada
aashika9266@gmail.com

Venkatesh Galla
Information Systems Engineering
Concordia University
Montreal, Canada
venkateshgalla005@gmail.com

Akshayaa Venkatesan
Information Systems Engineering
Concordia University
Montreal, Canada
akshayaa.venkatesan@gmail.com

***Abstract*—Sensors have been an old concept of devices used to measure and detect events. Sensors can be wired as well as wireless. Wireless Sensor Network (WSN) usually consists of Sensing devices, a Base station and Internet. All the devices are monitored over a dashboard with the help of a mobile or web application. In this paper, we have surveyed about the background of the WSNs and their vulnerabilities. This paper further focuses on the defence methods that can be used to detect, mitigate or prevent all the cyber-attacks on or through WSNs.**

***Index Terms*—WSN, ZigBee, WiFi, AES-128, IDS, Virtual Gateway**

I. Introduction

The Internet of Things (IoT) has evolved to a very high standard with the developments of a large number of applications across almost all the available fields. One of the most important and useful was the Smart Home and Industrial Automation. It is a huge turn of events for Home Area Networks and Automation. The evolution of the Wireless Sensor Network (WSN) has brought the ease and comfort for the people to use almost all the devices just sitting remotely from their cell phones. The Wireless Sensor Network consists of wireless devices which may include sensors, actuators, a physical or virtual gateway, and a base station and all connected to the internet. They are responsible for collecting data from sensors and sending it to the base station for processing and storage.

There are three main components in Wireless Sensor Networks as given in [12]:

- Sensor node: The sensor's responsibility in a physical environment is to monitor a predetermined physical measure. The network has several nodes with sensing and communication capabilities. A sensor is a tiny component that is incorporated into a chip utilizing the SoC (System on Chip) technology, and it only has a few capabilities and resources.
- Base Station (BS): The component that consolidate the information transmitted by various network sensors intended to be relayed and reported at the supervision console in a network that is more intelligent. Therefore, it can be a point of aggregation in a dense WSN (density of sensors). This network sensor's element has physical and logical capabilities higher than sensor devices.
- Medium RF: The wireless infrastructure that categorizes WSNs. It is the Radio frequency transmission.

A. Problem Statement

Given where the sensors are located, finding an uninterrupted power source for these tasks is difficult. Making sure that power use is efficient is one technique to solve this issue is important. When it comes to the constraints of sensors, a number of other factors need to be taken into account in addition to the power consumption [11]. They are all discussed below.

a) Network security threats: The sensors are prone to a variety of attacks because they are positioned at remote locations. The currently used traditional security measures are not thought to be appropriate for WSN systems. This is mostly due to the fact that WSN systems are typically distinguished by their restricted power, processing, and communicating capabilities, necessitating the usage of specific protocols and solutions in order to maintain the system stability and security simultaneously. Another suggestion utilising PEGASIS will reduce this distance even more.

b) Data collection: Efficacy has two main problems in the domain of wireless sensor networks, particularly in the data collection phase. The first problem is that having communication problems will result in considerable energy loss because of the great distance. Between the sensor nodes and the distant base station, this might occur. Dealing with delays in the data collection process is the second problem. Both of those issues must be solved at the same time because they are inversely proportional to one another. For this, a cluster head node-based approach to launch a data gathering structure has been developed. Its use will reduce the amount of time the data collection takes.Additionally, by building cluster heads and reducing the number of sensor nodes, the distance

between the cluster head nodes and the base station will be shortened.

c) Deployment Techniques: It has become an emerging and largely applicable technology due to demand, advancement in technology, and simplicity of deployment of Wireless Sensor networks. With WSN, it is much more practical to monitor real-time phenomena at a much wider scale and with the highest degree of accuracy. Additionally, the deployment of WSN in remote areas has benefited other related scientific fields.

d) Coverage Problems: The issue of wireless sensor network coverage has been the focus of numerous research projects. The placement of the nodes is one of the major problems with this puzzle. It becomes challenging to detect and monitor the object since sensor nodes may be scattered and put randomly in the field [31].

e) Network Architecture: The WSN's main flaw stems from the network architecture's poor design. Unauthorized access to crucial data is likely to result from poor design. In order to ensure the security of an information system, the architecture is crucial. This necessitates careful study of the network blocks throughout the design phase. Another crucial query is what the server's main objective is.

B. Types of Sensors

Sensors are a crucial part of a network. It senses physical change in the model or any application by measuring and processing the gathered information. There are different types of sensors, ranging in complexity from extremely simple to very complex. The specification, conversion method, material employed, physical phenomenon sensed, characteristics of what is being measured, and application field can all be used to classify sensors [10]. Fig.1 shows various IoT sensor types, which are described below.

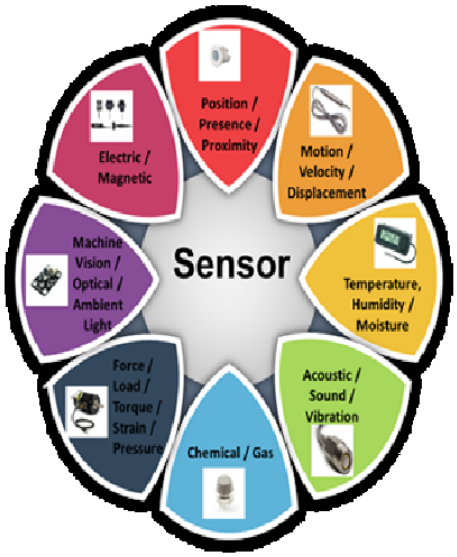

Fig. 1. Different types of Sensors [10]

a) Proximity Sensors: With a proximity/position/presence sensor, any adjacent object may be easily located without making direct physical touch. It detects the existence of an object by simply looking for any fluctuation in the return signal after emitting electromagnetic radiation, such as infrared.

b) Motion Sensors: A motion sensor is an instrument used to detect all kinetic and physical movement in the environment. Motion sensors can be used by an application to monitor residences while the owner is away, and if motion is detected, pictures or videos can be uploaded to the server.

c) Velocity Sensors: It is a sensor that determines the rate of change in position readings and continuous position measurements at predetermined intervals. Velocity sensors are of two types: Angular and/or linear.

d) Temperature Sensors: By sensing heat energy, temperature sensors are useful for identifying physical changes in the body.

e) Pressure Sensors: Pressure sensors measure the force and transform it into signals.

f) Chemical Sensors: An analytical tool used to determine the chemical composition of the environment is a chemical sensor.

g) Humidity Sensors: A humidity sensor determines the environment's relative humidity by measuring the temperature and moisture content of the air.

h) Water Quality Sensors: water quality sensors are employed for Ion monitoring and using that to calculate the quality of the water.

i) Infrared Sensors: To sense various characteristics of specific objects, infrared sensors may emit or detect infrared radiation. They are also used to measure if any heat emission occurs.

II. Protocols and Topology

A. Communication Protocols

In paper [13], the authors have given insight on different kinds of wireless protocols such as Bluetooth (IEEE 802.15.1), ZigBee (IEEE 802.15.4), Wi-Fi (Wireless Fidelity) (IEEE 802.11), and Z-Wave (proprietary-based standard).

a) Bluetooth: Bluetooth is a wireless radio technology that belongs to the IEEE 802.15.1 standard, which was first introduced by Ericsson. The "cordless computer", which consists of several devices such as PCs, laptops, mice, keyboards, scanners, and printers, is the most popular application for Bluetooth. Each of them has a Bluetooth card and may connect wirelessly. It utilizes Wireless Personal Area Network, a personal network application, and it enables short range (WPAN). The maximum number of nodes in a Bluetooth network with a master is eight, and its operating frequency range is 2400 to 2483.5 MHz. Line of Sight (LoS) range is 10 meters, and it enables data speeds up to 1 Mbps.

b) ZigBee: ZigBee protocol is an IEEE standard 802.15.4 that is low-power, low-cost, and low-data-rate wireless personal area network that is specifically developed and implemented for smart home applications. ZigBee Alliance

is responsible for maintaining this standard (a group of companies). It supports star, mesh and cluster tree network topologies. A coordinator or router, also known as a Full Function Device (FFD), and an end device, also known as a Reduced Function Device (RFD), are the two different types of devices that make up a ZigBee network. For the high-level secure transfer of data, ZigBee offers security features like AES encryption, and no security option is also offered.

c) WiFi: The most widely used wireless network that belongs to IEEE Standard 802.11n/a/b/g for Wireless Local Area Network is Wireless Fidelity (Wi-Fi) (WLAN). When connected to an Access Point (AP) or in ad hoc mode, users are permitted to browse the Internet and connect to the cloud at their broadband speeds (supplied by the network vendor). Access points (Routers) and wireless stations are connected during infrastructure configuration. Each wireless station in the Base Service Set (BSS) (Access Points + Wireless Stations) connects to the Internet via its corresponding access point. One Service Set ID (SSID) serves as the unique identifier for each BSS. Wi-Fi offers many levels of protection, with the highest-level being Wi-Fi Protected Access 2 (WPA2) 802.11i, which also has no security feature (open network). Wi-Fi's high data rate results in a greater power usage (116 mA). Wi-Fi offers a good range indoors and out, with a LoS of up to 100 meters.

d) Z-Wave: It is an Internet of Things protocol intended for remote management of residential appliances and small-scale industrial applications. It features a constant speed of up to 40 kbps, a LoS range of 30 m, and indoor reduction potential. It is 128-bit AES encrypted for security and avoids interfering with other popular protocols like Wi-Fi, Bluetooth, and other systems. Z-Wave is a proprietary standard protocol that can be used to create networks with controller and slave device types. Slave nodes are unable to originate communications and only respond to and carry out commands given to them by controlling devices and inexpensive devices. The shape of an end device or a slave device can vary depending on its functioning. Mesh network topology is supported by Z-Wave. The Z-Wave network is always under the overall control of one controller. The maximum number of devices supported is 232.

