# A HYBRID FAULT-TOLERANT ENERGY MINIMIZATION TECHNIQUES FOR SECURITY ATTACKS IN WIRELESS SENSOR NETWORK

*A Thesis submitted*

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

**DOCTOR OF PHILOSOPHY**
**IN**
**COMPUTER SCIENCE AND ENGINEERING**

by

**Mr. B.Bharathi kannan**
**Reg. No. - 17SCSE301026**

**Supervisor**

**Dr. S.Srinivasan**
Professor

**GALGOTIAS UNIVERSITY**
**UTTAR PRADESH**

**September 2023**

# CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis, entitled "**A HYBRID FAULT-TOLERANT ENERGY MINIMIZATION TECHNIQUES FOR SECURITY ATTACKS IN WIRELESS SENSOR NETWORK**" in fulfillment of the requirements for the award of the degree of Doctor of Philosophy in the department of computer science and engineering and submitted in Galgotias University, Greater Noida is an authentic record of my own work carried out during a period from Aug 2017 to Sep 2023 under the supervision of **Dr. S.SRINIVASAN**

The matter embodied in this thesis has not been submitted by me for the award of any other degree of this or any other University/Institute.

**Mr. B Bharathi kannan**

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

**Dr. S.SRINIVASAN**
Supervisor
School of Computing Science and Engineering

The Ph.D. Viva-Voice examination of ____________________________ Research Scholar, has been held on _________________.

Sign of Supervisor                                        Sign of External Examiner

# ABSTRACT

Ensuring energy efficiency and attack identification in wireless sensor networks (WSNs) is critical due to the limited power resources of the sensor nodes. However, various security threats can compromise energy efficiency in WSNs. The proposed approach for improving energy efficiency by addressing three major security threats: Distributed Denial of Service (DDOS), wormhole attacks, and clone node attacks. Proposed a system for identifying and isolating malicious nodes that launch DDOS attacks, detecting and preventing wormhole attacks by leveraging location information, detecting and isolating clone nodes using a time-synchronization approach. Additionally, propose a node isolation and rerouting approach that enables the network to bypass nodes with low energy levels and reroute data through more energy-efficient nodes. Experiments demonstrate that our suggested strategy effectively boosts energy efficiency while preserving the WSN's security.

The Proposed scheme has two new energy-efficient intrusion detection systems Energy Efficient Intrusion Detection System (EE-IDS) and Energy Efficient Intrusion Detection System with Energy Prediction (EE-IDSEP) are presented to safeguard wireless sensor networks from wormhole and DDOS assaults. In order to improve security against wormhole attacks and reduce the energy consumption of the sensor nodes in wireless sensor networks, the EE-IDS was developed. Ad hoc on-Demand Distance Vector (AODV), Shortcut Tree Routing (STR), and Opportunistic Shortcut Tree Routing (OSTR) are three distinct routing protocols that are used to evaluate the effectiveness of the EE-IDS. Assess and compare the Energy Efficient Trust System for Wormhole detection (EE-TSW) and Energy Efficient Trust System (EE-TS) for detecting DDOS assault using in-depth simulations with NS2. The simulation findings show that the suggested IDS, EE-IDS-AODV, EE-IDS-STR, and EE-IDS-OSTR, perform better for wormhole attack detection than the existing EE-TSW, while the suggested system, EE-IDSEP, performs better for DDOS attack detection than the existing EE-TS with the performance measures of Packet Delivery Ratio (PDR), Average End-to-End Delay, energy use, and detection.

Clustering is a common Hierarchical network management strategy in Wireless Sensor Networks (WSN). Although separate clusters are often desired, several applications of inter-cluster routing, time synchronization, and node location make use of overlapping clusters. In overlapping clusters, replica node discovery is a difficult problem to solve. The first process identifies to reproduce by locating the position using Triangulation and RSSI (Received Signal Strength) methodology, while the secondary process uses RFID (Radio Frequency Identification) for distinctively identifying the item. The effectiveness of Line Chosen Multicast, Randomized Multicast, K-coverage WSN, and Fault Tolerant Virtual Backbone Tree (FTVBT) is compared with non-clustered and Multicast techniques. Due to its deterministic approach, the hybrid bat algorithm with differential equation (BA-DE) exhibits reduced communication overhead, a higher rate of detection, as well as lower storage costs, energy consumption, packet loss, and latency under a variety of scenarios.

The purpose of data collection, sensor nodes should form clusters and congregate. In multi-hop sensor networks, the Base Station (sink) might not be considered. Due to this, the network may experience a hotspot issue. This paper examines the sleep & wakeup approach, which aims to increase packet delivery ratio (PDR) and energy conservation to extend network lifespan and avoid the hot spot (WLAN) issue. In this method, the C-H (cluster-head) is chosen depending on base station distance and energy level. Using this method, to increase energy conservation and improve the PDR compared to Fuzzy Clustering Algorithm (FCA). To identify the source of danger signals, the Fuzzy Misuse Detector Module (FMDM) and the danger detector module collaborate. The Fuzzy Q-learning Vaccination Modules (FQVM), which improve system capabilities, receive the infected sources and transmit them. To create the best defence methods, the Cooperative Decision Making Modules (Co-DMM) integrate the threat detector module and the Fuzzy Q-learning vaccination module.

# ACKNOWLEDGEMENT

First and foremost, I thank the ***Almighty*** for showering his blessings abundantly throughout my research work and for guiding my path.

I wish to extend my deep sense of gratitude and profound thanks to my research supervisor ***Dr. S.Srinivasan,*** Professor, School of Computing Science and Engineering, Galgotias University, Greater Noida for their keen interest, inspiring guidance and constant encouragement to my work during all stages. I also thank ***Dr. Munish Sabharwal,*** Professor & Dean (SCSE), and ***Dr. Alok Katiyar,*** Professor & PhD Coordinator, School of Computing Science and Engineering, Galgotias University, Greater Noida, for their valuable suggestions and support throughout the course of my research work. I am extremely thankful to ***Mr. Suneel Galgotia,*** Chancellor, Galgotias University,a source of inspiration and motivation for me to do this research in a fruitful manner. I am very much thankful to my parents and family members for sacrificing their life for my achievements.

# TABLE OF CONTENTS

4. **LOCALIZATION BASED CLONE NODE DETECTION IN WIRELESS SENSOR NETWORKS**

5. **ENERGY EFFICIENT DDOS ATTACK DETECTION AND DEFENSE APPROACH**

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| MAC | Medium Access Control |
| QoS | Quality of Service |
| LEACH | Low Energy Adaptive Clustering Hierarchical |
| TDMA | Time Division Multiple Access |
| CDMA | Code Division Several Access |
| DDoS | Distributed Denial of Service |
| IDS | Intrusion detection systems |
| EE-IDSEP | Energy Efficient Intrusion Detection System with Energy Prediction |
| EE-IDS | Energy Efficient Intrusion Detection System |
| HMM | Hidden Markov Model |
| AODV | Ad hoc on demand distance vector routing |
| STR | Shortcut Tree Routing |
| OSTR | Opportunistic Shortcut Tree Routing |
| PDR | Packet Delivery Ratio |
| FPR | False Positive Ratio |
| AWC | Adaptive Weighted Clustering |
| RSSI | received signal strength |
| RM | Randomized multicast |
| LSM | Line Selected Multicast |
| FTVBT | Fault Tolerant Virtual Backbone Tree |

|  |  |
|---|---|
| CM | Cluster Member |
| CH | Cluster Head |
| RFID | Radio Frequency Identification |
| RDBRFID | Replica Detection Based on RFID |
| Co-DMM | Cooperative Decision Making Modules |
| FND | First number of sensor node expired |
| LND | Last number of node expired |
| BS | Base Station |
| SW | Sleep and Wake |
| FQL | Fuzzy Q learning |

# LIST OF PUBLICATIONS

## International Journals

1. B.Bharathi kannan. and S.Srinivasan (2022), “The cooperative-based fuzzy artificial immune system using Wireless sensor network”, Indian Journal of Computer Science and Engineering. (SCOPUS)
2. B.Bharathi Kannan and R.Viswanathan (2020), “RPL using MBCO based Efficient Parent Selection for Coverage based Dynamic Trickle Techniques”, International Journal of Advanced Science and Technology. (SCOPUS)
3. B.Bharathi kannan. and S.Srinivasan (2020), Paper Published for “Localization Based Replica Node Detection Technique Using Metaheuristic and Bloom Filter In Cluster Based Wireless Sensor Networks”, International Journal of Advanced Research in Engineering and Technology. (SCOPUS)
4. B.Bharathi kannan. and S.Srinivasan (2023), “Energy Efficient Intrusion Detection System in Wireless Sensor Networks” International Journal Of Computer Engineering and Technology (UGC).
5. B.Bharathi kannan. and S.Srinivasan (2023), “Flexible QoS Path selection for per-Open Flow Data enhancement in Software- Defined Vehicular Network in Wireless Networks” Submitted to Journal of Mobile communication, computation and Information. (SCI - Under review)

## International Conferences

1. Paper Presented the title Cutting edge networking based on multiple attack prevention using advanced wireless sensor networks. International Conference (IPDIMS 2021- Springer - 3rd Series) organized by National Institute of Technology Rourkela.
2. Paper Presented the title Detecting sinkhole attacks in wireless sensor networks via the M optimum routes hopping technique in International Conference On Advancement In Electronic Systems And Communication Technologies by ANIS (2022).
3. Paper Presented the title An Effective Binary Search Tree-Based Clone Detection Technique and Energy Minimization In Wireless Sensor Networks International Conference on Futuristic Digital Technologies for Sustainable Development-Organized by AMET University (2023).

# CHAPTER 1

# WIRELESS SENSOR NETWORKS

## 1.1 Introduction

Small, networked devices that may transmit data wirelessly to one another are known as wireless sensor networks (WSN). Small sensors are known as "nodes" and have a central processing unit, memory, battery, and transmitter for gathering and transmitting data (for receiving and transmitting signals or data among nodes). The ideal cluster size varies depending on the particular use case. It could need to be extremely small in some military and surveillance scenarios, for example Considerations including storage capacity, processing speed, and battery life are all taken into account when setting pricing [1]. Present days, wireless sensor networks are utilized in several different sectors, from the environment and habitat to healthcare and process monitoring, and even surveillance. I'll just provide an example here, wireless sensor networks to monitor a restricted military area. Sensor nodes monitor the environment for occurrences and relay that information to a central location (the sink) in the network.

Although wireless sensor networks are on the rise, the limited battery life of their sensors is a significant challenge. Since each node in wireless sensor network needs energy to function, this has become a significant issue. Even one node fails, the whole system or application is in danger. Each sensor node has the option to be in both active (receiving and sending) and idle (not actively doing anything) states. While a node is actively communicating, it is using power. Although the nodes use about the same amount of power when sleeping as they do when up, this is mitigated by turning off the radio.

The following procedures [2] may help wireless sensor networks save power.

- Scheduled node status is required (Whether sending, receiving, waiting or sleeping).
- To vary the communication separation between sensor nodes,
- Data collection and routing must be done more efficiently.
- One way in which unwanted information might be dealt with is by overhearing.

In WSNs, nodes rely only on their batteries for power. When connecting power is consumed when communicating with other nodes or when carrying out sensing operations is needed for data processing and transfer to the sink. Due to variety of reasons, it's not always necessary to replace dead or low batteries (such as in surveillance applications). The problems with energy efficiency, several researchers are working on power-aware protocols for networks of wireless sensors.

Because Situations wherein Wireless sensor being utilized include timely responses to data detection, processing, and communication are crucial, all WSN protocols must provide real-time support. For a protocol to be considered real-time, it must be able to respond instantly and reliably to changes in the underlying network. It must be able to deliver redundancy data to the central station or sink by aggregating data from every one of the sensors on the network. Data transmission delays between sensor nodes should be minimized for optimal response times.

## 1.2 Problem Statement

This study to learn more about energy-efficient procedures that can support high volumes of real-time communication, as seen in applications such as animal habitat monitoring and community safety. Wireless, battery-powered sensor nodes might be deployed to keep an eye on far-flung spots that humans would have a hard time getting there otherwise. For further action to be taken based on the data acquired by these sensors, the network must do its analysis. The health of a network depends on each sensor node, and each sensor node's power has to be considered.

Although several authors have made isolated contributions to this literature, with an emphasis on identifying which routing protocols are best suited to a certain surveillance application, no extensive study has been conducted on the issue as a whole. These nodes monitor the environment for anything that moves or reacts in any way and record the relevant information. This data is sent using a conventional protocol stack that does not account for network energy efficiency.

The following assumptions provide a basis for further study in the area networked connectivity detector surveillance applications.

- A smart sensor channel's foundation consists of sensing nodes dispersed over a vast area. These sensor nodes are either dispersed throughout a certain area or placed in key areas to monitor for environmental changes, depending on the requirements of the application at hand.

- Users can interact with a central hub (sink) that collects information from distributed devices (anyone who wants to observe the activities). Sensor node many methods can be used to collect information. Including through "hopping" techniques and the delivery of data at certain frequencies. The data transmission and processing capabilities, storage space, and power reserves of sinks are superior to those of sensors. To protect against the possibility of a bottleneck, a network may use more than one drain.
- Much power is wasted whenever nodes in a WSN exchange information with one another. Since surveillance and other mission-critical applications rely on batteries that can't be easily swapped out, saving power is crucial.
- Quality of service may guarantee the timely transmission of messages within a certain window of time. Protocols for distributing traffic should ensure the network's health and convey duplicate data via it. Limiting resources like bandwidth, memory buffer size, and processing power is also crucial.
- The transmission mode is crucial in WSNs. Depending on the network architecture in use, data transmission to other nodes may require a single hop or several hops.
- According on of use case, the sensor networks could be mobile or stationary.
- In surveillance applications, sensor nodes are often deployed in remote places and left unattended.

Ethernet and radio are the two main types of communication protocols when constructing a wireless sensing network, relay data from the nodes to the sink. Protocols for medium access control (MAC) and routing are implemented. Basic communication modes are used to send data periodically or in response to an event at the base station or sink. One additional major category is data retrieval from a particular area or place. These nodes require the ability to broadcast and participate in multicasting (region). Routing protocols not only account for these factors but also others such as power consumption and QoS.