B. Routing Protocols

A wireless sensor network is made up of self-organizing protocols and algorithms. Communication and data transmission between nodes require routing protocols. For WSNs, numerous routing protocols have been put out. Based on network structure, protocols can be categorized into the following groups: data-centric protocols, hierarchical protocols, location-based protocols, and QoS aware protocols as described by Anjali et al., in [14]. These are tabulated in Table I.

a) Data-centric protocols: Protocols which are used to transfer data from sensors at the source to those at the sink. The data is requested in the form of queries, so it is called query based. They employ the idea of designating desirable data to cut down on unnecessary transmissions, which leads to energy saving. Some of the examples are Directed diffusion, Gradient Based Routing, COUGAR.

b) Hierarchical protocols: This technique divides the network into clusters, with a cluster head in each. A cluster head (a special node, CH) is used to gather the data from the nodes of that specific cluster once clusters are generated from groups of various nodes. A data aggregation task is carried out using this protocol, which is energy efficient. Some of the examples are Low Energy Adaptive Clustering Hierarchy, PEGASIS, SOP.

c) Location-based protocols: Instead of sending the data across the entire network, protocols send it to the appropriate areas. For the transfer of data, it makes use of location data. Nodes are frequently required by these protocols to share coordinate information with their neighbors. Signals from the GPS (Global Positioning System) can provide location data. By figuring out how far apart two nodes are, an ideal path can be created using position data. Some of the examples are GEAR, Geographic Adaptive Fidelity.

d) QoS aware protocols: Quality of service (QoS) is a crucial condition for WSN routing protocols. QoS is very important in some applications, such as the military. Data delivery ratio, dependability, traffic load, and energy consumption are the primary factors considered in QoS-based routing systems. The routing protocols must minimize delays, maximize reliability, reduce traffic loads, and consume the least amount of energy to provide acceptable quality of service. Some of the examples Sequential Assignment Routing, SPEED.

TABLE I
CLASSIFICATION OF ROUTING PROTOCOLS [14]

Classification	Routing Protocols
Data Centric	SPIN: (Sensor Protocols for Information via Negotiation)
	DD: (Directed Diffusion)
	RR: (Rumor Routing)
	GBR: (Gradient Based Routing)
	CADR: (Constrained Anisotropic Diffusion Routing)
	COUGAR
	ACQUIRE: (ACtive Query forwarding in sensor networks)
Hierarchical	LEACH: (Low Energy Adaptive Clustering Hierarchy)
	TEEN and APTEEN: ([Adaptive] Threshold sensitive Energy Efficient sensor Network)
	PEGASIS: (the Power-Efficient GAthering in Sensor Information System)
	SOP: (Self Organizing Protocol)
Location-Based	GAF: (Geographic Adaptive Fidelity)
	GEAR: (Geographic and Energy Aware Routing)
QoS Aware	SAR: (Sequential Assignment Routing)
	SPEED (Stateless Real Time Routing Protocol)

C. Topology

There are some basic topologies that the Wireless Sensor Networks (WSNs) usually follow as discussed by Singh et al.,

in [1]. They are depicted in Fig. 2 and as follows:

- Point to Point Topology: A central hub is not required in this design. A sensor node can speak with other nodes directly. There is only one channel in this architecture, which is quite common.
- Star Network Topology: In contrast to point-to-point topology, a star network needs a central hub for communications. There is no direct contact between the nodes in this structure.
- Tree Topology: This topology combines the topologies of a star network with a point-to-point network. The parent node is the term for the primary hub. From the parent sensor node to the leaf sensor node, data is exchanged. This topology's key advantage is that it uses less power than other network architectures.
- Mesh Topology: Data can move from one node to another in the mesh structure. Without utilising a centralised communication hub, all nodes can communicate with one another directly.

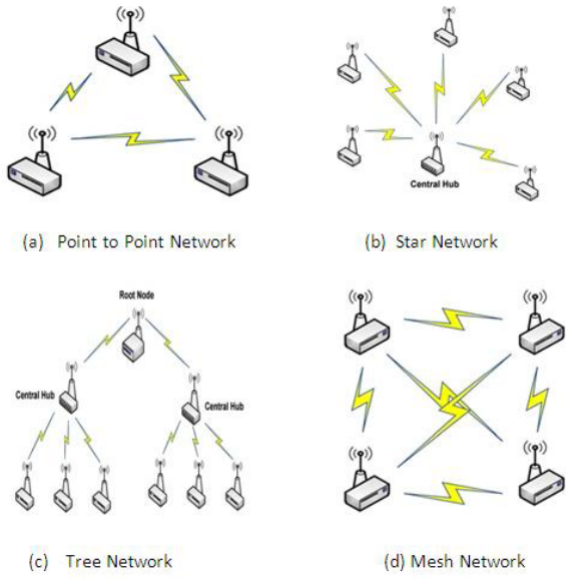

Fig. 2. Topologies of WSN [1]

The wireless sensor networks have relatively low reliability and security since they are typically set up in the field, have limited processing and storage capabilities, and use open wireless communication. When designing and developing sensor networks, it is essential to use the best localization technologies, increase the sensor's energy efficiency, implement security settings, and guarantee network security in order to enhance overall performance [2].

a) Energy Efficiency: When constructing wireless sensor networks, energy efficiency is a top concern because most sensors are field devices. The three components of information sensing, data transfer, and data processing are where the majority of the energy used by sensor circuits is expended.

b) Node localization: A wireless sensor network's localization system needs to be reasonably environment-adaptable. It can effectively execute calculation and localisation regardless of how the environment changes.

c) Data fusion: Due to the high relevance and repetition of the data collected by nearby sensor nodes, the sensor network would produce a lot of redundant data as well as use a lot of energy and bandwidth. The amount of data that needs to be transmitted will be significantly reduced if the collected data are first centralised, screened, and processed, which is known as data fusion, and then the finished data are transmitted to the terminal through the Internet, thereby saving energy and bandwidth, lowering network load, and lengthening network life.

d) Network security: Information is transferred through the Internet between sensor nodes and terminals, however this lacks reliability and security because field-installed nodes could be attacked by animals and insects. Security must therefore be addressed in wireless sensor networks as a key problem.

Keeping all these constraints in mind Shetty at al., in [3] have discussed 3 basic classifications in the topologies of the WSNs.

1) Cluster Based Topology: The technique of clustering separates datasets into groups called clusters, making sure that every element in a cluster is of the same type. Each cluster has a "cluster head" who negotiates data transfers between the nodes. LEACH (Low Energy Adaptive Clustering Hierarchy) and HEED (Hybrid Energy Efficient Distributed Approach) are used in a few protocols that fall under the cluster-based topology.

A number of distributed cluster-based routing protocols exist, including LEACH. It entails choosing a cluster head, which is based on a threshold, which is a sensor-chosen random integer between "0" and "1". If a certain node reaches the threshold, it is chosen as the cluster head. LEACH aims to evenly spread the energy load among several other nodes.

The network is filled with the node's remaining energy thanks to the HEED protocol. It is similar to LEACH, but there is a variation in the cluster head selection, which depends on the residual energy of the node and the distance to other nodes. Every node other than the cluster head determines its likelihood of becoming the cluster head at the beginning of each cycle. HEED protocol extends the network's life span compared to LEACH. It succeeds in producing a consistently dispersed group of cluster heads. As a result, communication costs are reduced. The primary purpose of the cluster head is to bundle and restrict the data before sending it to the sink, also known as the base station.

2) Chain Based Topology: The deployment of sensor nodes forms a transmission chain that links them. By doing this, energy loss during data transport is prevented. The nodes communicate with one another through a chain. Up until it reaches the leader, data is sent gradually from one node to the next, with the successor then sending the data it receives from its predecessor along the path to the sink. The leader compiles

all incoming data before sending it to the sink node.
PEGASIS (Power Efficient Data Gathering Protocol For Sensor Information Systems) is the protocol that used to implement the chain topology. Sensing the data, receiving the data from the forerunner, fusing the received data with that of the node, and delivering the fused data to the following node are the main operations carried out. Data aggregation is achieved by the network's fusion of data packets from various sensors travelling to the base station in order to reduce the quantity and size of data transmissions. In turn, the sensors' energy is conserved. Only the closest neighbours of the nodes need to be talked with in order to extend the network's range. The nodes communicate with the base station alternately. Once every node has completed their turn, a new round begins. Therefore, the power consumption is distributed equally among all the nodes.

3) Tree Based Topology: The sensor nodes are placed in the shape of a tree in this topology. The data is summarised at the intermediate nodes and forwarded to the root node as a short representation. This approach is appropriate for in-network aggregation applications like radiation monitoring in nuclear power plants, where the highest value yields the most insightful information about the plant's security. One of the key goals of the tree-based network is to construct an energy-efficient data aggregation tree. Two techniques used in tree-based topology are briefly discussed in this subdivision.
An aggregation tree is created using the effective, energy-conscious distributed heuristic known as EADAT (Energy Aware Data-Aggregation Tree). According to this protocol, the sink sends a message with the identifier msg, which is a control message with the following five fields: ID, parent, power, status, and hopCnt. These fields represent the ID of the sensor, its parent in the aggregation tree, its remaining power, and its current condition in the tree. The sink s broadcasts a message. Sink, the aggregation tree's root, is thought to hold an endless supply of power. A sensor v that is tuned into the channel sets its timer to TV when it receives a message for the first time. Only when the channel is idle does the television's count decrease. During this procedure, v records the node with the most remaining power and shortest path to the sink as its parent. The message and the hopCntv are broadcast by v when the timer Tv expires. Any node s that learns that node v is its parent by receiving a message designates itself as a non-leaf node. An aggregation tree with roots in the sink is the result of this operation.
PEDAP (Power Efficient Data gathering and Aggregation Protocol) protocol implies that the base station already knows where every node in the system is located. This protocol creates a minimal spanning tree, which creates a system that uses the least amount of energy. Base station uses the provided cost model to calculate the remaining energy levels of the nodes based on the amount of energy each node uses in a round. After a predetermined number of rounds, it then recomputes the routing information, excluding the dead nodes. The required data, such as each node's parent in the tree, the time slot number during which the node should send its data to the parent, etc., are sent to each node by the base station after the computation. The total cost of operating each node's receiving circuitry plus the cost of constructing the system using fresh routing information.

III. Security Features

A. Security Objectives

The vulnerabilities and risks that can be used against electronic information are used to set the security goals for that information. While a vulnerability refers to the potential for harm due to a logical design or implementation defect, a threat is when an attacker attempts to identify and take advantage of the vulnerability to do harm [8]. The following are some crucial security requirements for WSN security that are frequently used to gauge how well different secured systems perform in comparison to one another as described by Islam et al., in [8]:

1) Confidentiality: To maintain confidentiality, information must not be disclosed to uninvited parties, people, or systems. By prohibiting unauthorized parties from accessing the data generated, such as domain-specific information, such as the user identification, positions, and other related information conveyed in the network, confidentiality secures the network. In other words, a confidential message shouldn't be accessible to eavesdroppers by which he can extract the content.

2) Integrity: Integrity refers to prevention of unauthorized individuals or systems from falsifying or altering data that is delivered over a network. This goal involves network-based defense against information modification via message insertion, replay, and delay. Integrity violations can affect safety concerns because altered or misleading data can cause control systems and infrastructure to malfunction, including lighting, heating, and hydro systems as well as communications and security systems.

3) Authentication: For many applications in sensor networks, message authentication is essential. Numerous administrative tasks necessitate authentication (e.g., network reprogramming or controlling sensor node duty cycle). Since an adversary can easily insert messages into a sensor network, the receiver needs to be certain that the information utilized in any decision-making comes from a reliable source. Legitimate nodes should be able to recognize messages from unauthorized nodes, and data authentication stops unlawful parties from using the network [9].

4) Availability: The concept of availability refers to making sure that authorised users can access system resources without being blocked by unauthorised systems or people. When referring to automation systems, this includes all of the IT components found in a typical house, such as control, security, utility, and entertainment systems, as well as the communication networks that link them to one another and to the outside world. It simply means that the availability of services guarantees that only authorised organisations can access data, services, and other readily available resources when asked. Denial-of-service (DoS), or a breach of availability, may not only result in financial losses but may also have an impact on

security and put people's lives in danger because there may be circumstances (such as heart attacks or breathing problems) when prompt and decisive action is required.

5) Freshness: Freshness refers to freshness of both data and the key. It is important to make sure that any data generated or measured by the system is recent and that no adversary-made old messages are present. This is crucial in the context of the smart home environment because sensors frequently detect and send time-sensitive data, such as a person's blood pressure and heart rate, at specific periods that are more significant than others and should be handled in real-time to ensure the safety of lives.

B. Secret Key Management

Confidentiality, integrity and authentication are some of the important security objectives in WSN and can be achieved with the help of key management. However, due to the ad hoc nature, intermittent connectivity, and resource limitations of the sensor network environment, key distribution is a difficult task.

The foundation of conventional key management services is a certificate authority (CA), a trustworthy entity that issues every node's public key certificate. Reliable CA is necessary to enable public key infrastructure that is frequently online and supports renewal and revocation. But establishing a sensor's key management service utilizing a single CA network is risky. The solitary CA will represent the weak link in the system. If a CA is compromised, the entire network goes down so setting up a trusted key management service is critical. To solve this issue, we have some key management schemes [22].

- Hybrid key-based protocols: For all topologies, densities, sizes, and circumstances of sensor networks, a single keying protocol won't be the best option. Until the network's routing infrastructure is sufficiently well-established, protocols like Identity-Based Symmetric Keying and Rich Uncle have limited utility. Other protocols, such pairwise keying and public-key groups, use too much energy when used alone. A combination of public key-based protocols, such as pairwise, group keying, and distribution keying, offers greater energy efficiency for large sensor networks than utilizing a single protocol.
- Threshold cryptography: Here, there is a set of special server nodes that generate partial certificate using a threshold scheme to distribute the services of a certificate authority. These partial certificates combined give a valid certificate. However, this scheme is not very suitable for WSN as for ad hoc networks.
- Certificate repository: The authors proposed a scheme where each node must store its own certificate repository. The public certificates that the nodes themselves issue and a certain set of certificates issued by the other nodes are stored in these repositories. Performance is determined by the likelihood that any node, using only the two users' local certificate repositories, can obtain and validate any other user's public key.
- Fully Distributed Certificate Authority: To distribute an RSA certificate signing key to every node in the network, it employs a (k, n) threshold approach. Additionally, it employs proactive and verifiable secret sharing procedures to guard against denial-of-service attacks and key compromises for certificate signing. There is no requirement to elect or select any specialized server nodes because the service is distributed among all nodes when they join the network.

C. Cryptographic Techniques

Cryptography can be divided into 3 kinds of techniques as described in [11]:

1) Symmetric technique: In this technique, data is encrypted and decrypted between nodes using a single secret key. The key is kept secret within the network. Symmetric key cryptography is divided into two parts: Block and stream cipher. Compared to block ciphers, stream cipher approaches are more vulnerable to attacks.

2) Asymmetric technique: In the technique, there are two keys used: Private key (used for decryption) and public key (used for encryption). Only the private key should be kept secret inside the network. The key size is larger than the symmetric cryptography, and so it requires more memory and energy.

3) Hybrid technique: This technique is a mixture of both techniques. It takes advantages from both and is designed to consume less memory and lower power consumption.

D. Encryption Algorithms

There isn't a standardized security system that can guarantee complete protection for WSN. Furthermore, because WSNs are used in a variety of application areas with varying levels of security needs, providing such a system is not practical. Designing a secure WSN requires accurate mapping of security mechanisms or solutions with various security factors. For WSN security research, this also provides a hurdle. We anticipate that as wireless sensor networks spread and become more widespread, additional security standards will be expected of the apps utilizing them [6].Following are different encryption algorithms used/proposed in different papers to secure communication in WSN.

1) AES (Advanced Encrypted Standard) algorithm: In [**?**], the authors have described AES (Advanced Encryption Standard) encryption, that has been applied to provide the necessary degrees of security for maintaining the privacy of the data in the WSN network.

AES is an iterated block cipher which takes initial block and cipher key as input which goes through several rounds of transformation before the output is generated. A State is the name given to each intermediate cypher outcome. Round keys are a collection of specially derived keys used in the encryption process. On an array of data that contains exactly one block of data that needs to be encrypted, these are applied along with other operations. We refer to this array as the state array [6].

The encryption and decryption process of AES is shown in Fig. 3. The State is a two-dimensional 4 X 4 square matrix array of bytes that represents the plaintext or the 128-bit block input of the encryption. The order of the bytes in the square matrix for both the plaintext and the key is sequenced by column. The key is also written as a square matrix of bytes. The encryption comprises of SubBytes, ShiftRows, MixColumns, and AddRoundKey as its four phases. The AddRoundKey phase starts the cypher off, and then there are nine rounds with all four stages before the final round without the MixColumn phase [7].

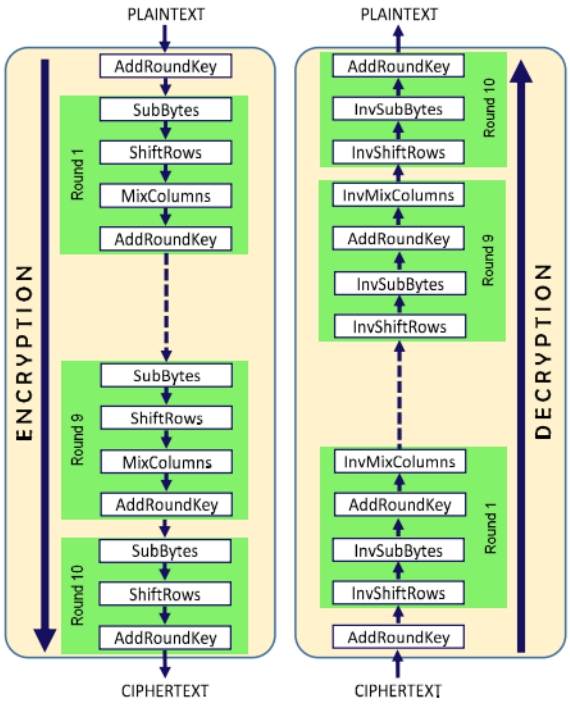

Fig. 1. AES cipher function.