The Data Link Layer's Media Access Control (MAC) surface is a sub-layer. Effective utilization of a communication channel prevents interference among its users. The channel connection and data transmission for the node are facilitated by this. The MAC protocol may impact how well a network performs in terms of energy efficiency, throughput, Quality of Service (QoS), and latency. Transmission, communication, and energy usage are just a few of the criteria that researchers use to determine the best protocols for a given network topology. Analyzing routing protocols and media access control (MAC) protocol varieties may provide light on which protocols are most suitable for surveillance applications concerning energy - efficient as well as immediate needs.

An outline of all the elements that influence networking and MAC protocol operation is given before digging into their internal dynamics. Data like these will help us to evaluate the efficacy of current practices. The efficiency of wireless sensor networks is affected by [3] factors. A node is said to have latency if it must detect or monitor and relay information about the activity. The use case plays a secondary role. Some sensors collect information and send it somewhere else. Network latency takes into consideration the time it takes a sensor to send data, regardless of whether the network is high-volume or low-density. Scalability is essential in wireless sensor networks. The requirements of its users drive the constant evolution of a network's physical space. All network nodes need to be scalable, or able to adapt on their own to shifting network topologies [4].

Energy is required for every function between individual nodes, including sensing, processing, storing, and transmission. Depending on the functionality or activity required for a given task, a network node's energy expenditures might vary from high to moderate to low. The phrase "Node Processing Time" is used to quantify the total amount of time it takes for a network node to perform its many functions. Sensor nodes may use either a flat or a multi-hop routing strategy when transmitting information to the ground station or the sinkhole. Sensor network in a system consumes a certain amount of bandwidth power to carry out network-wide operations including sensing, computation, and grouping. Power consumption in a network is the sum of the energy used by all of the sensors in the system.

## 1.3 Protocols that rely on or do not rely on the existence of a specific agreement

The four most important types of MAC (Medium Access Control) protocols: individuals with the intention of rely on contention with persons that don't. Due to the protocol, several nodes in a contention-based network may share a solitary canal. Even before information can be transferred, every node must first determine the medium. Repeated transmission may be required due to frequent collisions, but Central argument techniques divide the channels into distinct time frames. Every knot receives its share of the data in a staggered fashion and each node is aware of the available time slots in advance, so there are no disruptions in the flow of data. When the data flow and reception are carried out at the same pace, Synchronize among network cells is what happening here in a network, and it happens when the sensor nodes make certain that the information received by the other endpoint can be recognized there at receiver side in the precise sequence that it is supplied. Each node has to share the same concept of time so that it may go to sleep and get up at the correct times. Any information can be sent before two nodes, a "control packet" must first be sent. The control packet includes information such as the amount the quantity of data getting delivered, the destination network node hostname, and a number of indicators to help prevent clashes.

## 1.4 Protocols for WSN Network Routing

Since routing protocols' operation is largely reliant on the kind of network structure used to execute the application or the specific network activities carried out with the aid of these protocols, their implementation in a WSN presents a wealth of options for study. Figure 1.1 shows the classification for protocols also known seeing that a routing taxonomy, used for the classification of routing protocols.

## 1.5 Using a Structured Approach to Routing Protocols

Structure-based routing methods may be further subdivided into three groups: location-based route, hierarchy routing, and flattened routing. The protocols in these groups are effective within the framework of the specified requirements for the network topology or geographic region.

### 1.5.1 Routing in a Plane

The similarity in the roles played by the sensor nodes and the sink, this routing strategy enables data obtained in a far-flung location to be reused or reproduced [7].

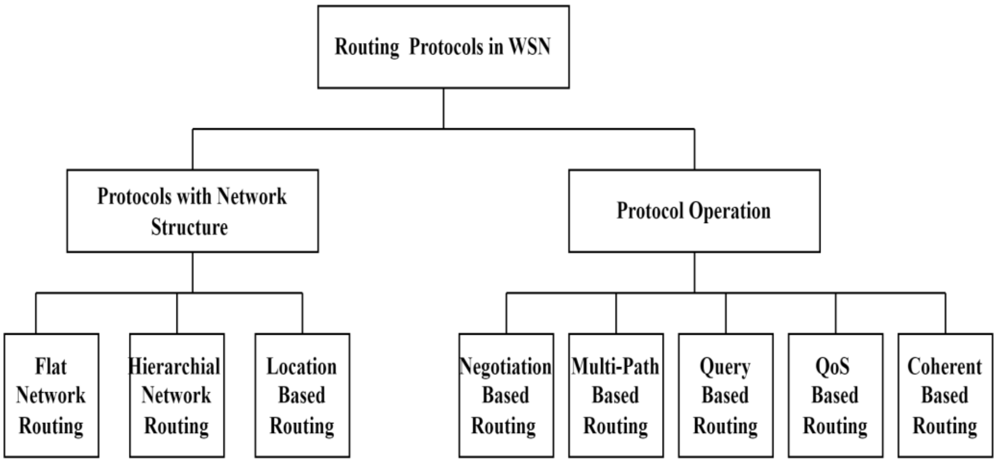


**Figure 1.1: Types of routing protocols**

### 1.5.2 Hierarchical Routing

All network sensors are grouped using this routing scheme, with one node acting as the aggregator and a redundancy checker for all data before it is routed to the sink, because of this lot of effort and time is spared. [7].

### 1.5.3 Navigation Geographic Location

In Navigation Geographic location, a sensor network is individually address depending on their location. It's doable to use the strength of the incoming signals as a proxy for the distance to the next nearby node. In these scenarios, SMECN excels because it constructs a dense graph of the nodes in the system before broadcasting the subsequent base station, making it simpler for nodes to discover their nearest neighbors. This information is shared so that all nodes in the network are cognizant of one another. This may be a useful means of communication and data sharing. Location-based approaches, which are mandated by routing systems, require nodes to enter sleep mode when no activity is observed. This system wants to save the most power, put to sleep as many nodes as possible. GEAR (Geospatial Extended Accurate and Resilience) and GAF (Geospatial Adapted Frequency) are two instances of the many location-based systems out there (Geographic and Energy-aware Routing).

### 1.5.4 Routing Protocols Based on Protocol Operation

Coherence routing mechanism, inter, inquiry, negotiations, Quality of Service and others fail under the umbrella of operation-based routing protocols, which are a cornerstone of the taxonomy of routing protocols. Adapt their behavior to the demands of the network, taking into account the frequency with which the network topology itself changes.

### 1.5.5 Multipath-Based

These procedures deal with several routes well. Instead of depending on a central link, nodes in a network use a decentralized system of several interconnected links to disseminate information. An alternative path is accessible in case the primary connection fails, increasing the network's reliability and fault tolerance.

### 1.5.6 Query-Based

To evenly disperse the use of queries, route-based on queries makes employing keywords generated through the access point. The central hub periodically polls the network's other nodes for updates. A network receives requests and is responsible for charge of perceiving and gathering information from other nodes or the base station, and if a match is discovered, it starts transmitting that data to the other nodes (here). The process by which the base station distributes interest signals across the network is known as Directed Diffusion [6]. These signals of interest, as they propagate across the network, eventually create a path that links all of the sensor nodes. Any sensor node with relevant data for a certain interest message will transmit that message to the base station. Data is collected along a journey to decrease power use.

### 1.5.7 Negotiation-Based

High-level descriptors included at the protocol's abstract level are used to prevent data duplication during transmission. The overlap and collisions that occur during transmissions of flooding data serve to distribute the data. Nodes get many copies of the same data during transmission and also, nodes in a network use a lot of energy transmitting what amounts to the same information over and over again. Sending Negotiations methods like SPIN [15] could reduce redundant information and stop redundant information from being delivered to the next surrounding stations.

### 1.5.8 Quality of Service (QoS)-based

When deploying a routing system of this kind, it is crucial to balance concerns about power consumption and data quality. When a sink requests data from network nodes, the nodes must meet certain QoS criteria, such as a maximum allowed latency (the data must be delivered promptly after it is recognized) and a maximum allowed throughput (the amount of data sent). It is groundbreaking because it is among the first routing protocols that consider QoS while making routing decisions. The sink's and the network's energy consumption, the QoS of each route, and the delivery priority of each packet are all factors in SAR routing choices. [8].

### 1.5.9 Coherent-Based

In a WSN, data is collected by sensor nodes and sent to the nearest neighbors or sink. The processing of data is the most important step here. The data processing techniques employed inside a network may be split into two sections at large: coherent seems illogical routing. Every node in the network acts as a data collector and processor, sending its results to the node in the network that is geographically closest to it. This technique is also known as non-coherent data process routing or aggregators. In coherent routing, data undergoes minimal processing before being forwarded to aggregators. Some examples of what is meant by "minimal processing" include time stamping and the elimination of duplicates. In this method, the nodes perform all of the processing, which results in significant time and energy savings [8].

## 1.6 Classifications that aren't on the list

According to the cable network wilderness communication channels, the data transfer process might be either proactive, reactive, or hybrid. The cable network wilderness routing protocols that are reactive estimate the routing elements before every network node are contacted, while in reactive routing protocols, this step is performed only when required. In cable network the routing values are computed, and the optimum wireless data channel is found when a sink needs to interact with a certain node.

The cable network "Hybrid" routing protocols, as the name indicates, integrate both proactive and reactive characteristics to determine whether or not to calculate the routing from either the sink to the source based on the form of communication. When the nodes are presumed to be immutable, table-driven (proactive) routing approaches are often used. Proactive routing approaches, in contrast to reactive systems that depend on finding the best route for data transmission, may significantly reduce energy use. Proactive routing removes the requirement to find nearby nodes while transferring data.

### 1.6.1 An in-depth Investigation of Routing Protocols

There are many cable network with several types of communication algorithms, including structure designed and operation-based ones. Hierarchy navigation, personal information routing, destination sending data, and performance enhancements are all types of route discovery are all examples of QoS-based routing approaches. This whole set of levels is called "hierarchical routing," and it's what's at the heart of modern internet architecture.

### 1.6.2 LEACH (Low Energy Adaptive Clustering Hierarchical)

Recent years have seen a proliferation of application-oriented protocols for use with wireless sensor networks, the most promising of LEACH [9] is an instance. LEACH employs a cluster-based design in conjunction with non - linear and non-routing. The cluster-based method designation may be attributed to the collaborative nature of the LEACH protocol's implementation across several sensors. Data is sent between clusters and ground stations via multi-hop routing. The wireless sensors collect information, compile it, and send it through radio transmission to a central hub. The sensors provide information to the base station. Several difficulties exist all throughout this process, such as data collision and data aggregation. Reducing the amount of data the cluster head gathers before transmitting it to the base station, LEACH may employ local data fusion to alleviate data aggregation problems. All sensors contribute to the formation of a self-organizing network by serving as cluster leaders at the very minimum time. The group leader is in charge of transmitting the collected sensor facts in bulk to the base station. There is an effort to reduce the network's energy usage, which extends the useful life of the sensors [10].The LEACH protocol comprises two distinct stages of operation.

### 1.6.3 Phase of Setup

Every sensor in a network exchange quick messages during setup to group into nodes. When the sensor at the head of the cluster is operational, it sends out short messages to rest of the nodes. The leaders of the clusters evaluate the intensity of the signals being sent out by the sensors and use that information to choose which groups or regions the sensors will join. The sensors that are looking to join a certain cluster head or area, please respond signals. The leader of a cluster could be the one to decide how many people should be included in it. Entering before a steady state, some factors are considered. These factors include the network's design and the relative costs of processing and communication. All members of the cluster group are subject to a TDMA schedule to send information to and collect them from the cluster head within the access point. Figure 1.2 shows, the first phase a detector in a Leach algorithm, where all detectors join together to create a cluster and report their data to the cluster leaders. Heads of clusters in the second stage of a multi-hop network send data to the sink nodes. The diagram following depicts a transmitted signal method.

### 1.6.4 Phase of Constant Motion

Once a Cluster head (Ch.) node is chosen every bit of data for an area data collected or detected in that region was delivered to the cluster head through the TDMA.

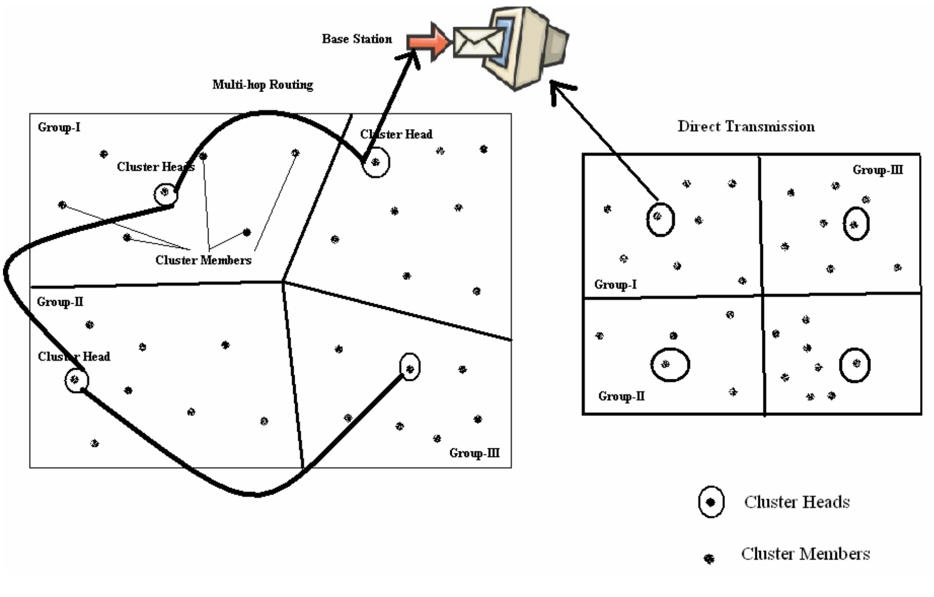


**Figure 1.2: Depicts an illustration of a LEACH procedure.**

When the cluster head send acquired numbers toward the support position which inside a compressed form, this concludes the second phase, known as the Stage of Stability When the stable state is reached has finished sending the information to the disposal search for cluster heads in a given region may be abandoned in favor of the search for new cluster members. At the time of completion, data transfers to the sink. A new settling-in period and steady-state will commence. Energy consumption is decreased or kept to a minimum thanks to the area's self-organized selection of cluster heads. Some sensors may not be utilizing as much power as the nearest node, depending on their distance from the cluster's brain. Synthesis of cluster heads or their roles in Nodes inside a cluster take turns serving as the group's leader. Frequently distributing work among a cluster's nodes, LEACH may significantly cut down on power usage [12]. Compressed information is sent between the cluster members and the central node. Since not everyone cluster heads are necessarily located A cross transportation network near to the gateway node is set up to deliver the compressed data to the nearest disperse beginning. When data transmission to the core network, LEACH employs that would save energy, the root node is rotated at randomly. Every single one of sensors will record this rotation so that no one sensor's power or battery would be depleted. Let's look at some numbers, and see how LEACH stacks up against direct transmission techniques. The energy lost in a straight line connecting randomly generated nodes in the network is the same as the energy lost in a strong network link connecting pair of nodes with either zero or one hundred percent cluster heads. By optimizing the number of cluster leaders in our network, to improve performance by minimizing the power needed to transmit data to and from cluster members. Sensors in the network will be in perfect energy balance if the network contains N1 cluster heads. If there are less than N1 cluster nodes, then all network nodes must use a longer transmission range to get data to the designated collect top when there are more of it than N1 cluster members, a node at the cable network edge must transfer its acquired data to a clusters. Leader closer to its location. [11] [12].