Fig. 3. AES Cipher Function [7]

The four phases are described below as discussed by Acla et al., in [7]:

- SubBytes Phase: SubBytes, also known as a substitute byte transformation, replaces each byte in a block using a substitution box called an S-Box.
- ShiftRows: ShiftRows transformation is a simple permutation done by performing a byte circular left shift on last three rows of the matrix.
- MixColumns: MixColumns transformation is an individual linear diffusion method that works on each state matrix column.
- AddRoundKey: AddRoundKey transformation is a simple XOR performed on the state matrix and the round key.

The data can be saved in databases securely by utilising this approach. Even if hackers somehow crack the entire database, they can only see the encrypted versions of the data. The attacker cannot get the records unless he is aware of the precise Key length.

2) A low complexity security algorithm: In paper [4], the authors have proposed a low complexity security algorithm for WSN that provides data confidentiality. The proposed security algorithm has basically five steps as shown in Fig. 4. It begins with the deployment of WSN, following with encryption of data at N nodes. The model consists of a base station and N number of sensor nodes. The data is encrypted at each node and then forwarded to the next node and finally to the base station. Third step is to transmit the data from nodes to base station. Then in the next phase the data is decrypted at the base station and is matched to the original data, if matched then accepted otherwise discarded. Last step is to solve errors if any encountered. This security protocol proposed provides strong security and low complexity by protecting it against various attacks.

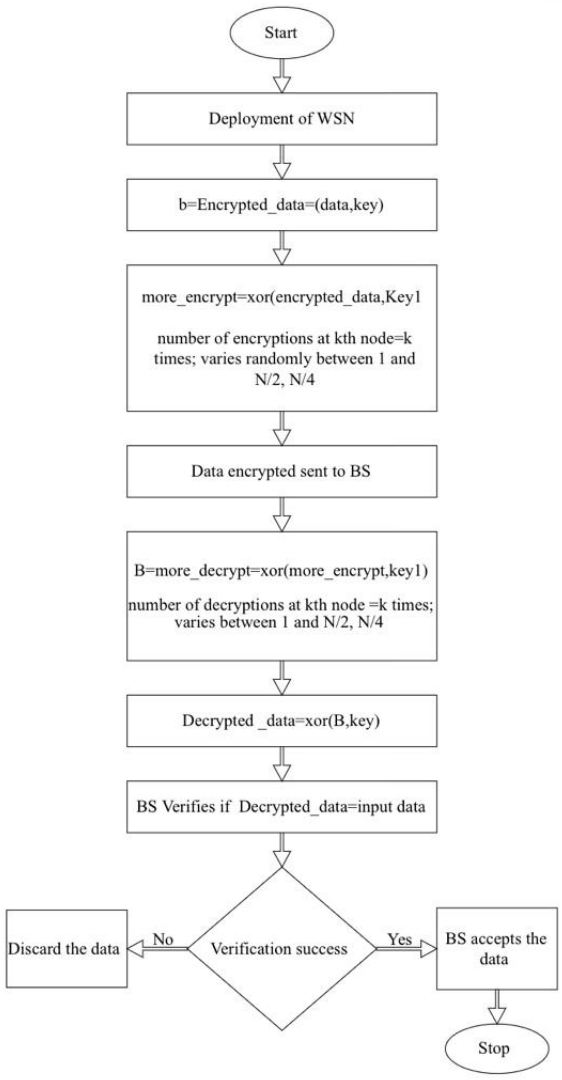

Fig. 4. Proposed Security Algorithm [4]

3) A new chaotic encryption algorithm: According to authors in paper [5], The authors of this research suggest developing an S-box-based chaotic encryption technique for wireless sensor networks (WSN). Additionally, they described it in their paper and made comparisons to the other proposed methods. Utilizing the TinyOS operating system, which enables the management of the WSN's resources, the evaluations and measurements of the suggested algorithm tests are performed. Additionally, they demonstrated how the suggested algorithm might work with AS-XM1000 sensors. The suggested approach is adaptable; in fact, the suggested encryption technique can be used to encrypt messages of any size, including those as large as pictures. The authors demonstrated how their suggested solution and three additional methods—KLEIN, LBlock, and Hammungbird—could be implemented on the TinyOS operating system. The applications: KLEIN and the suggested algorithm are best suited to the WSN, according to the energy tests and occupancy tests in ROM and RAM described in their study.

IV. Attacks on WSN

The attacks can mainly be classified into Active and Passive Attacks. The classification is given in the Fig. 5.

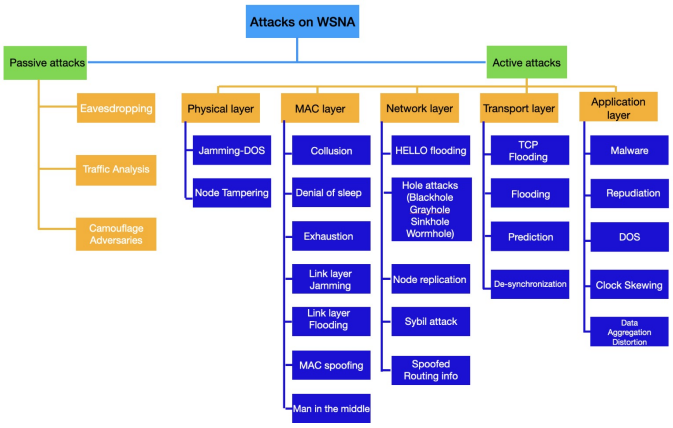

Fig. 5. Types of Attacks

A. Passive Attacks

Passive attacks are carried out in such a way that they cannot be detected by any means. This is since the attackers emit no radio waves. It is easier for an attacker to get unauthorised access to a communication. The most frequent passive attack is eavesdropping, which may be easily conducted by listening to wireless communication between sensor nodes in the WSN without recording any of them and ensuring that the message is not altered or destroyed [15]. The primary goals of a passive assault are to steal sensitive information, compromise privacy standards, and degrade performance. Passive assaults are mostly targeting data secrecy, and they are defined as unauthorized invaders monitoring communication lines. These attacks have no effect on communication because the attackers are merely listeners, but they represent the preliminary stage of all active attacks. The following are the most common Passive Attacks:

a) Monitoring And Eavesdropping: Passive information gathering is another term for eavesdropping. Communication lines can be tapped to intercept classified data. As a result, wireless networks are more vulnerable to passive attacks. Because WSNs employ short-range communications, an attacker must be nearby to gain useful information by eavesdropping, and hence WSNs are less vulnerable to tapping than long-range wireless technologies. Interception of WSN messages may expose the following useful information: physical location of certain nodes such as cluster leaders, gateways, key distribution centres, and so on, message identities (IDs), timestamps, other fields, and basically everything that is not encrypted [15].

b) Traffic Analysis: For attackers, a network's traffic pattern may be as useful as the substance of data packets. Analyzing traffic patterns can provide valuable information about the networking structure. In WSNs, the sink nodes produce more transmissions than the other nodes because they relay more packets than the nodes farther from the base station. Similarly, clustering is a key scalability strategy in WSNs, and cluster heads are busier than other network nodes. Adversaries may find detection of the base station, nearby nodes, or cluster heads particularly useful since a denial-of-service attack against these nodes or eavesdropping on packets headed for them may have a higher impact. This type of vital information can be obtained by analysing traffic. Furthermore, traffic patterns can reveal sensitive information such as activities and intentions. Silence in tactical communications might signify the preparation for an attack, a tactical move, or infiltration. Similarly, an abrupt spike in traffic rate could indicate the start of a planned invasion or raid [15].

c) Camouflage Adversaries: An adversary or attacker compromises a sensor node in a wireless sensor network in this case. This hijacked node, also known as a WSN camouflage node, is used to disguise the remainder of the WSN's conventional sensor nodes. The camouflage node then publishes a false advertisement regarding the routing information, causing packets from other nodes to be routed through the compromised node. When packets are received, they are routed to a strategic node where privacy evaluations of packets are performed routinely [16].

B. Active Attacks

Active attacks compromise not just data confidentiality, but also integrity of data. Active attacks can also be used to gain unauthorized access to and use of resources, or to disrupt an opponent's communications, such as putting error files into the system, packet alteration, modification, unlawful access, or overcrowding the sensor network. An active attacker emits a radio signal or performs an action that the WSN elements detect. Active assaults include interfering with system functionality, removing some sensor nodes from the network, data tampering, denial of service, and overall system performance deterioration. Active attacks are classified into five major categories using the OSI stack protocol layered structure, as

shown in the figure. The physical, datalink or medium access control (MAC), network, transport, and application layers of a WSN network structure can be represented by a 5-layer OSI model. It should be noted that the classic OSI network model's Session and Presentation levels are all considered in the WSN Application layer [15].