### 1.6.5 Multiple Clustering

Let's say that cluster A sends some information to cluster B. If this transmission has an impact on the adjoining cluster C, data in that cluster may be corrupted or lost entirely. Because of this, LEACH has used code division multiple access (CDMA) coding, in which an arbitrary component in a cluster selects itself to advance to the position of group head and then it spreads this arbitrary system across the system and the community at large. This enables it to filter or sort information of other organizations that employ various propagation methods. [12].

### 1.6.6 Segmentation Architecture

Nodes in the cluster interact with cluster heads at random, both within the group and across numerous clusters, to avoid data collisions. The idea may be expanded to create hierarchical clusters. All cluster heads in the preceding hierarchy, together with any additional as cluster heads, they connect to the access point. Super cluster heads. Because a result, the cost of transmitting information across large networks is drastically decreased [12].Simulations in [10] LEACH is compared to LEACH-C, MTE connectivity, and stable cluster, and find that LEACH provides superior achievement in terms of longevity and energy usage consumption, and data transfer speed.

### 1.6.7 Performance of Protocols in Surveillance Systems

The network nodes form clusters and relay information to the hub. Since a high amount of come together member may cause transparency otherwise excessive transfer many on their sinks, it is essential that a Cluster Head (the leader of the cluster) only need a small number of nodes to build clusters. Since a surveillance system needs to be able to take in a wide area, such as a battlefield, can't restrict the number of nodes it uses to a manageable level. To guarantee the highest quantity of statistics reaches the collapse, LEACH employs a continuous data-delivery mechanism. For a habitat-monitoring application like retina scanning, whereby just a single time-node deployment is needed, performance is likely to be better since the network density is modest. As a result, it has a longer network lifespan, lower latency, and superior scalability. Only the quality of service LEACH disregards, because the excellence of repair factor is kept low while building clusters for energy savings, there is no method to resend data packets if a cluster head fails to transmit data. Topology, or the structure of cluster formation, is updated whenever data transmission is complete in conjunction with both the sink and ground station.

### 1.6.8 Compressive Data Networks with Reliable Energy Harvesting

Similar to the LEACH clustering approach, Sensor nodes that operate wirelessly collect information and return it to their home position in a single packet or many packets. For LEACH, a clustering system is employed, with members of the cluster doing the sensing and a clustered boss collecting as well as sending the data obtained to the access point in a fused fashion (in a single packet). Using this below technique, a lot of power that would have been wasted has been preserved. Compressive Data Networks with Reliable Energy Harvesting (CDNREH) is an expansion of LEACH since it offers more efficient strategies for conserving energy. The simplest and most direct technique is from the core network to transfer data straight to the gateway node; however, this may result in rapid depletion of energy in all nodes. Nodes located further from the ground station lose power faster than those closer to it because more energy must be used to reach the furthest base station. The network's sensor nodes might be utilized to build energy-efficient cluster leaders and members. Cluster members do the Cluster leaders relay the resultant base station with information after data fusion. The furthest cluster head uses more energy again and again, but there is a time and a place for everyone in the network to be a clusters leader and transmit the merged information to the server. PEGASIS operates on the concept that all nodes can exchange information with their immediate neighbors. As can be seen in Figure 1.3, this is accomplished by establishing a chain. As soon as a node receives data, it combines it with data from its neighbors and broadcasts the result to the node nearest to it. Each node in the network gets information, combines it with information from other nodes, and sends the resulting signal back to the home base. Every node inside the system alternates as logistics. Delivering data collected from all other nodes back to the base station [13].

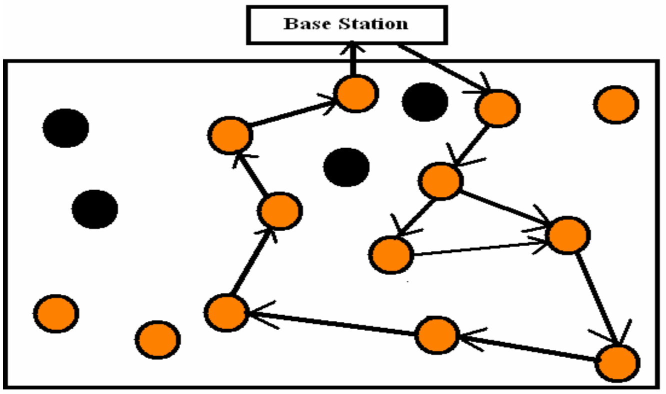


**Figure 1.3: Nodes in PEGASIS may be used to form chains.**

It means, on average, expect lower energy use across the board. Gluttonous algorithms are utilized to use all of the available network nodes. To calculate the energy cost of transmissions, it is assumed with the intention of every one of nodes through fluctuating could adjust for low levels of energy. A base station might accomplish this for all nodes, but it's also possible for each node to broadcast a signal identifying its neighbors. As the connection multiplies in size, the nodes adapt their communication such that they can only receive information from nearby nodes. Figure 1.4 shows the internal structure of PEGASIS. Using a greedy approach, connect all of the excellent node that really are nearby a short hop between themselves and the central node. Whenever the nodes furthest distant is chosen, data transfer can commence. For instance, if node 4 starts a chain by broadcast a message to all of the nodes of the network, the chain will be created. The closest recipient would be node 3, which would then relay the observed data. To find its nearest neighbor, it broadcasts a signal that mixes its data with that of node 4, which it then transmits to node 2. The information detected by use of nodes 1 through 2 is combined and sent to node 1. (Everything is packed together into a single package). Node 1 is the closest connection towards the access point. Node1 will now act as the leader and send all data transmission towards the core network. Single must begin with a nodule that has the data it had during chain building to fuse it with data from other nodes that have received it [13].

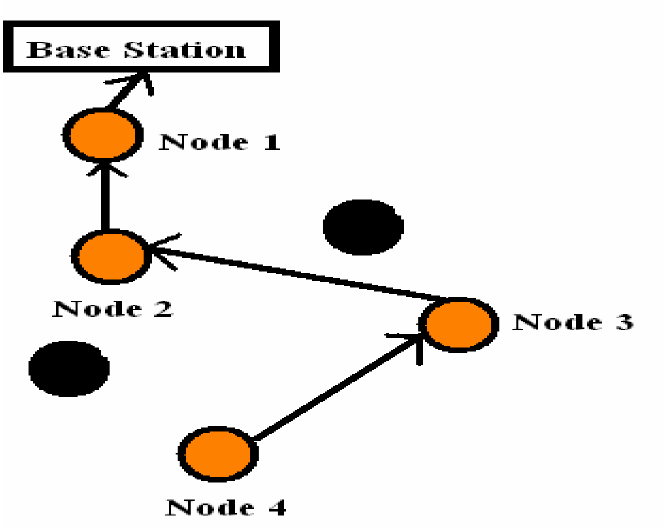


**Figure 1.4: Data is transferred in PEGASIS building link to approach BS**

If each of the cable network sensor cooperates to form the loop and carry out the most fundamental data forwarding activities, then the energy required to do so may be distributed more evenly. If a node in the chain fails, a new chain is created to take its place. The simulation in [13] demonstrates that PEGASIS is superior to LEACH due to its ability to save energy at several stages of the clustering process, including cluster member development and cluster head construction. In this setup, any node may take charge and relay information to the hub in a single cycle. The energy efficiency of the network's nodes is measured. When compared to LEACH, all types of networks benefit from a reduced number of node deaths during the chaining process. The network's longevity is increased when all nodes are actively involved [13].The results of simulation analysis of the PEGASIS and LEACH protocols across a range of network topologies. Several investigations have shown that PEGASIS extends network lifetime, improves energy efficiency, and boosts overall performance.

### 1.6.9 In Surveillance Applications, Protocol Performance is Critical

Since nodes in the network are blind to their location, PEGASIS employs a greedy approach to collect as much information as possible from as many nodes as it can locate. In this any node fails, it might be difficult to find an alternate way to the sink for transmission since the path between nodes is fixed. While it performs a better job of conserving energy, it doesn't take into account concerns about service quality. Adding nodes outside of the single-hop range forces the network to evolve into a multi-hop topology so that it can better manage the skewed load.

## 1.7 Routing Protocols Comparison

The comprehensive analysis of routing protocols allowed for a holistic evaluation of each protocol based on the criteria established at the outset of this thesis. How well a protocol communicates with the sensor nodes in a network is a major factor in its overall rating. The following table (Table-1.1) summarizes the protocols functionality concerning latency, scalability, mobility, and energy consciousness. In addition, the relevance of each process is elucidated in a brief paragraph that follows.

**Table 1.1: Routing protocols for adaptation of connectivity**

| ***Distinctiveness*** | **Time Delay** | **Durability** | **Adaptation of Connectivity** | **Energy Consciousness** | | |
|---|---|---|---|---|---|---|
| ***Protocol*** | | | | Short | Middle | Strong |
| **LEACH** | *When the network is small* | *High* | *The transmission is led by cluster* | *High use the clustering approach to just save energy.* | | |
| **PEGASIS** | *If connection density is high, the probability is high.* | *Strong* | *Communication is handled by a single point inside the network.* | *To approach the network device, it establishes a network of node.* | | |
| **SPIN** | *If the connection is small, intermediate* | *Reasonable* | *Data is exchanged with interested nodes in order to reach the sink* | *Medium, only nodes with energy supplies participate in Transmit.* | | |
| **GEAR** | *Involves checking for depleted nodes* | *Medium* | *Calculates the cheapest routes to the sink.* | *Moderate, using the same pathway until the new route is computed* | | |
| **GAF** | *Medium makes use of fewer units.* | *High* | *Every component from of the grid is still in the sleep state.* | *High usage of sleep, discovery, and awake states by the node* | | |

| ***Distinctiveness*** | **Time Delay** | **Durability** | **Adaptation of Connectivity** | **Energy Consciousness** | | |
|---|---|---|---|---|---|---|
| ***Protocol*** | | | | Short | Middle | Strong |
| **MECN** | *The relay region has a moderate number of edges.* | *Low* | *To reach the sink, relay nodes are needed* | *For each transmission, Moderate creates a sparse graph.* | | |
| **SAR** | *Low, Multi-path is present.* | *Moderate* | *The tree is constructed from the sinks to the branches.* | *High, determines the optimum path while not exhausting all entire network* | | |
| **SPEED** | *Medium, Transmitter is present.* | *Moderate* | *The tree is constructed from the sinks to the branches.* | *High, determines the optimum path while not exhausting all entire network* | | |

Quality of service, sensor transmission modalities, and network overhead for sink-to-sink and node-to-node data transfers are all summarized in Table 1.2. Power consumption in the network and the nodes' routing strategy for communication are also investigated. An exhaustive explanation of the methodology used to arrive at these conclusions is provided below the table.

**Table 1.2: Performance of protocols in network power consumption**

| ***Distinctiveness*** | **QoS** | **Network Traffic** | **Network Power Consumption** | **Scheme of Transmission** | |
|---|---|---|---|---|---|
| ***Protocol*** | | | | **Smooth** | **Multi-Hop** |
| **LEECH** | *Low* | *High, entire member nodes begin data transmission to sink.* | *High* | *Omni, member nodes actually communicate to sinks* | |

| | | | | |
|---|---|---|---|---|
| **PEGASIS** | *Low* | *To transport information, all nodes create just one link.* | *High* | *Only use multi - path if the separation between neighboring is more than a single destination.* |
| **SPIN** | *Low* | *Low signal nodes are eliminated.* | *Low* | *Multi-hop, http request method to data exchange* |
| **GEAR** | *Low* | *Moderate,* | *Low* | *That once shortest path determined is used; it remains flat until nodes problems happen.* |
| **GAF** | *Low* | *Moderate,* | *Low* | *Mega employs simulated network networks as works by interfering.* |
| **MECN** | *Low* | *Small, accurately chooses connections from of the relaying area* | *High* | *Generated inter, heterogeneous network with components picked across relaying areas* |
| **SAR** | *High* | *To circumvent this, fresh router tables must be built each occasion.* | *Low* | *Mega, Trees are created from node to sink or sink to node.* |
| **SPEED** | *High* | *Consequently, congestion control getting the proper is prevented.* | *Low* | *When no network outages or congestions occur, number of co is used* |

### 1.7.1 LEACH

The Protocol compared with direct transmission and lowest transmission energy routing, Leach may cut communications wasted energy among clusters members and leaders by as much as eight times [12]. Each head makes sure that data gets to its destination either by inter-cluster transmissions or by intra-cluster transmissions, making LEACH very efficient and reducing latency. Since nodes may begin processing as cluster members with signals given by cluster chiefs, large-scale deployments may be easily handled. Clusters are more energy efficient than networks made up of individual nodes since only the cluster heads are responsible for data transmission. Due to limitations in available resources, such as the amount of the memory buffer utilized for processing, the quality of service is low. Since all of the network's nodes are constantly moving to new clusters, the flow of traffic is very irregular.