1) Physical Layer Attacks:

a) Jamming: A malicious device can jam a communication by emitting at the same frequency as the signal. The jamming signal adds to the noise in the carrier, and its strength is sufficient to lower the signal-to-noise ratio below the level required for the nodes utilising that channel to receive data correctly. Jamming can occur continually in a region, disrupting the entire network or a segment of the network and causing data transmission delays. Jamming can also be done briefly at random time intervals, which can still effectively disrupt transmissions [15]. If a jamming assault is detected, the sensor nodes go into sleep mode and periodically wake up to investigate the channel, however this does not prevent DoS attacks; it just increases sensor node lifespan by lowering power consumption.

b) Node Tampering: The attacker obtains physical control of the sensor node by attaching cables to its circuit board and reading stored data, as well as continuing transmission in the WSN. Furthermore, by tampering, attackers can change the original wiring of the electronic board or the content of the nodes' memory and utilize the seized slave node in any way. The main goal is to capture sensitive information, particularly revealing cryptography-related keys, which may compromise the entire WSN [15]. In this instance, two issues arise:

- The captured node can perform arbitrary searches on the attacker's behalf (DoS attack against availability).
- A captured node may provide bogus data to legitimate users (attack against integrity).
- The attack is prevented by periodically changing the key and implementing adequate key management techniques.

2) MAC Layer Attacks:

a) Collision: When a legal network node begins transmitting, the attacker broadcasts data on the same frequency channel. As a result, two packets from two different sensor nodes collide, causing an error since the received data cannot be interpreted by the receiver. The recipient eventually requests re-transmission of the same packet. A single byte of a message colliding would result in a CRC (Cyclic Redundancy Check) error, rendering the entire message unusable. For an attacker, this technique is more advantageous than jamming because it consumes less transmission energy and has a lower risk of detection [15].

b) Denial Of Sleep (Sleep Deprivation Torture): Denial of sleep attack will result in energy depletion for battery-powered devices. This attack is carried out by conducting collision assaults or repetitive handshaking, i.e., repeatedly altering request to send (RTS) and clear to send (CTS) flow control signals, preventing the node from entering the sleep phase [15].

c) Exhaustion: The exhaustion attack is carried out by continuing collusion assault (disrupting the channel by continually sending requests) until the targeted node's energy is depleted. This type of assault may be carried out utilizing a standard node or a laptop that can emit radio signals in the same frequency range as the rest of the sensors. As a result, legitimate users are unable to access the channel [15].

d) Link Layer Flooding: In this sort of attack, a hostile node exploits the fairness of medium access by delivering excessive MAC data packets or MAC control packets to surrounding nodes. Finally, affected nodes experience DoS or their batteries run out of juice. This attack may also deplete channel bandwidth resources [15].

e) Link Layer Jamming: The most valuable packets, i.e., data packets, are targeted for jamming in this form of assault. The probability distribution of packet arrival times is obtained and used to packet transmission. This attack has been demonstrated to be effective against the following MAC protocols: B-MAC, L-MAC, and S-MAC [15].

f) Mac Spoofing: By altering the allocated MAC address, an adversary might perform a MAC spoofing attack. Although the MAC address is hardcoded into the NIC card, a rogue node can nevertheless use spoofing to engage in illegal activity [20].

g) Man In The Middle: Man-in-the-middle (MITM) attacks and network injection are other MAC layer attack types. The attacker in an MITM attack sniffs network traffic to get the MAC addresses of the trustworthy nodes. The MITM attacker uses two victims as a relay. Switches, routers, and other networking equipment cannot function due to the network infiltration. All infected networking devices will need to be rebooted or reprogrammed if further compromised components cause the network to become paralysed [20].

3) Network Layer Attacks:

a) Hello Flood: In this technique, an attacker sends out HELLO packets to the whole network, convincing other nodes that it is in their one-hop neighbourhood. A significant number of nodes receiving such a packet presume that it is within the sender's radio range, which may not be the case during this assault. The attack employs HELLO packets as a weapon to persuade WSN sensors. This attack can be launched by a node that sends an extremely powerful Hello packet. When the other nodes transmit their packets to the rogue node, none of them get them [15] [16].

To avoid a Hello flood assault, the nodes must check the bidirectional link to guarantee that they may reach their parent within one hop. A cryptographic approach is used to avoid the hello flood attack. This method employs two sensors as the same secret key. A fresh encryption key is produced during the connection. This assures that only accessible nodes may decrypt and validate the message, preventing the attacker from assaulting the sensor network. The downside of this strategy is that any attacker may impersonate it and then launch assaults [17].

b) Warmhole: A tunnel (out of band fast transmission link) is established between two nodes, which may be used to transport packets more quickly. In this manner, two remote

regions of the network marketed as neighbours to attract nearby traffic. An out-of-band channel allows a malicious node to intercept or receive data packets at one point and send them to another malicious node in another area of the network. The packets are subsequently replayed by the second malicious node. This leads all nodes that can hear the second malicious node's broadcasts to assume that the node that delivered the packets to the first malicious node is their single-hop neighbour and that they are receiving packets straight from it. Packets sent via the standard path arrive at the target node later than those sent via the wormhole and are thus discarded since they have more hops - wormholes are often constructed using quicker channels. Wormholes are extremely difficult to identify and can degrade the performance of numerous network services, including time synchronization, geolocation, and data fusion [15] [17].

DAWWSEN, a proactive routing system based on the development of a hierarchical tree where the base station is the root node and the sensor nodes are the leaf nodes of the tree, is one strategy for overcoming the wormhole assault. DAWWSEN has the advantage of not requiring any geographical information about the sensor nodes [17].

c) Sinkhole: A malicious node can advertise to all its neighbours that it is the best next hop for forwarding packets to its destination. When a node becomes a sinkhole, it becomes the hub for its immediate surroundings and begins accepting all packets destined for the base station. All network traffic is directed to this single node, although in this situation, the sinkhole node does not discard any packets. It hopes to avoid detection by the IDS in this manner [15]. This opens a plethora of possibilities for any further strikes. The term is given to this assault because every network traffic flows through this specific node, which essentially "sinks" any data it receives [17].

Geographic routing systems are one type of protocol that is immune to these assaults. These assaults are tough to repel. Geographic protocols build a topology on demand using just localized interactions and information and without the need for base station initiation [17].

d) Selective Forwarding (Grayhole): It is a type of blackhole attack in which the malicious node behaves more cunningly and drops just the packets that it chooses. In this manner, the attacker intends to go unnoticed by the IDS. Because it is a version of the blackhole assault, this form of attack is also known as "grayhole attack." A rogue node, like sinkhole attacks, subverts the routing protocol by making itself part of many routes, but instead of dropping all packets, selectively drops some while forwarding others to evade discovery. A routing node's primary job is to forward packets. A malicious node, on the other hand, may purposefully discard any packet and forward others. Multi-hop networks are often established on the assumption that the participant sensor nodes will faithfully convey the messages they receive. In a selective-forwarding attack, adversary nodes may refuse to forward messages by simply discarding them and ensuring that these packets are no longer delivered. A malicious node, as an example of this type of attack, acts like a blackhole and refuses to send every packet it receives. However, such an attacker is at danger of the following: Neighbouring nodes will conclude that it has failed and may choose for a different path. When an adversary selectively forwards packets, this is a more subtle type of this attack. An adversary that is interested in suppressing or changing packets coming from a small number of nodes can reliably deliver the remaining traffic while minimizing suspicion of wrongdoing [15].

e) Blackhole: WSN's black hole assault includes two different features. Once the path is modified by stating that it has a route from the source to the destination node, the second node may discard all packets that it receives for forwarding [16]. When the blackhole node is also a sinkhole, this assault is extremely successful. Such an attack combination has the potential to halt all data transit surrounding the blackhole. By monitoring the network, adjusting packet routing, or employing authentication procedures, a black hole attack can be averted.

f) Node Replication: The attacker deliberately targets a sensor node in the network and takes the secret information from the compromised node [15]. After obtaining the secret information, the attacker copies the node and employs the duplicate nodes (Cloned nodes) in the sensor network, where they function similarly to the original node and relay sensitive information to the attacker. The cloned nodes will have valid IDs and keys to connect with other nodes in the operational network. The countermeasure is to create a one-of-a-kind pair-wise key that enables secure communication between neighbours. An attacker may sometimes clone the base station, posing a major danger to WSN [16].

g) Sybil Attack: In a Sybil attack, a single malicious node will appear to be a group of nodes, i.e., the attacker can appear in numerous places at the same time, by generating false identities of nodes placed at the network's edge and sending false information to a node in the network. False information can include node positions, signal intensities, and pretending nodes that do not exist. Public key cryptography can prevent insider attacks, but it is too costly to employ in networks. By conducting a Sybil assault on the sensor network, the outsider attack may be stopped using authentication and encryption mechanisms. The routing protocols in a WSN network has a distinct identity [17].