### 1.7.2 PEGASIS

The nature of PEGASIS's chain design, data from the furthest or first node in the chain carries crucial information that must be supplied promptly and must thus travel to that same core network across the whole loop. Since the transmission path is flexible, adding more nodes to the chain is easy. The nodes are found during chain creation that may save energy, they are added to the chain. Chain architecture used to reach the base station allows for far more energy consciousness than LEACH's cluster formation. Only one node in the network is responsible for transmission, and it is situated close to the sink or destination, hence the network incurs very little overhead. Each intermediate node adds information to the data packet before sending it on, which slows down the transmission, processing of the data and reduces the quality of service. Network failures, such as a node failure, a connection failure, or a power failure, may cause data loss.

### 1.7.3 SPIN

Ensuring that all relevant system components may acquire the necessary information, SPIN requires a little wait. Newly joined nodes send out requests for data exchange in the form of signals, but nodes that are running short on power will ignore them. Energy awareness in SPIN is thus modest since only nodes with an interest in data exchange will participate, whereas nodes with low energy reserves will not react to messages sent by adjacent nodes to preserve energy. Very little information is wasted on the network since so few nodes are involved in the transmission process. All the network nodes are exchanging the same information to keep the quality of service good. Since all of the nodes are sharing the same information, a lot of memory is being wasted, and there is a lot of interference from other nodes when they try to send their information to the sinks or access point.

### 1.7.4 Mechanism of GEAR

Until a new, less costly path is discovered, nodes will only travel along the already preferred routes. As can be seen from this example, GEAR is unable to achieve more energy savings after using the cheapest possible routes. This results in a short round-trip time for data transmission between nodes, or low latency. The nodes in the network are found to be at capacity, data transmission is delayed until a new least-cost route is discovered, and an average overhead is detected. Data transmission might fail due to network instabilities such as power outages and changes in the network's structure. It necessitates a significant amount of effort and money because utilize the various methods that are used to pinpoint the last node and the final target region.

### 1.7.5 GAF

Whenever original information in a grid wishes to important predictors to a neighboring matrix, the remainders of the components in the grid cooperate. In that grid go to sleep since only one node may be active at a time. There is no limit to the number of nodes that may be added to a network; instead, each node works independently inside a grid, with each node in the grid periodically switching to sleep mode when there are too many active nodes. Since the nodes may toggle between an active state, discovery mode, and sleep state, it includes the potential to achieve a high degree of awareness. The network's data overhead is minimized since just a few nodes function as active intermediaries. Poor quality of service is ensured because of unpredictable traffic patterns and lack of end-to-end transmission.

### 1.7.6 MECN

Since newly added nodes are not considered, even if they are the closest to the base station in a sparse network, their scalability is low. Every time a node has data to broadcast, it must first calculate the sparse graph for its nearest neighbors. This has the effect of keeping latency to a minimum. This results in severe energy loss every time a node transmits. Despite its low power consumption, MECN is considered an energy-efficient protocol. Poor service quality is caused by several factors, including but not limited to, broken connections, power outages, and bandwidth limitations.

### 1.7.7 SAR

The QoS is better than with other conventional protocols because of the decreased delay factor, and because SAR networks usually use a routing table to find the shortest path from of the junction to the sink. There is just zero overhead in terms of data transfer or processing power, and no need to reserve memory for its operation. As it is time-consuming and resource-intensive to create a routing table for each newly deployed node, its scalability is limited. In the event of a node failure, the system is capable of promptly and reliably resuming normal operation.

### 1.7.8 SPEED

To keep data flowing in the event of a node failure, SPEED employs backpressure rerouting. Direct connections between each node, this routing technique offers very low latency and deserves high praise. It uses the least amount of energy possible to locate the most effective pathways, hence establishing that it is an energy-efficient method. Achieves a state of network equilibrium in which data transmission may continue uninterrupted in the event of a connection failure and where a high quality of service features such as data redundancy and processing and memory buffer capacity limits are not present.

## 1.8 MAC (Medium Access Control)

Wireless sensor networks place a premium on reducing power consumption, however, collisions may occur when many nodes transmit information towards the sinks or access point at once, resulting in damaged packets that must be retransmitted. This protocol facilitates effective channel access on the node's part, which in turn allows it to reduce power consumption and maintain a high degree of service quality. Multiple access methods like TDMA, CDMA, and FDMA are often used in MAC protocols (explained below).

**Multiple Access Schemes**

In the following paragraphs, explain the various WSN multiple access schemes.

### 1.8.1 TDMA

The principle of Time Division Multiple Access (TDMA) in the direction of let multiple nodes share a channel without interfering with one another. WSNs (wireless sensor networks) are employed. To facilitate communication between the base stations or Additional connections as well as the sinks connection such as save power, TDMA schedules transmissions from nodes to the sink only at certain time intervals. During these periods of inactivity, routers that really are presently not sending information to such sink go to sleep. In this case, the period may use the whole bandwidth available. The system relies on sinks receiving and broadcasting the clock synchronization message to avoid collisions. Since active modes consume more energy, the device must be brought up from sleep mode when a packet is received.

### 1.8.2 FDMA

Time division multiple access (TDMA) requires all nodes to be actively listening before they can receive the synchronization packet, which might cause delays owing to the time-based nature of the access mechanism. With FDMA, the available bandwidth is partitioned into several channels, each of which may be used by a separate node to send and receive data without interruption. In an FDMA network, nodes share scheduling information to stay in step with one another.

### 1.8.3 CDMA

Code Division Several Access (CDMA) is a transmission technology that allows multiple nodes to send packets simultaneously while causing a little amount of interference. By giving each node access to its entire bandwidth, it avoids the communication delays of TDMA and the capacity constraints of FDMA.

## 1.9 Problems of Energy-Efficient Medium-Range Access Control

The media access control protocol is used in a cellular ad hoc network sub layer and error control may assist reduce the power consumption of individual nodes (WAHN). The Media Access Control (MAC) layer a number of wireless sensing network is accountable for two primary tasks: (a) it must set up data communication links to create the cross mobile broadband communication needs the bare minimum of internet services, and (b) it must control how each sensor node connects to a central television source. These networks place a premium on speed and responsiveness. The lifespan of the network is not considered a big worry since batteries and other energy sources are readily refilled or refilled. But in Mobile Ad hoc Sensor Nodes, in which these connections are frequently implemented in difficult to access types of terrain like seismic areas, open burning, or even hidden behind hostile forces, for which good access is unreachable and battery packs are not exchangeable or rechargeable, clean energy is essential.

Except for nodes acting as cluster leaders or gateways, which must remain active at all times owing to the huge volumes of data they must relay, nodes in WSNs may be put to sleep for considerably longer periods while waiting for an external event to occur than in WANs. As a consequence, this will lead to unfair bandwidth distribution within the cluster, as nodes closer to the head of the cluster will need to connect with the head less often while having more data to send. Retransmit of information or management packages as a result of conflicts or overcrowding constitutes one of the primary causes of energy losses by both the Intermediary stations in a Wireless Mobile Ad-hoc Network (WAHN) (Ye, Heinemann, et al., 2002). Due to the hidden node problem, a node will not bother decoding more than one packet from a separate source at once. Retransmitting these packets causes the afflicted nodes to use more energy and results in network congestion. Another source of MAC layer power consumption is dormant channel detecting. When nodes get arranging packages or wishing to communicate waste energy by constantly sensing the channel until it is free. Since data transmitted by one node in a shared media is appreciated wherever the nodes can spend resources receiving packages that aren't intended for it during that communication range. Due to the fact that nearly all Communication systems need transmitting control messages of various sorts (for synchronization, RTS, CTS, ACK, and so forth), thus may dramatically increase the operating energy costs of wireless sensor nodes with limited resources. As has been seen above, throughput in a network is of equal importance to other factors such as energy efficiency and system longevity. However, a balance between network durability and throughput must be achieved, taking into consideration the needs of the application.

Limiting power usage at individual nodes is a pressing issue for WSNs. There has been and is now continuing research aimed at developing energy-efficient MAC protocols to deal with the aforementioned problems. The most basic way for MAC layer protocols to save power is to turn off the radio and put the node into sleep mode. It is clear from looking at Figure 1.5, that there are three distinct categories of wireless MAC protocols: centralized, distributed, and hybrid.

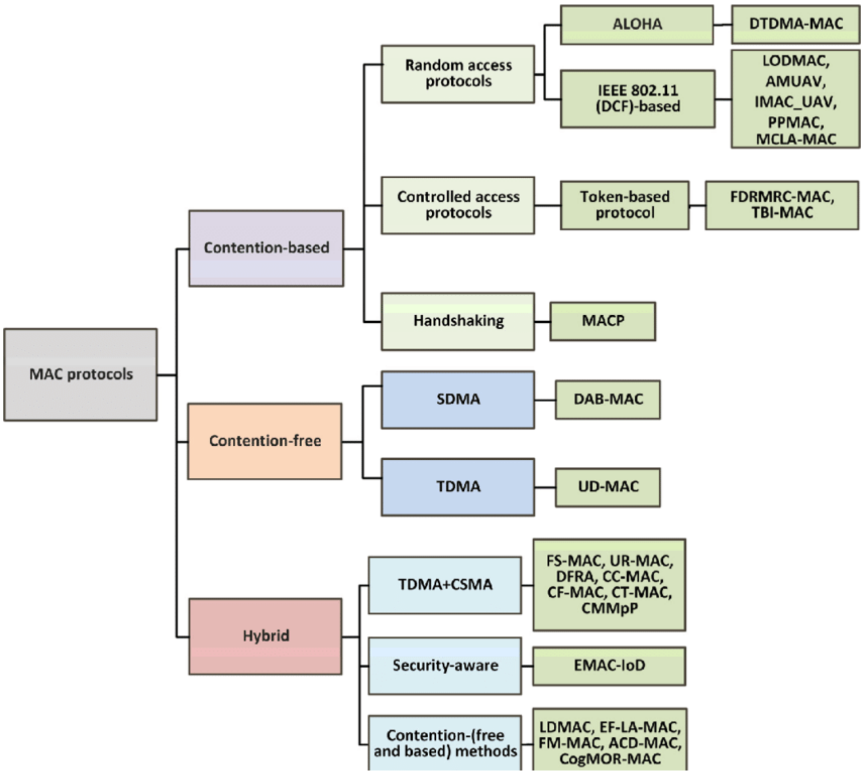


**Figure 1.5: Wireless Mac Layer Taxonomy.**

## 1.10 Centralized MAC Protocols

The goal MAC techniques that are consolidated is to ensure that all sensor network nodes may communicate with one another without interruption, and this task is delegated to a centralized controller. Various channel multiplexing techniques have been proposed, including Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA) (Pottie and Kaiser 2000). TDMA, on the other hand method has a serious flaw in that the energy requirements of the central controller are much larger than those of the other nodes. Due to fluctuations in size and WSN when stations was included as well deleted, sophisticated and keep an efficient operating routine, hardware components and computer techniques are necessary. Adding control information to the overloaded and power-hungry sensor nodes is also a significant difficulty, because of the restricted channel capacity and the significantly larger number of nodes assigning a particular operating frequency becomes impossible. When all nodes are assigned the same set of frequencies but only a subset of them are utilized, bandwidth is wasted and the duty cycle is low. There may be problems with frequency allocation if the network quickly grows in size, as all of the available frequencies may already be in use. While CDMA enables simultaneous transmission from an unlimited number of nodes, the required transmitters and receivers are necessarily complex because each node uses a unique data encoding scheme.

### 1.11 DMAC Protocols for Wide Area Networks

Under some circumstances, all of the nodes in the network may be able to access a large number of channels thanks to the support of these MAC protocols. Carrier sense multiple access/carrier aggregation (CSMA/CA) is a well-known example of such a protocol since it requires all participants to regularly check to see whether the medium is in use. The transmission bandwidth is already being used, the broadcast will be delayed. Collisions may be avoided by the employment of time-delay methods like the IEEE 802.11's multi-hop communication functionality employs a randomized spine technique. Based on work first published in 2002 by Cheng et al., this is a paraphrase. However, distributed MAC protocols cannot completely avoid packet collision, which has a profound impact on network quality of service due to the presence of both "hidden" and "exposed" nodes. In this context, a "tucked away node" refers to a node that is within the recipient's reach but outside the transmitter's capability. The correspondent shouldn't restrict the exposed node from broadcasting to avoid a collision if the receiver is outside the sender's spectrum. Using control messages, the DCF reserves transmission time between nodes, so resolving the problem (RTS and CTS).Large-scale sensor networks benefit greatly from the flexibility and ease of deployment offered by distributed MAC systems. Listen-before-talk systems, on the other hand, waste energy by continually monitoring the channel, and they don't even help prevent accidents.

## 1.12 Hybrid Media Access Control Protocols

The present centralized and distributed MAC approaches are not ideal for WSNs because they do not maximize power efficiency or scalability. The optimum procedure would indeed be have the manageability of central systems as well as the adaptability as decentralized ones. Redundancy, low power consumption, and the ability to narrow their broadcast range in response to events and activities are just a few of how wireless sensor networks stand apart from conventional network architectures. IEEE 802.11 is primarily concerned with using networks for WLAN (Wide Area Network) purposes. These nodes use a lot of energy since they are constantly scanning the channel. There is IEEE 802.11 has an energy option as well, although there is no requirement for a precise sleep-wake regimen. IEEE 802.11 wireless networking, the distance between a nodule and a base station is often just one hop. Due to radio interference and the mobility of the nodes, clock synchronization becomes increasingly challenging as the network expands and multi-hopping is employed. Wireless (Haartsen, By et al., 2000) is also one more relatively brief wireless transmission technique system that employs a TDMA/CDMA hybrid scheduling approach and finds widespread application in consumer devices. In a Bluetooth Piconet, one node serves along with owner while the others are slaves. Massive Scatter Nets are constructed using smaller networks called Pico nets. The deployment of Bluetooth devices at the size of a WSN presents challenges, however. Bluetooth's scalability is lower than that of contention-based protocols due to the difficulty of TDMA in planning and synchronizing all the nodes..

## 1.13 Limited Medium Access Development for Wireless Communication

Many of the existing WAHN protocols have been modified so that they may be used with WSNs. For WSNs, several common MAC protocols are shown below. The MAC Detector (DMAC) (Ye, Heinemann, et al. 2002) proposes to lengthen the battery extending the life of wireless sensors networks by programming devices to enter periodic physical buttons states while not in use broadcasting.

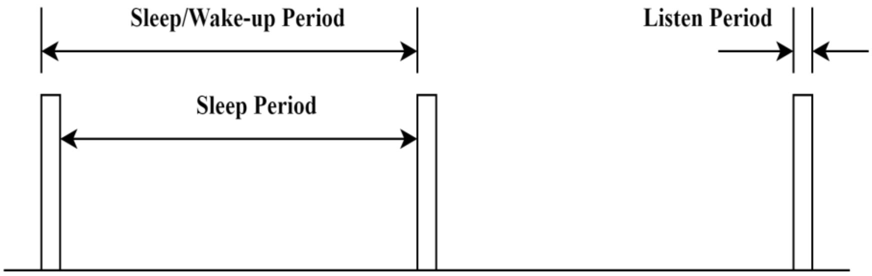
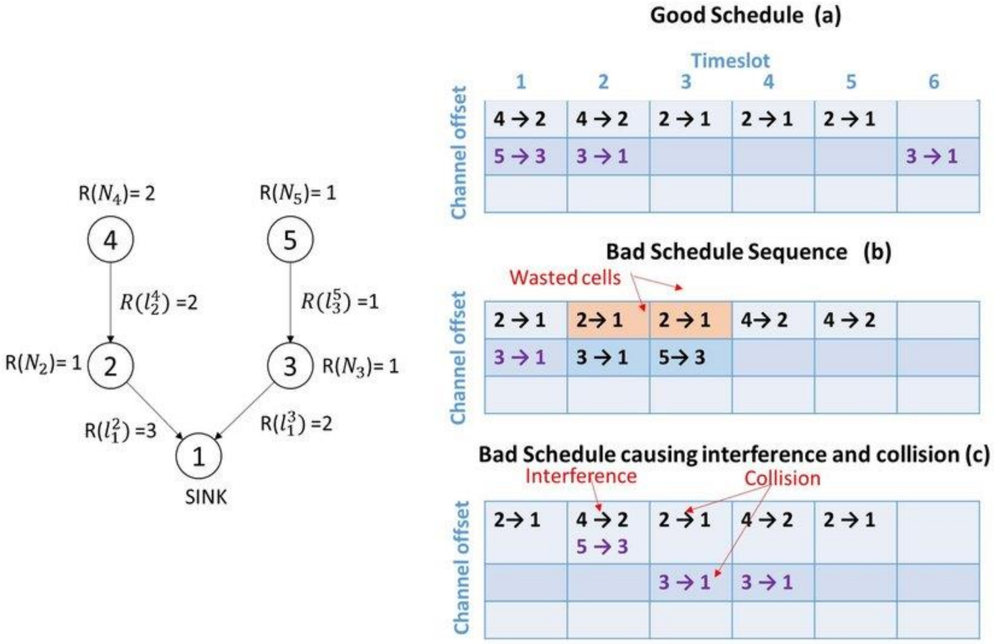


**Figure 1.6: Sleep-wake D-MAC's switching frequency.**

In each frame, a node has two states: listening and resting. The duty cycle (or the length of time that receivers actively listen) may be modified in response to changes in traffic loads. During startup, a node will stay awake for some time before falling asleep to learn the sleep-wake schedule of its neighbors. If given a schedule, it will follow it to the letter. When a synchronization broadcast is expected but none is received, the network takes over as the synchronizer and broadcasts its message. When a cluster of nodes hears a pattern, the ones nearest to the source are more likely to begin performing the routine. This results in the formation of virtual clusters. Due to the impracticality of a unified physical cluster, a sensor network may instead consist of many virtual clusters. Depending on their proximity to the cluster's edge, certain nodes may be subjected to some different sleep-awake patterns and, as a consequence, may wind up adopting a hybrid schedule to properly transmit data between clusters. Due to the ease with which any network infrastructure node might well be established, schedule packets are constantly broadcast. As a result of clock drift between nearby nodes, scheduling errors might occur.

After resuming sleep, all nodes except the leader wait silently throughout the SYNC period to check whether any updates have been broadcast. Just as with IEEE802.11, SMAC makes use of the RTS/CTS packets to avoid collisions. Physical carrier sense and virtual carrier sense are both used by the system. Figure 1.6 shows that during the "Listen for Sync" period, nodes 1 and 3 get the SYNC packet, represented by the shaded rectangles, to synchronize with the routine of node 2. To do this, nodes use their physical carrier sense to identify whether the channel is busy, and if it is, they refrain from transmitting and instead focus on receiving the packet. The period spent waiting for Node 3 to transmit an RTS packet to Node 1 and therefore begin virtual carrier sense transmission is illustrated either by darkened rectangle outline, which corresponds to the "For RTS" time Node No. 3 The RTS payload will also include data about the sender, the receiver, as well as the packet's duration. The shaded rectangle represents the period during which Network device would send a CTS message. At that start of the period, non-receiving nodes will wake up and stay awake until the Network Allocation Vector (NAV) is no longer zero. Consequently, node 2 is now resting while nodes 1 and 3 carry on a lively dialogue.



| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| 4 → 2 | 4 → 2 | 2 → 1 | 2 → 1 | 2 → 1 | |
| 5 → 3 | 3 → 1 | | | | 3 → 1 |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 2 → 1 | 2→ 1 | 2 → 1 | 4→ 2 | 4 → 2 | |
| 3 → 1 | 3 → 1 | 5→ 3 | | | |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 2→ 1 | 4 → 2<br>5 → 3 | 2 → 1 | 4 → 2 | 2 → 1 | |
| | | 3 → 1 | 3 → 1 | | |
| | | | | | |

**Figure 1.7: Network nodes' scheduling patterns**

In figure 1.7, the choice of scheduling pattern depends on factors such as the application requirements, energy constraints, node capabilities, and the desired trade-off between energy efficiency and network performance. Designing an effective scheduling scheme is a challenging task in WSNs and requires careful consideration of the specific deployment scenario. When more information should be given before fit into a single packet, SMAC segments the data such that many packets may be sent using a single RTS message. The nodes reduce energy consumption, but the trade-off is increased latency. A networked packet will have to wait between hops because the nodes in the middle going to sleep. Adaptive listening was created to decrease network latency and handle increasing network traffic (Ye, Heinemann, et al., 2004). The networks will raise their switching frequency to handle the increasing bit rate. And stay up for longer if the network is busy. During its listen-to time, node 'A' will be able to anticipate when the data will be complete if it can pick up on its neighbor's RTS/CTS broadcast. Node A will sleep until the transmission between its nearby nodes is complete, therefore reducing network congestion and latency. If node A is the next hop in the chain, its neighbor will bypass the next awake schedule and deliver the message immediately.

While SMAC has the potential to reduce energy expenses, it is not perfect. Latency is reduced by putting the nodes to sleep at appropriate times according to TDMA scheduling rules. However, the network's performance is greatly hindered by a constant duty cycle that cannot adjust to unexpected increases in traffic. In addition, many nodes will belong to several clusters, allowing them to remain up for considerably longer and transmit more data than the network's leaf nodes that belong to a single virtual cluster. It won't take long for the energy stored in these nodes to run out, making them useless. Developing a flawless low as the network size increases, the navigation system's power usage will increase will be challenging, if not impossible, because of the dynamic nature of the virtual cluster, which raises the cost of network tunneling.

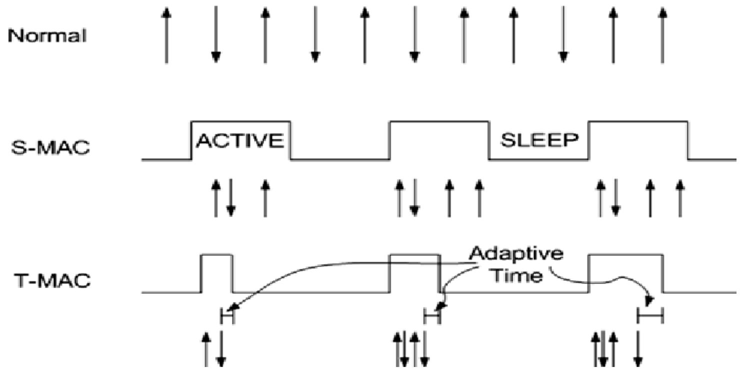


**Figure 1.8: Comparing T-MAC and SMAC frames.**

Timeout MAC (T-MAC) is a kind of MAC protocol that functions similarly to SMAC but automatically adjusts to fluctuating network traffic (van Dam and Langendoen 2003). T-MAC outperforms traditional MAC protocols because it can better handle fluctuations in network activity. Following the end of the listening period, a timeout interval is applied, and each frame consistently lasts the same amount of time (TA). The timer won't put the node to sleep if it receives any control or data messages within the timeout period. Each fresh package shipment triggers the clock to start ticking a new. T-renewed MAC's flexibility to respond to changing traffic loads is a direct outcome of this procedure. Figure 1.8 depicts the parallels and distinctions between SMAC and T-MAC frameworks. After receiving a message in SMAC, the network primary requirement until the listening period ends. When a node uses T-MAC to receive a packet, it wakes up briefly and then goes back to sleep until the time out (TA) counter reaches non-zero, conserving T-MAC frequently transmits delayed data in a burst, low latency for multi hop networks. T-early MAC's sleep syndrome weakness might potentially lower its throughput. If a node has to go dark for a while because of congestion, it won't be able to send or receive any data during that period. When the conflict time ends and the sender is free to send, the receiver is likely to be fast asleep.

## 1.14 Low-Power Map-Reading Protocol

The fundamental objective of this research is to identify effective innovative routing algorithms for lowering the power requirements, sensor nodes in wirelessly ad hoc wireless systems are characterized by the absence of a previous foundation for networks. A procedural channel's mobile node are continually exchanging information with one another. Several low-power methods have been suggested and implemented in recent years, and their efficacy has been examined in a variety of studies (Lindsey, et al.). Connectivity-based and activity-based routing are the two main categories into which the authors (Li, Cordes, et al., 2005) classify protocols for routing.

## 1.15 Protocols for Active Energy Conservation

Active energy conservation solutions seek to identify the most productive path. The primary goal is to cut energy usage per package (Singh, Woo, et al. 1998). Power-Aware Routing Optimization (PARO) protocol is shown in a simplified form in Figure 1.8. (Gomez, Campbell, et al., 2003). To get a message from node 'a’ to node 'e,' 'a’ will calculate the multi-hop path that uses the least amount of energy. Power consumption increases significantly when data is sent directly to the target node, hence this measure is necessary. By Xue and Li (2001), a greedy localized approach that takes advantage of relay areas is the foundation of the Location-Aided-Power-Aware Routing protocol. This approach ensures that every node in the network is aware of both its own location and that of its neighbors. The set of all the places where destination nodes can be reached more effectively by relaying through node r than by broadcasting directly from node s is known as the relay region R(s, r) of a source node s and a relay node r. Node r should ideally relay the message if the receiver node is situated within the relaying area. If the target node really is located where a number of neighbors’ relay zones meet, using a greedy approach, the next hop that uses the least amount of energy is chosen. One alternative protocol is low-power networking (Banerjee and Misra, 2002), which can control the radio's transmission power to use just what is required to maintain a sufficient signal-to-noise ratio (SNR).Nodes that are frequently employed to send a signal lose strength much more rapidly when active power-aware routing is in effect. Moreover, node B needs node A to send its message to nodes C and D. Node A may exhaust the network's power supply and make the whole system useless.

## 1.16 Protocols for Extending the Lifespan of a Network

Protocols developed with lifespan in mind try to distribute energy consumption evenly throughout the networks to address the issue of overuse of different nodes. Power consumption may be lowered using a technique called Minimal Battery Cost Routing (MBCR) (Toh 2001). This navigation algorithm computes every route's overall power usage route by factoring in the battery cost of each hop along the way to the ultimate destination. The goal this time is to reduce energy use as much as possible. Maximum Survivorship Routing (MSR) (Marbukh and Subbarao, 2000) bases its route cost on the number of nodes whose remaining battery life is higher than a specific criterion Communications will not be delivered to stations that are below a specific level of battery performance.

## 1.17 Conclusion

These procedures have shown to be superior to previous ones in several respects, including their ability to efficiently route the most important data while conserving the sensor's battery life. This thesis investigates the routing and MAC protocols in detail, with a particular eye on the protocols' support for real-time applications like security and their energy-saving measures. Looked at when procedures are used, the architectural compromise among conserving energy and the level of service provision considered for wireless sensor networks based on assumptions like latency, scalability, energy awareness, synchronization, etc. To save power on the nodes, Central argument systems such as SMAC, TMAC, and TEEM use a single transmitter and modify its configuration periodically at periodic times. STEM is an energy-efficient protocol that utilizes two transmitters (one for statistics as well as one for get up). The data radio may stay in a low-power sleep mode until it is needed for processing, at which point the nodes can activate it. In contention-based protocols, collisions and delays occur in transmission since every bump is given access to those same social networks. Protocols for avoiding collisions are those that do not cause collisions, such as DEMAC, PACT, and LMAC. Each node is given a certain amount of time in advance to transmit data, but to stay in sync, it must also listen to the transmissions of the other nodes. This might potentially raise total energy consumption. Because clock drift is a problem for contention-free protocols, tight synchronization is essential. Central argument procedures use less resource but cannot give serious support, whereas central argument techniques use less resource but do not assure actual support. There are still many sensor node issues that must be handled. Adaptive locally-implemented algorithms and precise synchronization of time and space are essential components of routing protocols for achieving the desired perspective of the society [3].

# CHAPTER – 2
# LITERATURE SURVEY

## 2.1 Introduction

The spread of communications systems, World Wide Web, had greatly facilitated many facets of life, including personal interactions, commercial transactions, the delivery of services and more. In the meanwhile, security problems and attack methods have caused many types of network security risks to become quite dangerous. As a result, safeguards that prevent these dangers while still preserving the privacy, reliability, and accessibility of computational assets are of paramount importance. Intelligent intrusion detection systems (IDS) a vital preventative strategy in computer security due to the extensive malicious network traffic. Packets in a computer network are monitored and collected. Through packet analysis, IDS may identify suspicious activity and prevent intruders from establishing connections to the network.

## 2.2 Review of Articles Related to Intrusion Detection System

(Mingjian Cui 2018) have presented an MLAD approach for forecasting attack loads. Reconstructing the benchmark and scaling information is achieved by k-implies clustering using the Predicted load. To conclude the specific assault plan, the naive Bayes arrangement is applied. Finally, these events as well as parameters information for something like a specific cyber-attack are combined using evolutionary algorithms to create a stress indicator.