The strategy for avoiding the Sybil attack is to use identity certificates. Before each deployment, each sensor node is given a unique ID. The server then generates an identity certificate that associates the node's identity with the provided unique information and uploads it into the node. To securely confirm its identification, a node first displays its identity certificate and then demonstrates that it has the related unique information. Several communications must be exchanged during this procedure. The Sybil attack is therefore avoided [17].

h) Spoofed Routing Information: The attacker interrupts network operation by spoofing or impersonating one entity by another and convincing the victim that they are communicating with a different entity. MAC authentication can prevent this

exploit. The faked routing, as well as the attacker's impersonation or spoofing of its own identity as another entity, leads the recipient to assume that communication is with a different entity. The network's usual operation is stopped and disturbed. This attack causes misleading error signals, route changes, and message discarding in the network. Spoofing attacks may be avoided by utilising MAC to produce the secret keys using the same hash algorithms [16].

4) Transport Layer Attacks: TCP flooding, UDP flooding, TCP prediction and de-synchronization attacks are a few of the security threats that UDP and TCP are susceptible to.

a) Flooding: Anytime a protocol needs to keep track of state at either end of a connection, flooding can cause memory depletion. An attacker is free to request new connections periodically until all available resources are used up or a cap is reached. Any more justifiable demands will be declined in either scenario. Ping flooding, also known as a TCP flooding assault, is a transport layer denial-of-service attack in which the attacker bombards the target nodes with multiple ICMP ping queries. Input and output victim buffers are flooded as a result, delaying connection to the destination network [18].
The TCP prediction technique creates the transmitting node's packets and guesses the sequence index. Victims end up receiving fake packets, which damages data integrity. In a UDP flooding attack, many UDP packets are sent, forcing the victim nodes to send a large number of replies to packets in response, rendering the victim nodes unavailable for many legitimate nodes [18].

b) De-Synchronization: De-synchronization is the disruption of an established link. In a de-synchronization attack, a hostile party sends phoney packets with phoney sequence numbers to break up the connection between two nodes. Such an attack can be thwarted by using header or complete packet authentication. The ability of the end hosts to effectively communicate data may be impaired or even prevented by an attacker if the timing is right, causing them to expend energy trying to fix faults that never existed. For instance, an attacker may send fake messages to an end host frequently, forcing the host to ask for the retransmission of missed frames [**?**]. By decreasing the UDP packet response rate, the effects of an attack via UDP flooding can be mitigated. Firewalls can also stop UDP flooding attacks by filtering malicious UDP packets. The point-to-point or end-to-end communication that is enabled by data encryption is one method for ensuring message secrecy in the transport layer. Despite being the most connection-oriented, dependable Internet protocol, TCP does not work well on MANET. Ad hoc transmission control protocol (ATCP), ad hoc transport protocol (ATP), TCP feedback (TCP-F), and TCP explicit failure notification (TCP-ELFN) have all been created, however none of this address the security concerns associated with MANET. Public key cryptography served as the foundation for the Secure Socket Layer (SSL), Transport Layer Security (TLS), and Private Connections Transport (PCT) protocols, which offer secure communications. TLS/SSL offers defence against man-in-the-middle attacks, replay attacks, rollback attacks, and masquerade attacks [18].

5) Application Layer Attacks: The application layer supports several protocols, including FTP for transferring files and HTTP for providing online services and SMTP for email transmission. These protocols are all susceptible to network security intrusions. Attacks on this layer can affect the semantics of the data by manipulating the data since they are aware of the semantics. As a result, apps are given misleading data, which causes inappropriate behaviour. At this layer, an adversary can attempt to use sensor stimuli to overwhelm sensor nodes, leading the sensor network to send massive amounts of communication to the base station. Such an attack uses up network bandwidth and drains node energy [18].

a) Malware: Numerous malicious software, including viruses, worms, spyware, and Trojan horses, attack user applications as well as operating systems, slowing down or even destroying the computer system and network. Malware attack is a type of HTTP attack that intentionally interferes with or intercepts legitimately confidential data. SMTP worms and viruses for email spoofing and password sniffer are examples of SMTP attacks [18].

b) Repudiation: Denial of participation in the communication is referred to as repudiation. A selfish person could refuse to use a credit card to make a purchase or refuse to perform any online transactions as an example of a repudiation attack on a commercial system. Another name for this attack is a clone attack. The WSN is exposed to an unsecure setting where the malicious nodes can create several copies of themselves. The replicated nodes will have valid IDs and keys to communicate with other nodes in the operational network like regular nodes [18].

c) Denial Of Service: When an attacker attempts to overwhelm a node by activating its sensors, a high amount of data traffic is forwarded toward the sink. This is known as sensor overflow. The bandwidth is overloaded by this attack, and node power is wasted. The type of DoS assault known as a "Vampire Attack" uses the sensor nodes' power to totally shut down the network. The AODV routing system uses the additional field known as Bcast id in data packets and the routing database at each node to identify directional antenna threats [21].

d) Clock Skewing: In this attack, the attacker forges the target skew by changing the forwarding packets' date. Every physical component for the Wireless Sensor Network has a different clock skew depending on the application. The sensors that need their functions to be coordinated are the targets of this attack. The assaults are designed to de-synchronize the sensors by broadcasting erroneous timing information [20].

e) Data Aggregation Distortion: Sensors often send collected data back to base stations for processing after it has been gathered. Attackers might purposefully alter the data that is to be aggregated, resulting in altered final aggregation results computed by the base stations. The base stations may respond inappropriately because of having an inaccurate perception of the surroundings being tracked by the sensors. Attacks that target black holes or sinkholes can completely

stop data aggregation. No data can reach the base stations in this case [20].

Application data semantics are used in attacks at the application layer. Therefore, whether data is being used for control, the countermeasures are centred on preserving the integrity and confidentiality of the data. The misbehaviour detection strategies can be used when authentication is not used, for practical reasons, or when data integrity is somehow endangered. The distinctions are in the data that must be evaluated to gather evidence of anomalies. Flooding time synchronisation protocol (FTSP) can thwart clock skew attacks by altering the time synchronisation interval. By adjusting sensor sensitivity and capping the nodes' data-sending pace, DOS attacks can be avoided. This attack can be successfully made less effective by setting bandwidth restrictions and using effective aggregation. Numerous validations are carried out to prevent packets from being delivered in endless loops, which would disable the network and deplete the battery, to defend against the vampire attack. An efficient method to block attackers from deciphering collected data is encryption [18] [20] [21].

V. Defence Mechanisms for WSN

A. Security Solutions for WSNs

1) Secure Data Aggregation: Denial of service attacks are one of the many threats that sensor networks and data aggregation methods face. Data traffic is the most significant issue in networks as data transfer increases. In the data aggregation (or data fusion) process, intermediary nodes referred to as "aggregators" gather the unprocessed information obtained from the sensor nodes, do local processing, and then transmit only the result to the end-user. By basically reducing the amount of data transmitted on the network, this crucial activity increases the network's total lifetime. An adversary can easily inject false data into the network if an aggregator node is compromised. A sensor node being compromised and having fake data injected via it is another potential attack. Without authentication, the attackers may trick the aggregators into sending the base station invalid information. A secure data aggregation process needs integrity, confidentiality, and authentication. Furthermore, in order to identify the compromised sensors, secure data aggregation also needs cooperation from the sensor nodes. Secure data aggregation protocols are of two types:(i) plaintext-based aggregation and (ii) ciphertext-based aggregation [23]. They are visualized in the Fig. 6.

2) Secure Grouping: WSNs have a large number of small nodes that are automated, portable, and small devices. Despite the fact that overall security may also be used, it is crucial that the group members communicate securely between each other since sensor nodes must bind themselves in order to fulfil a specific task. This task requires group key management which causes problems when a node is added to or deleted from the group. Thus, secure protocols for grouping are necessary where more powerful nodes are capable of protecting the nodes [9] [24].

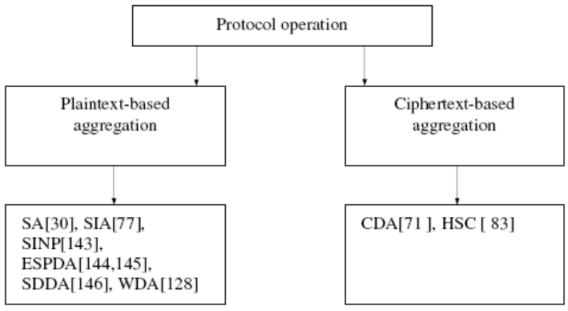

Fig. 6. Secure Data Aggregation in WSNs [23]

B. Intrusion Detection

An Intrusion Detection System (IDS) is used to monitor a network and detect any suspicious activity patterns that are occurring outside the normal behavioural pattern [28]. IDS has three main components as shown in the Fig. 7.

- Monitoring components: Here the nodes are monitored by its neighbors.
- Analysis and detecting components: Network activities and node behaviour are examined in the analysis and detection component, which serves as the key module, in order to determine whether to flag them as malicious or not.
- Alarm components: When the alarm component detects unusual behaviour, an alert is created and delivered to the processing unit.

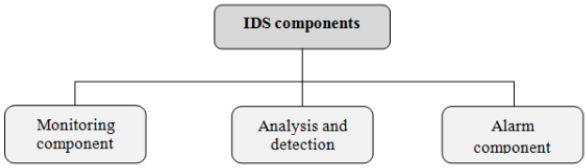

Fig. 7. Components of IDS [29]

An IDS is of two types based on its detection techniques. The comparision between the two are given in the Table II.

a) Signature-based IDS: They are used to detect known patterns of intrusions with the help of known set of signatures or rules. It has a low false alarm rate. These could be located in network packet headers as well as in data sequences that match other harmful patterns or recognised malware. Along with specific data sequences or packet series, an attack signature can also be identified in source or destination network addresses. The known set of rules or signatures are known as indicators of compromise (IOC). While they are limited to identifying known threats, they have high processing speed and greater accuracy. These types of IDS have a low false alarm rate.

b) Anomaly-based IDS: They detect new or unknown intrusions. Anomaly-based IDS uses a node's normal behaviour

and stores it as it's profile and any behaviour apart from that is considered as an anomaly. An anomaly-based IDS has high intrusion detection rate. An anomaly-based IDS will raise a potential flag for concern if it detects anything that does not match the current normalised behavior, such as a user trying to log in outside of normal business hours, new devices being added to a network without authorization, or a flood of new IP addresses trying to connect to a network. The drawback of this is that many benign behaviors will be tagged for being abnormal despite not being malicious. Because anomaly-based intrusion detection is more likely to produce false positives, it may take more time and money to thoroughly look into all of the potential danger alarms. An anomaly-based IDS has high intrusion detection rate.

TABLE II
COMPARISON: SIGNATURE-BASED AND ANOMALY-BASED IDS [29]

Characteristic	signature-based IDS	Anomaly-based IDS
Detection rate	Medium	Medium
False alarm	Medium	Medium
Energy consumption	Low	Low
Suitable to WSN	Yes	Yes
Advantage	Detects accurately all the attacks (known attacks)	Detects new and unknown attacks
Disadvantage	Cannot detect new attacks	Sometimes, introduces a large number of false alarm

The network architecture has a significant impact on how effective and efficient the IDS for WSN is. Based on that, there are three different types of architectures:

- Stand-alone architecture: Here all nodes contribute equally, and each node collects information from the network to detect any intrusions.
- Distributed and cooperative architecture: Here, an intrusion detection agent is placed at each node which detects any intrusions happening and also cooperates with other local agents by exchanging intrusion related data.
- Hierarchical architecture: Multiple clusters are created from the network with a cluster head (CH). CH is in charge of finding malicious activity inside the cluster. It is used in multi-layered WSN. Different criteria are used to categorise different IDS types. IDSs are divided into three categories based on how they are deployed: NIDS, HIDS, and Hybrid IDS.

1) Features of IDS:

- Principles of intrusions detection: There are two approaches: signature-based and anomaly-based IDS.
- Behavior after detection: after the intrusion detection process, the IDS can give an answer in two ways:
  i) passive response, eg: sending an alarm to the administrator
  ii) active response, eg: setting up new filtering rules.
- Data Source: Because they can originate from the network, applications, packets sent and received, or another IDS, the IDSs can be categorised in accordance with the source of their data.
- Architecture: An IDS can be implemented in a decentralized manner or a centralized manner. Also, a hybrid of both is possible.
- Frequency of use: Based on the monitoring approach IDS are of two types
  i) real-time monitoring (online), done in a continuous manner
  ii) periodic monitoring (offline), done periodically.

2) Properties of IDS: IDS must satisfy the following properties.

- Low consumption of resources: The detection task has to be easy and simple as it has limited computation, energy, bandwidth, and memory resources.
- Distributive: to reduce the intrusion detection load, the process should be distributed between various nodes.
- Local Audit (Local Surveillance): An IDS for WSNs must be able to use local and partial data.
- Distrust of other nodes: It is possible to have malicious nodes with monitoring nodes in collaboration. Thus, it is not a good idea to completely trust other nodes.
- Self defense (Security): If an IDS agent is compromised, the system must be capable enough to handle the disruption process.

C. Prevention and Mitigation

a) DoS Attack Prevention: In [25], the authors talk about the preventive measures against DoS attacks and demonstrate the necessity for security enforcement using auction theory. Here, nodes compete against each other in order to gain respect in the network by forwarding incoming packets. The authors also proposed a non-cooperative nonzero-sum two-player game between the adversary and WSN. Nash equilibrium is achieved in this game which works as a defense strategy for the network and such an approach is known as Utility based Dynamic Source Routing (UDSR). The end results demonstrate that by considering each route's utility value and deciding an acceptable threshold for cooperation and reputation of sensor nodes, suspicious nodes can be discovered, and a dependable delivery can be provided.

b) DDoS Attack Prevention using AODV and DSR routing Protocols: DDoS attack is one of the most severe attacks on WSN where it drains the battery capacity in order to disrupt the network. This paper provides a solution to the above-mentioned problem in DSR and AODV protocols. To simulate and assess the effectiveness of the suggested approach for AODV and DSR routing protocols in WSN, Qualnet 5.0 simulator was employed. It also helps to increase the life of a network as the malicious node is detected and shut down [26].

c) Sybil Attack Prevention: To detect and prevent Sybil attack, the authors have proposed a dynamic method with Random Password Comparison (RPC) and Message Authentication and Passing method (MAP). Here, RPC algorithm helps to identify a Sybil node which prevents data leakage. This

allows the network to continue transmission of data. While the MAP reduces time consumption and increases network throughput [27].

d) Sinkhole and Wormhole Attack Prevention: Having each node use a new symmetric shared key with the base is one potential defence against Wormhole and Sinkhole attacks. To lessen the impact of such attacks, it can be beneficial to design effective routing protocols like multi-path routing. Another option is to use Needham Schroeder-like protocols to create a shared key between nodes and allow them to independently verify each other's identities (perhaps utilising the shared key between a node and the base station) [8].

e) Mitigation technique for Routing Protocols: The most common mitigation technique for routing attacks is AODV. Ad hoc On Demand Distance Vector (AODV) is a routing protocol designed for ad hoc mobile networks. It is an extended version of DSDV [30]. This protocol's best feature is loop-free communication, which solves the Count to Infinity problem. In comparison to other routing protocols, the AODV routing protocol uses comparatively less resources. It can be described as a routing protocol with rapid link establishment, minimal network utilisation, and little processor and memory overhead. AODV consists of two major phases:

- Route Discovery: Here, whenever a node wishes to communicate with another node, it looks for its information in the routing table. Routing table is a logical table which stores the information about all the destination addresses and the next hop addresses of the destination. If the source node is able to find the destination node through the routing table, it starts the communication process, otherwise starts the route discovery process.
  After this, source generates and broadcasts a route request RREQ packet and when the destination nodes receive it, it sends a route reply RREP packet. This makes the communication process easier.

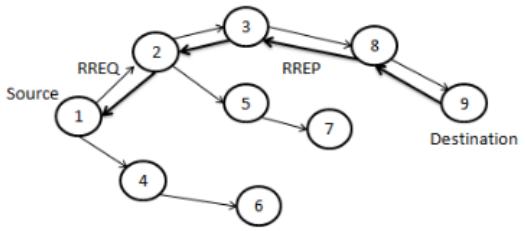

Fig. 8. Route Discovery in AODV [30]

- Route Maintenance: In this second phase of AODV, packet loss due to link failure is reported. A packet loss can happen due to two reasons (i) source nodes moves from its initial position and (ii) destination or intermediate nodes move. If a source node moves, a fresh route discovery is done whereas, if a destination or intermediate node moves, a Route Error Message (RRER) is generated and sent to all the nodes to update in their routing tables.

VI. Future Work

The wireless devices were invented in order to reduce the Human Effort and let go of the complexity of physical wired networks to save space and create damage-proof networks. They manufactures forgot to keep the cyber-security in mind while creating first of their projects. The Hackers saw this as an opportunity to breach into the network quite easily. Later, the security in automating devices became the topmost concern because of the weak security features.
The main problem within the current model is that certain device using the protocols Z-Wave and ZigBee devices need a central hub for the communication within the sensing devices and internet. The Central hub is not aware of the private key of the sensing devices and preforms an initial key exchange while adding the device. The attackers can use sniffing softwares like Wireshark, Ubiqua, NetworkMiner, Fiddler etc. to read the key exchange when the sensor is added to the network. The key is usually encrypted which is to decrypt after replaying a few key exchanges. Also, the signals may sometimes get jammed because of the common frequency used for data exchange. For example, the devices working on WiFi and ZigBee devices may share the common frequency of 2.4GHz.
In one of the recent research by Apostolos Malatras et. al., in [31], a new approach to the current WSN architecture was proposed. The authors defined a network where, for each WSN, one of the gateways takes on the role of the Master Gateway (MGW), and any more gateways are referred to as Secondary Gateways (SGW). Both the MGW and SGWs oversee their assigned sensor nodes, but the MGW also serves as the single point of access to the WSN for external communications and is in charge of coordinating all gateway activities within a zone using a properly specified gateway coordination protocol. They created a new concept of virtual gateways. The device need to strictly use WiFi for the communication for the data transfer. The authentication of the device happens at the virtual gateway's backend. The backend will have the complete list of the whitelisted devices by the manufacturer. So their is no need for any Key exchange between the Gateway and the device as the device is already know to the system.