(Juniad Akram 2019) have provided a method for creating a defenselessness standard at many granularities, including the task level, the document level, and the component level, all of which contribute to successfully repelling cyber security assaults. Online, you may find a sample of a vulnerability benchmark that can be used to track vulnerabilities in your framework. The data of defenseless systems have also been provided at a granularity that makes it possible to identify individual components; if you are using such components, you are vulnerable.

(Colin Urquhart 2019) Vehicles with an embedded relationship module and self-driving capabilities are advancing quickly, as has been suggested. While these modules increase the number of services available to end users, they also make the system more vulnerable to attack. A little formal study has been conducted on the cyber security aspects of existing automotive advances. Therefore, it is crucial to provide computerized criminology examiners utilizing information to study accident data or wrongdoings dedicated to automotive advancements and to increase the remote keyless entry technologies to ensure the protection of the inhabitants.

(Chen Peng 2018) Attacks against SGs have been suggested as a means of achieving this reduction. The accessible security arrangements can't be accomplished correctly by a single explicit arrangement due to the variety, complicity, and insight of system assaults. The attacking side will always try to maximize the impact of their assaults on the defensive operation, while the defenders will do all in their power to mitigate the damage they incur. Furthermore, as threats are increasingly diversified, sophisticated, and complicated, traditional IT security approaches may no longer be effective.

Lee DH, Chen H-H, Jo M, Kwon T, and Cho K. Clone detection methods in wireless sensor networks are categorised and subjected to experimental investigation. IEEE (2013). The notion of cell topology is used in the replica detection methodology, and in this system, the replicas are found using the multi-cast location approach, which claims to be a single or multiple cell. It improves the precision of detection strategies. Zhou J, Boa F, Robert HD, and Zhu WT. A survey on the detection of node replication threats in wireless sensor networks. (2012) J Network Computer application. In a cluster system, the cluster head is chosen via an election procedure in which nodes are given the chance to participate in the process in order to avoid having a single individual in charge of the system.

(K Suganthi 2015), to extend the life of wireless sensor networks, use a fault-tolerant virtual backbone tree that has been randomly generated. The replication attack problem in the WSN with cluster protocol is represented by a framework named NI-LEACH in Computer Electric Eng. (2015). In order to do large computations and energy-efficient tasks, this protocol requires witness nodes. The first factual methodology for analysing honeypot-caught assault data in its totality has been provided by (Zhen Xin Zhan 2013). The architecture was built on our ground-breaking idea of unpredictable attack evolution, a cutting-edge method of using a numerical substance to compare various cyberattack types. The "dim box" prediction models' expectation intensity justifies the time and effort invested into understanding the sophisticated quantitative properties of stochastic cyber-attack types when compared to "discovery" expectation models.

(Ying Wan 2017) Using a cyber-physical system framework, investigate the distributed-following difficulty intended for composite dynamical systems that include Lipchitz-type nonlinear features. The circumstances of the operators are often unreachable for controllers because of sensible limits in some situations, therefore distributed eyewitnesses used to recreate the conditions of hubs are necessary, which will first necessitate planning. Many assaults may cripple both the channels used to convey control input indications and perception signals, even though they are often assumed to be independent of one another.

(Chen Zhong 2018) has suggested that security operations centers (SOCs) use a variety of cyber shield techniques to monitor operational events. For incident localization and response, SOCs rely not just on these automated systems, but also on human analysts. To discover the fundamental trademark restrictions that may be used as guidelines for information filtering and connecting, suggested a chart-based follow-digging approach. Because of these guidelines, restricted state machines were designed to guide automated information triage.

(Paul M. Sea shore 2019) have suggested that the growing inevitability of assaults emphasizes the need for better system security research and design in health essential as well as vital systems. Furthermore, given the trend in the direction of making intricate, predictable system systems, the building issue of extending secured and adaptable systems that fulfill the specified requirement of expense, timetable, and execution is constantly challenging. Practical guidance on when and how the 18 plan standards may be utilized for more effective SSE activities is presented, along with real-world examples of their application.

(Sukumaran 2017) have proposed ,disseminate a few practices and techniques in creating strong cyber protection architectures for transmission and distribution automation infrastructure and applications that seem to be able to survive intrusions, to recuperate in the case of any problem, and to continue the transmitter functioning and satisfies its primary function even when under assault. Cybersecurity is a constantly evolving field. The distributed power infrastructure is organized by transfers and a SCADA system. Consistent updates are essential for these devices and systems to be safe and reap the benefits promised by the dazzling lattice.

(Gaoqi Liang, 2017) Cyber security for today's military systems be a relatively novel region of study. In this research, suggest a new kind of topology assault, one that disrupts the operation of intensity systems and is brought about by false information infusion attacks (FDIAs). Three different types of topology attacks are presented, including line extension, line expulsion, and line swapping. The suggested cyber topology assault affects financial activity and system security by legally questioning the dynamic process of the Independent System Operator (ISO). Suggest two types of assault scenarios, one aimed at inflicting financial harm to the infrastructure and its consumers, and another at compromising the safety of transmission lines. The suggested attack models are understood with the help of NAA and DE computations and MOEA/D. The line-exchanging assault, which has not been discussed in the literature, has been shown in simulations to have much more severe negative consequences than the line-expansion attack or the line-expulsion attack.

(Harbinger Singh Lallie 2018) put up an argument for It may be a challenging task to detect and identify cyber intrusions. Although this issue is well-documented and generally anticipated, more robust approaches are desirable to aid in attack monitoring. However, no precise or relative research evaluates the efficacy of attack showing procedures (AMTs), along with inadequacy branches and threat graphs that may be diagram is an instrument that can assist with attack detection.

(Nasser R. Sabar 2018) Cyber-crime in the presence of big data sets is well recognized as a challenge for the exploration network. It has been suggested that AI computations could be able to help with the massive information security challenges now facing the world. Support vector machines (SVMs) are one kind of algorithm that has made great strides in solving many kinds of ordering problems. However, to construct an effective SVM, the client must describe the optimal SVM setup in before, which is a difficult process that needs specialized knowledge and a significant number of human labors for validation. To solve this problem, conceived the SVM arrangement procedure as a bi-target advancement challenge, whereby accuracy and model complexity is seen as competing goals. The suggested hyper-heuristic framework is effective in addressing the bi-target enhancement problem. Disintegrational and Pareto-based strategies for dealing with complex systems are included in the framework. Two occurrences representing the gold standard of cyber security challenges have been used to test our system. Large data ordering and anomaly detection for Microsoft malware.

(2019)Cai X., Cai J., and Chen J.., Journal of Parallel and Distributed Computing, The suggested system's operation is divided into four phases: clustering, outlier identification, security maintenance, and secured routing. Finally, there are three subphases that make up the secured routing phase: the computation of trust, encryption and decryption, and authentication. Effective judgements regarding cluster formation, security analysis, and routing have been made using fuzzy temporal rules that have been created.

(Adam Gauci 2017) cyber-attacks represent a greater threat of blackouts now that they have been recommended for the new connected parts within the DSO's system and immediately available powerlessness data on the Internet. DSOs need to implement a security association and use dynamic security forms to assist reduce risk and the attack surface for cyber threats. The technique being analyzed here requires regular upkeep and this test will show that. Their assessments of security have led to the creation of cyber security heat maps, which show and describe where certain benchmarks have been met. Upgrade the electronic basic resources life-cycle board and transition to Supported and made sure about renditions of parts with the help of the current plan, which provides a structured evaluation and remediation strategy for going into a prudent security circle and logically moving from an uncontrolled security state to an increasingly controlled security state. Put all of the data you can about cyber security threats into a heat map.

(Fardin Abdi 2018) There are rigorous security requirements for the actual physiological structures which comprise Cyber-Physical Systems (CPS), and persistent assaults include shown that breaches may cause damage to these plants. Once the stage is compromised, how to protect the physical infrastructure. Alter the system so that an adversary can't immediately cripple the plant, which is important because of physical delay. Provide a framework for comprehending attacks on embedded control devices that protects physical plants while in the line of sight of adversaries. Moving toward a physical plant from an offered condition to a dangerous state isn't fast and sometimes takes limited time because of the physical dormancy, even with complete malicious management.

(Lu-Xing Yany 2017) experts believe that advanced persistent threats (APTs) pose a real danger to the network since they disable the standard safeguards against cyberattacks. This study addresses the issue of how to evaluate cyber system security in the face of APT attacks. Theoretical analysis demonstrates that this framework permits an overall stable equilibrium. Based on this concept, advocate using a different security measure called harmony security. Hypothetical analysis or computer replay reveals the impact of certain events on harmony security. A cyber system's harmony security has been investigated, along with the impact of a few parameters. The estimate of the harmony security takes just a few examples of information on the system state and does not need any knowledge of the model, suggesting that it ought to assess the protection of actual enterprise networks using APT’s.

(Haris M. Khalid 2015) Bayesian-based estimate channels have been developed and shown to make observational applications more resistant to data-infusion threats. The calculation's ability to make foresightful allocations has let us see the effects of force wavering even in the face of a data disaster. (Guohua Wang 2019) Data and communication security devices have been widely distributed as a result of the need to ensure the integrity of sensitive information inside a network. Managers analyze the data collected by security devices to determine whether an attack is in progress or if there are any other unusual aspects to the current state of the system. Nevertheless, if the first observational data gathered by integrated control strategy that integrates equipment is manipulated with by the attacker, integrated control strategy that integrates intelligence will commit an error and prolong the best time to undertake protective operations. It also provide a double-check method for validating data that relies on both numerical variables and geometric sequences. The initial data on a security device was generated using an unconventional approach and a covert social-level method.

(Jianing Li 2018) Deeply integrated data and communication technology (ICT) developments only provide highly developed impose system better perimeter consciousness, enticing dynamically facilitation, and premier P&C to improve organizational trustworthiness and sturdiness. To deal with the dangers significantly affecting the current technological P&C process, a method of cyber defense verification is warranted for mechanics P&C equipment. The P&C architecture may be tested frequently using the customizable HIL analytics tool to assure upcoming dependability, predictability, and privacy. Ahmed AlB and ElS. Ayman (2018) Hierarchical routing protocols, which rely on LEACH protocol to improve its performance and lengthen the lifetime of wireless sensor networks, have developed a new technique for cluster head selection in LEACH protocol for wireless sensor networks. Node rank algorithm boosts throughput, delivery packet ratio, and sensor lifetime while lowering packet delay and power consumption.

(Jie Lin 2016) mist/edge registering may provide a faster response and a more prominent character of administration for IoT applications, as advocates have suggested. This means that haze/edge processing combined with IoT will be the next-generation framework for IoT advancement. These applications include smart lattice, smart transportation, and smart urban communities. Structures, enabling developments, security and protection challenges, and the combination of mist/edge registration and IoT to support various applications are all part of a thorough examination of the IoT technology that has been presented. To be more specific, the connection and differentiation between IoT and CPS have been outlined at the outset. Both standard three-layer engineering and provider architectural style four-layer engineering have been suggested as viable Internet of Things architectures.

(Md Masud Rana 2018) have suggested the sharp lattice as a state-of-the-art power framework for revamping the standard network to enhance its safety, availability, efficiency, and maintainability. Unbelievably, the sophisticated framework is vulnerable to malicious cyber assaults that may cause authentic, specialized, affordable, social, and control concerns in power arrange duties. In this research, offer a robust approach to state estimation and input control computation in a brilliant system, intending significantly reduce the platform's vulnerability to cyber-security threats. It is suggested that the framework states adopt an excess insurance approach for cyber-attacks, using a coded RSC. When the received signal is contaminated by noise or cyber assaults, Log-MAP decryption may be used to recover the original state of the system.

(Yu A 2019) put up an argument for, In today's widely used cyber-physical systems (CPS), accurate estimate data is crucial to the functioning of the robotization control process. However, cyber assaults against CPS may manipulate the estimates and trick the control framework into making poor operational decisions. Currently, the examples of two distinct types of cyber assaults (ephemeral and persistent attacks) along with the attack plans for each. A multivariate Gaussian-based strangeness detection method is offered as a means of effectively and accurately identifying these fake information injections. To differentiate between fleeting and persistent cyber threats, develop a multivariate Gaussian-based inconsistency detection technique. By establishing connections between different aspects of estimate data, multivariate highlights are produced. Specialists define an operation possess happened once the frequency of a cyberwar incidence in the multidimensional Linear model is under a predefined level.

(Jiankun Hu 2016) put up an argument for the use of semi hydropower with greater performance benefits and indeed the introduction of vitality have been accomplished thanks to the limited availability of petroleum products and the need for economic conditions. By fusing cutting-edge data and communications technologies, the "savvy matrix" is a promising new development that has the potential to fulfill such needs (ICT). Large volumes of data on vitality volume, velocity, and variety will be generated by the inevitable structure of advanced ICT, especially smart metering. In addition to resolving the traditional 3Vs problems associated with very large data sets, ensure the strong cyber-physical connection that serves as one of the sharp lattice's most prominent features. Suggested a scientific categorization based on energy-related big data to better grasp the intricate and fascinating interconnections between various components, security concerns, and associated arrangements.

(Pengfei Hu 2017) put up an argument to ensure that people's identities online and offline are consistent, innovations in face distinguishing proof and aims are essential. As the IoT grows in popularity and Big Data comes a corresponding increase in the need for computational, communicative, and storage capabilities, as new applications rely more on facial recognition evidence and end objectives. Thus, to enhance the preparation limit and spare the data transmission capacity, offer the haze registering based face distinguishing proof and aims structure. This study expands upon our previous work by addressing the safety and privacy concerns raised by the haze figuring-based facial recognition proof and objectives structure suggested. Preserving identity documents and facial features is a priority, hence measures for their safety and preservation have been recommended.

(Hoon Ko 2019) have suggested that there are a plethora of online publications dedicated to recommending restaurants and cafes. Furthermore, other forms of fake news spread false information and statistics. Both are the work of a blogger, who is free to write about whatever interests them. Online visitors check these reviews to see whether a restaurant or other dining establishment is appropriate. It seems the blogger's bias has a role in the decision. Since the blogger's personality dictates all the decisions, this cannot be considered objective. Poor bloggers hurt the number of people who live in and visit a place in search of good dining options. There is a risk of confusion caused by this unreliable information. Recently, several bloggers have begun posting praiseworthy comments that agree with a local business desire of the proprietor this might result in blog postings that exaggerate the severity of the problem, make sweeping generalizations, and repeat themselves endlessly.