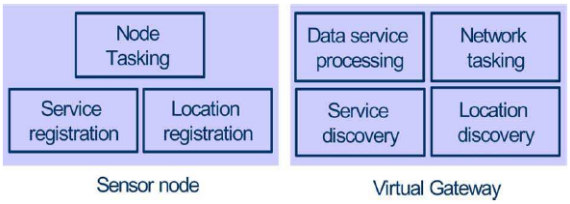

Fig. 9. Tasking functional entities in Sensor node and VGW [31]

An overall SOA for facilities management exposes the WSN service interface. To support the integration of the WSN with enterprise services, the authors have designed a representational state transfer (REST)-based style Service Oriented Architecture (SOA). REST-based Web Services (WS) enable scalable and dynamic resource monitoring since they lack the complexity of SOAP-based WS and constitute an open, flexible framework. It must be made clear that in order for clients to find the WS interfaces, they must be registered to a service registry on a web server. The Virtual Gateway entity implements the actual functionality hidden behind the WS interface. Prior to instructing the WSN to gather data, the necessary processing is carried out at the Virtual Gateway. Between the WSN and the Virtual Gateway, the MGW and SGW entities act as network bridging devices. Fig. 9 depicts a high-level perspective of the functional elements of the tasking middleware. On the functional differences between the two entities, there is a distinction between the sensor node's capabilities and those of the virtual gateway.

REFERENCES

[1] Singh, Manish Kumar, et al. "A Survey of Wireless Sensor Network and Its Types." 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), IEEE, 2018, pp. 326–30. DOI.org (Crossref), https://doi.org/10.1109/ICACCCN.2018.8748710.

[2] You, Guoping, and Yingli Zhu. "Structure and Key Technologies of Wireless Sensor Network." 2020 Cross Strait Radio Science and Wireless Technology Conference (CSRSWTC), IEEE, 2020, pp. 1–2. DOI.org (Crossref), https://doi.org/10.1109/CSRSWTC50769.2020.9372727.

[3] Shetty, Nisha P., et al. "A Comparative Study of Various Protocols in Different Topologies of Wireless Sensor Networks." 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), IEEE, 2017, pp. 1–6. DOI.org (Crossref), https://doi.org/10.1109/ICECCT.2017.8117945.

[4] A. Rani and S. Kumar, "A low complexity security algorithm for wireless sensor networks," 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017, pp. 1-5, doi: 10.1109/IPACT.2017.8244966.

[5] T. Farah and S. Belghith, "A new chaotic encryption algorithm for WSN and implementation with sensors AS-XM1000," 2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2017, pp. 684-689, doi: 10.1109/STA.2017.8314968.

[6] Panda, Madhumita. 'Data Security in Wireless Sensor Networks via AES Algorithm'. 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO), IEEE, 2015, pp. 1–5. DOI.org (Crossref), https://doi.org/10.1109/ISCO.2015.7282377.

[7] H. B. Acla and B. D. Gerardo, "Security Analysis of Lightweight Encryption based on Advanced Encryption Standard for Wireless Sensor Networks," 2019 IEEE 6th International Conference on Engineering Technologies and Applied Sciences (ICETAS), 2019, pp. 1-6, doi: 10.1109/ICETAS48360.2019.9117387.

[8] K. Islam, W. Shen and X. Wang, "Security and privacy considerations for Wireless Sensor Networks in smart home environments," Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2012, pp. 626-633, doi: 10.1109/CSCWD.2012.6221884.

[9] A. Jain, K. Kant and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks," 2012 Second International Conference on Advanced Computing and Communication Technologies, 2012, pp. 430-433, doi: 10.1109/ACCT.2012.102.

[10] Sehrawat, Deepti, and Nasib Singh Gill. 'Smart Sensors: Analysis of Different Types of IoT Sensors'. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, 2019, pp. 523–28. DOI.org (Crossref), https://doi.org/10.1109/ICOEI.2019.8862778.

[11] Pinar, Yasaroglu, et al. 'Wireless Sensor Networks (WSNs)'. 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), IEEE, 2016, pp. 1–8. DOI.org (Crossref), https://doi.org/10.1109/LISAT.2016.7494144.

[12] W. Charfi, M. Masmoudi and F. Derbel, "A layered model for wireless sensor networks," 2009 6th International Multi-Conference on Systems, Signals and Devices, 2009, pp. 1-5, doi: 10.1109/SSD.2009.4956693.

[13] Naidu, Gollu Appala, and Jayendra Kumar. "Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi." Innovations in Electronics and Communication Engineering, edited by H. S. Saini et al., Springer, 2019, pp. 229–39. Springer Link, https://doi.org/10.1007/978-981-13-3765-9.24.

[14] Anjali, et al. 'Wireless Sensor Networks: Routing Protocols and Security Issues'. Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), IEEE, 2014, pp. 1–5. DOI.org (Crossref), https://doi.org/10.1109/ICCCNT.2014.6962992.

[15] Butun, Ismail, Patrik Osterberg, and Houbing Song. "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures." IEEE Communications Surveys and Tutorials 22, no. 1 (2020): 616–44. https://doi.org/10.1109/COMST.2019.2953364.

[16] Keerthika, M., and D. Shanmugapriya. "Wireless Sensor Networks: Active and Passive Attacks - Vulnerabilities and Countermeasures." Global Transitions Proceedings 2, no. 2 (November 2021): 362–67. https://doi.org/10.1016/j.gltp.2021.08.045.

[17] Sampada A, Khorgade, and Namrata D. Ghuse. "Attacks and Preventions in Wireless Sensor Network." International Journal of Engineering Research and General Science 2, no. 2 (April 2015). http://pnrsolution.org/Datacenter/Vol3/Issue2/244.pdf.

[18] 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, pp. 288–93. DOI.org (Crossref), https://doi.org/10.1109/CSPC.2017.8305855.

[19] Mohammadi, S., and Jadidoleslamy, H. (2011). A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks. organization, 4, 21.

[20] Xing, K., Srinivasan, S. S. R., Rivera, M. J., Li, J., and Cheng, X. (2010). Attacks and countermeasures in sensor networks: a survey. In Network security (pp. 251-272). Springer, Boston, MA.

[21] Gavrić, Željko, and Dejan Simić. 'Overview of DOS Attacks on Wireless Sensor Networks and Experimental Results for Simulation of Interference Attacks'. Ingeniería e Investigación, vol. 38, no. 1, Jan. 2018, pp. 130–38. DOI.org (Crossref), https://doi.org/10.15446/ing.investig.v38n1.65453.

[22] Hu, Fei, et al. Secure Wireless Sensor Networks: Problems and Solutions . SYSTEMICS, CYBERNETICS AND INFORMATICS, p. 11.

[23] Sen, Jaydip. A Survey on Wireless Sensor Network Security. International Journal of Communication Networks and Information Security (IJCNIS), Aug. 2009, p. 24.

[24] T. Kavitha, and Sridharan D. Security Vulnerabilities In Wireless Sensor Networks: A Survey. Journal of Information Assurance and Security , 23 June 2009, p. 14.

[25] Agah, A., et al. "Enforcing Security for Prevention of DoS Attack in Wireless Sensor Networks Using Economical Modeling." IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005., IEEE, 2005, pp. 528–35. DOI.org (Crossref), https://doi.org/10.1109/MAHSS.2005.1542840.

[26] Upadhyay, Raksha, et al. "Detection and Prevention of DDOS Attack in WSN for AODV and DSR Using Battery Drain." 2015 International Conference on Computing and Network Communications (CoCoNet), IEEE, 2015, pp. 446–51. DOI.org (Crossref), https://doi.org/10.1109/CoCoNet.2015.7411224.

[27] Wadii, Jlassi, et al. "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks." 2019 IEEE 19th Mediterranean Microwave Symposium (MMS), IEEE, 2019, pp. 1–5. DOI.org (Crossref), https://doi.org/10.1109/MMS48040.2019.9157321.

[28] Farooq, Yumna, et al. "Intrusion Detection System in Wireless Sensor Networks - A Comprehensive Survey." 2019 Second International Conference on Latest Trends in Electrical Engineering and Computing Technologies (INTELLECT), IEEE, 2019, pp. 1–6. DOI.org (Crossref), https://doi.org/10.1109/INTELLECT47034.2019.8954984.

[29] Mekelleche, Fatiha, et al. "Monitoring of Wireless Sensor Networks: Analysis of Intrusion Detection Systems." 2018 5th International Conference on Control, Decision and Information Tech-

nologies (CoDIT), IEEE, 2018, pp. 421–26. DOI.org (Crossref), https://doi.org/10.1109/CoDIT.2018.8394844.

[30] Sharma, Mayank Kumar, and Brijendra Kumar Joshi. "A Mitigation Technique for High Transmission Power Based Wormhole Attack in Wireless Sensor Networks." 2016 International Conference on ICT in Business Industry and Government (ICTBIG), IEEE, 2016, pp. 1–6. DOI.org (Crossref), https://doi.org/10.1109/ICTBIG.2016.7892698.

[31] Malatras, A., et al. "Web Enabled Wireless Sensor Networks for Facilities Management." IEEE Systems Journal, vol. 2, no. 4, Dec. 2008, pp. 500–12. DOI.org (Crossref), https://doi.org/10.1109/JSYST.2008.2007815.