(Kuai Xu 2008) cyber assaults and the steady growth of applications that impact Internet traffic components have suggested that it is essential to develop practical ways for isolating and comprehending meaningful Connections in Web traffic information can be used to organize and strengthen information security. Right now, provide a broad strategy for creating in-depth behavior profiles of spine traffic on the Internet, complete with illustrative uses and advantages. Given recent cyber assaults and the proliferation of new and complex apps, extracting meaningful events from massive amounts of Internet information has assumed fundamental importance.

(Saurabh Amin 2013) This brief proposal seeks to carry out a security risk assessment of a structured control system with supervisory and managerial levels of control, investigate the existence of a model-based demonstrative plan (supervisory layer) and a relative fundamental controller (administrative layer) under a set of deceptive assaults. Choose a moderate approach by assuming the attacker is aware of 1) the framework components, 2) the parameters of the demonstration plan, and 3) the sensor-control signals. This new double-dealing technique paves the way for automated channel systems to be hacked remotely, allowing for the theft of water supplies. Results from a field operational test of the Gignac water SCADA framework were presented, and conducted a security risk analysis of a progressively structured water SCADA system. Analyzed how covert double-cross assaults may affect a PI control scheme (at the managerial level) and a UIO-based analytical strategy (supervisory layer). In both strategies, estimates from downstream sensors were used.

(Yingshuai Hao 2016) Internet information assaults have been presented as the worst-case scenario for coupling bad data with control framework state estimation, and they are not detectable using currently available bad data indicators. This research specifically explores the possibility of cyber security information assaults by showing a hostile assailant's acts in an odd context, where another sovereign of the power framework evolves and estimating devices may become inaccessible as a result of unique attacks. If the administrator wants to know how vulnerable the intensity system is to cyber assaults, then they need to do this analysis. Simply put, this article explores the likelihood of cyber information assaults on control systems. Using a Markov Decision Process, simulate an intruder's attack steps (MDP). The likelihood of an attack is analyzed concerning the ideal attack tactic that an intruder has learned.

(Nong Ye 2004) Introduce the usefulness of the Markov-chain concept for detecting cyber-attacks via discussion and practical examples. The presentation of intrusion detection relies heavily on the type of movement information to use the Markov-chain process and other stochastic procedure approaches to illustrate the sequential requesting of instances.(Gideon Creech 2014) put up an argument for the creation of a host-based unusual intrusion localization framework is notoriously difficult because of the alarmingly an increased incidence of wrongful convictions This study proposes a novel server abnormality incursion localization method that makes use of a discontinuous framework called architectures.

## 2.3 Existing works of Intrusion Detection System

(Zubair Md. Fadlullah 2013) Despite claims that CRNs may help solve the problem of limited radio bandwidth; current implementations are vulnerable to security flaws. Few experts have recently investigated using intrusion detection systems (IDSs) to combat these threats against CRNs. Currently, please give an example of a CRN depending upon IEEE's WRAN and considering slew of vulnerabilities organization encounters. The need for a well-planned intrusion detection system in the fight against assaults on intellectual radio systems was highlighted. Developed relatively straightforward however efficient ID that can be applied in the auxiliary customers' mental radio. One of the unique features of our proposed IDS is the use of a non-parametric CUSUM computation to pinpoint instances of anomaly.

(Izhar Ahmed Khan 2019) have stated that dealing with asymmetric intrusion datasets, such as when one class is denoted by a smaller number of cases, is the acid test for designing an intrusion detection system (minority class). As a result, devise a plan to control this problem and suggest an anomaly-finding technique for the ICS. In our proposed method, make use of a mixture a concept which benefits from predetermined as well as designed nonverbal signals typically happen amongst grounding components in Industrial control systems. To institutionalize and scale the data, First used certain preprocessing techniques. Our proposed method for ICS-explicit system oddity detection sequentially combines a Bloom channel-based parcel-level irregularity discoverer with a time-arrangement-level variance from the norm indicator.

(Chunjie Zhou 2015) put up an argument for As a result of their high flexibility, interoperability, and easy organization, data correspondence innovations are being increasingly used in the field of industrial process robotization. Nonetheless, it also sets in motion new security threats to present and future systems. To better guarantee safety, intrusion detection has emerged as a significant technological advancement. The reality is that the intrusion detection methods often used in the IT sector are not practical for robotic process automation. Currently, models are created by carefully exploring the multi-space data on field control layers in mechanical process mechanization from the perspectives of both material science and data.

(Jiong Zhang 2008) It is absurd to believe that the latest security innovations can prevent all security breaches. Therefore, detecting the location of an incursion is a crucial part of any security system. Many contemporary systems that detect intrusions (IDSs) are, though, commandment solutions, making it difficult for them to spot new types of attacks. As an added downside, encoding rules are time-consuming and heavily rely on data on previously discovered security holes. Therefore, suggest new effective structures for IDSs based on misuse, inconsistency, and half-and-half systems, which make use of a computation from the field of information mining known as irregular woods. In the field of abuse detection, samples of incursions are collected in a sequential fashion using an ad hoc method of computation in the wild.

(Song Han, 2014) have proposed CPS shows remarkable promise to be the central foundations of the cutting-edge enormous scope smart system, which has been identified as a need, investigate territory. Because of characteristics unique to CPS, such seeing that its massive level, decentralized organize and governance, practicality, and number of variables, new challenges should arise in ensuring CPS reliability and security. Some effort has been put into thinking about ways to keep CPS against getting harmed misused by cyber assaults and erratic disappointments, and intrusion detection has been considered a crucial tool for doing so.

(Hichem Sedjelmaci 2017) To yet, research on systems for unmanned aerial vehicles (UAVs) has been scant. Because these systems transmit vital information, they are subject to a wide range of risks, and security is a top priority. Now is the time to build and deploy a revolutionary intrusion location and response mechanism that can detect malicious discrepancies at the UAV and ground station levels. Current proposals include a series UAV characteristics are analyzed using threat detection algorithms, which classify them into the proper categories (ordinary, aberrant, dangerous, and harmful) according on the type of cyber-attack that has been discovered. In this study, investigate the most hazardous cyberattacks that might affect a UAV setup, such as false data dissemination, GPS spoofing, sticking, dark gap and dim gap assaults.

(Khalil El-Khatib 2010) When it comes to preventing intrusion detection systems, illegal accessibility to our program's capabilities are a crucial first line of defense. Classifiers are often used as identifiers in intrusion discovery models, particularly in inconsistency detection models. If you want to guarantee the presentation, speed of learning, accuracy, and dependability of these indicators as well as to eliminate noise from the arrangement of highlights employed to form the classifiers, then you need to make sure you choose the right arrangement of highlights. Current system highlights used for creating and testing the intrusion detection system consist mostly of basic data identifiable with the TCP/IP header, with little to no consideration given to the highlights associated with lower-level convention outlines.

(Nikos Tsikoudis 2013) Much attention has gone into the creation and operation of low-power systems during the last decade. It began with battery-powered computer servers and mobile phones and has now moved to other essential network equipment such as switches. However, the rising demand for a reduced framework arrangement has not been included into surveillance equipment, which is critical in today's society. As move forward, want to eliminate the need for Intrusive internal communication system for intrusion detection are already being implemented to enhance the security of contemporary networks. Regrettably, conventional techniques to reduced proposed framework, such as recurrent scaling, unevenly enhance bundles manipulation and alignment times.

(Mohammed Hasan 2017) A supervised intrusion detection system is an IDS architecture that may learn from attack models to detect new threats. As ANN can learn from real-world models, its use in intrusion detection holds promise for reducing false negatives and false positives. Currently, a novel FLN learning system based on PSO (particle swarm optimization) has indeed been proposed and named PSO-FLN.

(Hyun Jin Kim 2011) This research offers an experience equal string coordinate scheme for the lowest effort instrument-based intrusion discovery system. To reduce the number of transitions between states, a string matcher uses bitmap graphics embedded in its finite state machine tiles. To deal with deterministic limited automata, long objective instances are broken down into smaller, uniform patterns. Memory use in homogeneous string matches may be optimized by limiting the range of target design lengths via example partitioning. A two successive coordinating plan is provided for the progressive matches with sub patterns, which will allow for the identification of each lengthy example being partitioned.

(Iftikhar Ahmad 2018) Intrusion detection is a crucial component of many types of security technology, including firewalls, IDSs, IPSs, and other intrusion prevention systems. There are a variety of intrusion location methods in use, but how they are presented might be confusing. The success of intrusion detection depends on its accuracy, which must increase to reduce false positives and boost the discovery rate. Multilayer perceptron, Support vector machine (SVM), and other methods have been used in recent work to identify execution-related concerns.

(Rossouw von Solms 2013) The terms "cyber security" and "data security" are commonly used interchangeably with one another. Even though there is a lot of overlap, this study argues that cyber security and data security are not the same things. Furthermore, the study argues a certain information technology goes than what is traditionally covered by user privacy by protecting not just digital products however also the confidentiality about other systems, such people. When discussing data security, the term "human factor" often refers to the individual(s) involved in some capacity inside the security process. Taking into account human beings as cyber-attack targets or even unwitting participants is an additional dimension of cyber security.

(E. Kritzinger 2010) they now live in a time where network which includes use is part of the routine to a wide spectrum of people. Companies turn to the Internet for something like a broad range of electronic interactions, and a growing number people are accessing it online services from their homes due to the numerous benefits it offers. However, increased Internet dependency and use presents new and possibly severe hazards. This is owing to the attempts of undesirable outsiders to get unlawful access to private information, which has resulted in an increase in cybercrime overall. As a result, it is It is crucial that all Online users comprehend the risks associated with internet access, the significance of preserving the confidentiality of data, and the penalties of failing to do so.

(Kaikai Pan 2018) Accurate security and recovery procedures can't be designed without first understanding sophisticated matrix cyberattacks. Propelled assaults attempt to increase influence while decreasing costs and they may pinpoint a target's capacity. This study offers a random analysis of combined information credibility and availability assaults on state estimation in the force framework. Compare and contrast consolidated assaults with pure uprightness attacks, often known as false data infusion

(FDI) attacks. As a mixed-number direct programming problem, suggest and provide a protection recording when assessing susceptibility with those various threat kinds. Demonstrate that coordinated assaults may be successful with fewer resources than traditional FDI attacks.

(Longjie Li 2017) Intrusion detection has been a crucial defense mechanism against malicious assaults on processing systems. In this research, propose a two-pronged half-breed technique reliant on parallel characterization and the k-NN process to enhance detection execution and reduce susceptibility to visit assaults. In the first stage, certain classes of system relationships are identified using a small number of two-fold classifiers and a single collection module. Associations with doubtful class memberships are sent to Stage 2 for further classification determination using the k-NN algorithm.

(Yihan Xiao 2019) However, they have problems such as a high false alarm rate (FAR), weak speculative ability, and low practicality, and they don't eliminate the trademark data of customer practices. Currently, offer a model for system intrusion discovery that makes application of a deep neural network for (CNN–IDS).

(Waleed Bulajoul 2019) It has been suggested that current network intrusion, identification, and avoidance systems (NIDPSs) have certain limitations in spotting or preventing growing undesired traffic, as well as some risks in real-time environments. This demonstrates that the NIDPS's performance may be subpar in the face of quick and high-load malicious traffic, as shown by package drops, exceptional bundles that go unchecked, and a failure to recognize or prevent unwanted traffic. The intrusion detection and avoidance implementation is a monumental feat of administrative (QoS) engineering.

(Xiujuan Wang 2016) has put out Designed to work in tandem with firewalls, intrusion detection aims to identify malicious activity. It can detect malicious system communications that use attack methods that are undetectable by standard firewalls. Artificial intelligence manages a variety of intrusion detection methods. Evidence from the literature suggests that a joint learning or coordination method for presenting an incursion locating technique is preferable to lone learning innovation.

(Fangyu Li, Yang Shi 2019) have suggested that the IoT is defenseless to both cyber and physical assaults. Therefore, it is desirable to have in place cyber-physical security architecture capable of repelling a wide range of threats. As a rule, attackers may be identified by looking into framework logs. Framework logs, however, such as organized insights and access records, may be generated. Moreover, current safeguards are mostly geared at protecting against cyber assaults. This study suggests the first IoT monitoring gadget based on the inspection and analysis of vital signs. To the best of the researcher, it is the first endeavor to discriminate between electronic and physical assaults within the Internet of Things using power analysis. Utilize data from energy meters to build a machine learning modeling approach that could also adapt to various conditions. (Timmy Schuller 2018) Expanding traffic demands are used to test Internet service providers. One strategy for passing this exam is called Propelled Traffic Engineering (TE). When it comes to TE, the concept of Portion Routing (SR) is rather new. Whether or not SR is an effective strategy for such organization in bearer IP spine systems depends on whether or not it can demonstrate its benefits in certified instances while still being believable from the standpoints of system activity and the board.

## 2.4 Existing works of Systems for detecting attacks and Mechanism for preventing attacks

(Majjed Al-Qatf 2017) When compared to more conventional system protection advances like firewalls, Network Intrusion detection systems (NIDS) offer a more efficient approach for security risk management. Success with NIDS relies heavily on being able to publicly display the computations and improvement approaches used to increase the precision of the characterization and decrease the time required for their development and testing. Introduce the STL-IDS deep learning approach, which is founded on the architecture of self-taught learning (STL).

(Adel Binbusayyis 2019) have suggested that an intrusion detection system (IDS) may serve as the last line of defense against cyber threats and contribute significantly to protecting the security of IT funds and facilities. There is currently no conclusive study that addresses the challenge of extracting useful information from massive amounts of organized traffic data used for IDS.

(Haitao He 2019) To ensure the safety of sensitive system data, a network intrusion detection system (NIDS) is a crucial piece of equipment, and in recent years, neural systems have emerged as the solution of choice. However, when the system situation becomes more unpredictable, present arrangements based on the ordinary neural system are unable to make advantage of the wealth of information contained within network data as a result of their monolithic nature. More importantly, the current NIDS will clearly have no knowledge of the infiltration location space, leaving it incapable of achieving a high detection performance and great soundness in the new circumstance. (Lin Wang 2007) Increasing utility devices' connection to external systems raises serious security and reliability concerns for utility computer networks. This exacerbates the Utilities equipment' susceptibility to cyberattacks via connectors.

(Selcuk Cevher 2018) To reliably support real-time communications, Software-Defined Networks (SDN) must be able to quickly recover from information-plane disruptions caused by unforeseen circumstances. The Internet Engineering Task Force (IETF) established Multi Topology Routing (MTR), which provides routing table redundancy through the processing of virtual topologies (VTs) that vary in their connection loads. For MTR-based failure recovery systems, virtual topologies (VTs) are used, with each VT assigning a high importance to a physical topological link such that it is not had been using if shorter paths exist. (Muhammad Shakil Pervez 2014) An intrusion occurs when malicious actions compromise a system's security measures. To practically acknowledge the privacy, Computer products are correctly, dependability, general usability framework, intrusion location (ID) seems to be a set of procedures towards identifying but instead interpreting unusual activity.

(Junaid Akram 2019) The global rise in cybercrime has been startling. Every sector of society that may be significant importance to a physically topological link such that it's had not been using if cheaper paths exist in its respective crime rates. The basic another goal of this study is to contrast the protection of different programming systems by analyzing their source code and fixing history. To help security professionals, organizations, and software developers maintain safety, they have developed several methods for collecting or following the Vulnerability code.

(Chen Peng 2018) Smart grids (SGs) are a kind of distributed control system designed to transmit electricity generated at several power plants across a channel of interaction for average customers. Since a vast number of electronic devices are interconnected via communication manipulates all through basic force offices, cyber security develops into a fundamental issue due to the complexity of circumstances, the dispersion of the spatial areas, and the defenselessness of the communication systems.

(Rafał Kozik 2016) have brought up the possibility of using robots to investigate the structure of Hypertext Transfer Protocol (HTTP) requests to identify cyber threats at the web layer. For the time being, suggest a machine-learned classifier be used in conjunction with an HTTP grouping computation that takes into account a variety of possible configurations. The major motivation for our approach is the fact that make use of the request's architecture and accurate estimates of its content to identify anomalous behavior in preexisting customer-server connections.

(Gaoqi Liang 2017) Increased focus in recent years has been placed on ensuring the safety of the modern power grid against cyberattacks. Intending to disrupt the operation of an intensity system, this study offers a category of cyber topology assaults derived from false data injection attacks (FDIAs). There are three potential forms of cyber topological attacks: Line-expanding, -evacuating, and -exchanging all types of attacks.

(Guohua Wang 2019) Digital security devices are widely used in the telecommunications and information industries. Infrastructure as a precautionary measure. Arrange security chairmen to analyze the data collected by security equipment to determine if there has been an attack or if somehow the platform's condition therefore at moment is unusual. However, if the first observation data acquired by the arrangement's security hardware is tampered with by the aggression, then the arrangement's protection managers should develop an incorrect evaluation and postpone the best moment to undertake precautionary measures.

(Arsalan Mosenia 2016) There has been an exponential growth in the number of cyber-physical systems (CPSs) that enable various administrations in different application spaces, such as smart homes and savvy matrices, as a result of rapid mechanical advances in microelectronics, systems administration, and software engineering. In addition, the proliferation of the IoT viewpoint has mandated the ubiquitous deployment of CPSs enabled by the IoT. (Fan Zhang 2019) Concern about the cyber security of today's control systems has been raised in light of the rising frequency of assaults on cyber-physical systems (CPSs) (ICSs). Firewalls, information diodes, and other intrusion prevention methods are now relied upon heavily in ICS cyber security efforts, however, these measures may not be sufficient in the face of emerging cyber threats from motivated attackers.

(Limei He 2017) have suggested the Long Term Evolution (LTE)/LTE-Advanced (LTE-An) framework with all of its increased data flows, it gives improved sorts of assistance for billions of customers, improved range efficiency, and less idleness in comparison to legacy cellular networks. Nonetheless, As a result of its Internet protocol heterogeneity architecture, new vulnerabilities emerge. Consequently, LTE/LTE-A system security assessment must be carried out swiftly and precisely. (Ahmed S.2017) The accuracy of computerized estimates is crucial for the monitoring and management of electrical force systems. These refined estimates are reflective of the precision of the newly installed sensors, which are vulnerable to the introduction of unknown variables such as device failure and cyber threats.

(Farhan Ullah 2017) As the IOT (Internet of Things) continues to provide services to the organization, the associated system, applications, data storage, and services provide a potential new entry point for cyber assaults. Theft of source code and virus assaults are now major threats that might compromise the security of the Internet of Things. Large amounts of data might be stolen by these threats, resulting in monetary and reputational losses. Presently, suggested a unified deep learning approach to identify the stolen code and malware-infected documents throughout the IoT network.

(Hadis Karimipour 2019) have suggested an individual irregularity's location based on the verifiable link between estimates. The goal is to design a flexible inconsistency detection motor suitable for broad-ranging clever matrices, one that can distinguish between a true weakness, a disturbing impact, and a smart cyber assault.

## 2.5 Applications of CNN and FCNN

(Jonghoon Lee 2017) Leveraging on mimicking neural networks, a machine learning algorithm for spotting cyber risks has been developed. The suggested method employs a deep learning-based identification mechanism to better identify cyber threats by transforming massive amounts of collected security events into individual profiles. In this study, developed an AI-SIEM framework that utilizes a variety of fake neural system techniques, such as FCNN, CNN, and LSTM, and combines the use of event profiling for data pretreatment.

(Yu A 2019) These days, a typical cyber-physical system (CPS) includes a modern power distribution network, where accurate estimate data is crucial to a reliable mechanized control process. However, cyber assaults on CPS may distort logical information and mislead the management structure, resulting in incorrect led to differences. (Emna Bahri 2011) have suggested a new method for faster and more accurate intrusion detection that relies on Greedy-Boost, a multiple classifier architecture. To use information mining and AI methodologies for intrusion location, it is necessary to first identify the irregularities in the information handling systems.

(Claude Fachkha 2015) To build cyber literacy, today's Internet security infrastructure places a premium on routine web browsing. Quick, put up a critique of the underground web. The latter is a powerful approach to covertly monitoring online activities and preventing cyber threats. Essentially define the darknet, depict it, and list its alternative monikers. (Waleed Mugahed Al-Rahmi 2019) has advocated looking into the effects the effects of harassment and online harassment on academic achievement in online collaborative learning environments. Because these tools improve student learning, collaboration, and information exchange, they are fundamental to the educational process. As key motivators for open learning within the context of instruction, perceived enjoyment and practicality were also highlighted throughout this investigation. (Yumei Li 2015) have suggested the identification of numerous stochastic cyber threats centering on a control framework's multiple communication channels. Under various cyberattacks, likely structure a locator for the control framework. An algorithmic discovery strategy is provided in light of the recurrence area change system and the auxiliary location instruments.

(Patricio Zambrano 2019) have identified practice as a vulnerability in social infrastructure and data protection. This will allow for supporting investigations connected with recognizing instances of spiteful behavior on the web, and the exhibiting of points will allow for the resolution of distinct phases or times in a lifecycle of preparation linked to social construction. In addition, presented a conceptual and nuanced profile of the specific sort of offender that engages in online pedophilia.

(Randy C. Paffenroth 2019) Denial-of-service (DOS) attacks aim to prevent users from accessing intended resources on a computer system. DOS attacks are difficult to detect and stop because they don't often target private information but rather disrupt the freely available resources that their intended victims provide.

(Hongyan Li 2019) Data reinforcement and recovery strategies like Continuous Data Protection (CDP) are becoming more popular in the realm of Cyber Security. When compared to conventional data backup and restoration techniques, it provides much-improved reliability and lets you restore the status of your data to any previous point in time. CDP continually collects and records each plate update, providing a large measure of data, thus urgently wants a competent instrument for sorting out such data (about the circle I/Os) to guarantee the presentation is worthwhile.

(Amol Borkar 2017) Here, describe some of the suggested techniques that have been developed to detect gatecrashers. These characteristics may be used as part of a continuous framework for future IDS design, allowing for easier identification of malicious insiders. This will be a genuine IDS that may be used by certain companies, MNCs, to protect their sensitive data from intruders on the inside.

(Gong Shang-fu 2012) As vulnerabilities in the system become more apparent, protecting the framework and the assets it contains becomes a pressing concern. Distinguishing (ID) interruptions is now a major area of study. Due to the assist vector machine's (SVM) strong speculation capacity, high arrangement accuracy, and such advantages in practice, which includes little illustration, and high measurements, will mostly focus on contemplating and concluding the SVM methods in a barge in distinguishing.

(Ahmad W 2016) A To identify attacks, a decentralized intrusion detection systems (IDS) are recommended topologies for a remote organizational control framework are focused on a small number of cyber-attack scenarios. More specifically, this research proposes a visual layout a mathematical technique for developing and implementing the IDS, in addition to the shuttered controller integrating the IDS.

(Hichem Sedjelmaci 2017) Thus far, unmanned aerial vehicle (UAV) systems have not received substantial funding for the study. Particularly worrying is the fact that such systems are vulnerable to a wide variety of assaults precisely because they carry such crucial data. To detect cancerous anomalies that weaken the system, Create and put into action a special intruder identification and responding scheme that works at the central controller and UAV echelons.

(Antonia Nisioti 2018) have proposed that current IDSs go beyond simply finding to include causality and attribution. Provide commentary on how information collected by IDS may be repurposed and linked to identifying attackers utilizing cutting-edge approaches to data investigation and analysis. Then, argue that the existing IDS threat classifications might be expanded to include the latest violent attacks and propose three new types predicated on the proportionality of the inverting amplifier.

(Adel Binbusayyis 2019) The success of an ID relies heavily on various data points. To date, there hasn't been any conclusive research on how to best select informative highlights from organized traffic data for IDS.

## 2.6 Conclusion

This chapter has covered a lot of ground, including a literature review of IDS varieties, approaches, and technologies, as well as their benefits, uses, and potential future restrictions. While this strategy may be effective, it comes with the potential drawbacks of a high false-alarm rate and the time and effort required to develop and update information on new threats. In this paper, summarize the findings of prior studies and show the techniques used in the current state of scenario generation as a means of addressing challenges in the intrusion detection system. Additionally, the most well-known and often utilized research datasets have been explored, together with their associated jargon, methods, estimated outputs, and limitations.

# CHAPTER 3

# IDENTIFICATION OF INTRUSION ATTACKS (DDOS AND WORMHOLE ATTACKS) OVER WSN

## 3.1 Introduction

Detecting intrusion attempts like DDOS (Distributed Denial of Service) and Wormhole attacks in a Wireless Sensor Network (WSN) can be challenging in terms of resource-constrained nature of sensor nodes. To recognize these assaults, there are a number of tools and procedures that can be used. Implement real-time algorithms for identifying anomalous energy use trends. These algorithms can use statistical techniques, such as threshold-based or statistical outlier detection methods, to identify significant deviations from expected energy levels. Sudden spikes or drops in energy consumption may indicate the occurrence of an intrusion attack.

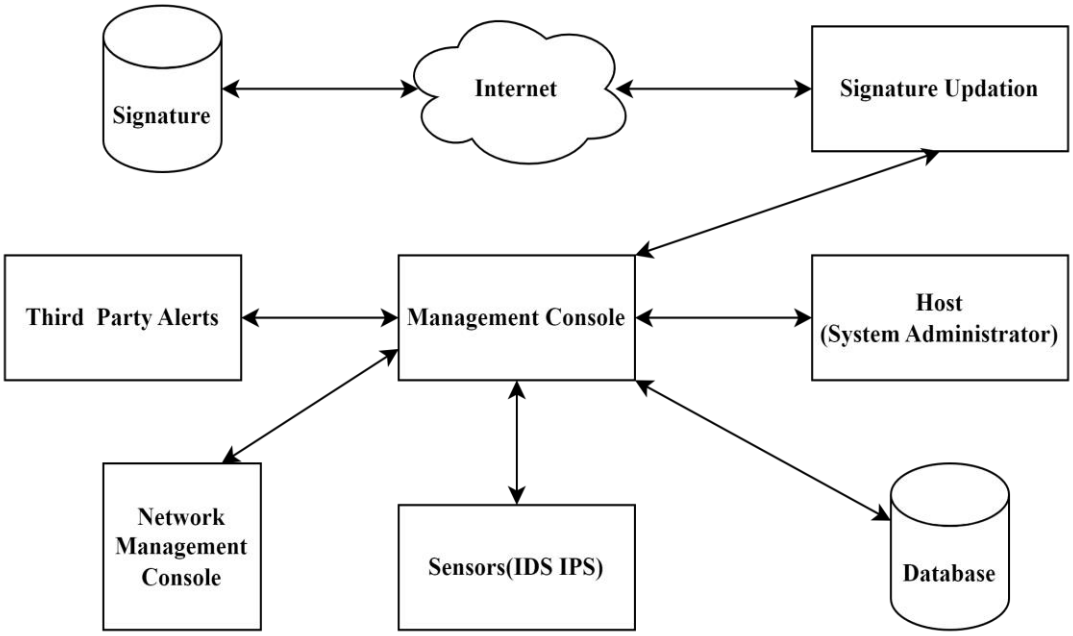


**Figure 3.1: IDS system architecture and framework, appliance**

Intrusion Detection system has been a huge activity to assurance of computer network systems from unauthorized attacks is shown in Figure 3.1. Intrusion Detection System is a major part of detecting and identifies the attack it may be occurs in the computer networks [11]. It becomes a necessary instrument for maintaining a trustworthy and safe information system. The performance of the various intrusion detection techniques is an issue. Accuracy is a key factor in intrusion detection performance, which must be increased to lower false alarm rates and increase detection rates. These methods demonstrate its shortcomings and perform well with sizable datasets, such as network and system data.

The EE-IDSEP, which consists of an improved watchdog system and a Hidden Markov Model (HMM), is created to detect this attack in the ZigBee WSN. The optimised watchdog mechanism is employed to keep an eye on the node's operations. The Hidden Markov Model (HMM) is used to forecast the rate at which sensor nodes lose energy. The remnant energy from the monitored nodes are collected by the watchdog nodes. It also calculates the reported residual energies, actual energy consumption and contrasts it with the HMM's anticipated values for this quantity. DDOS attacks are thought to be nodes with abnormally high energy usage.

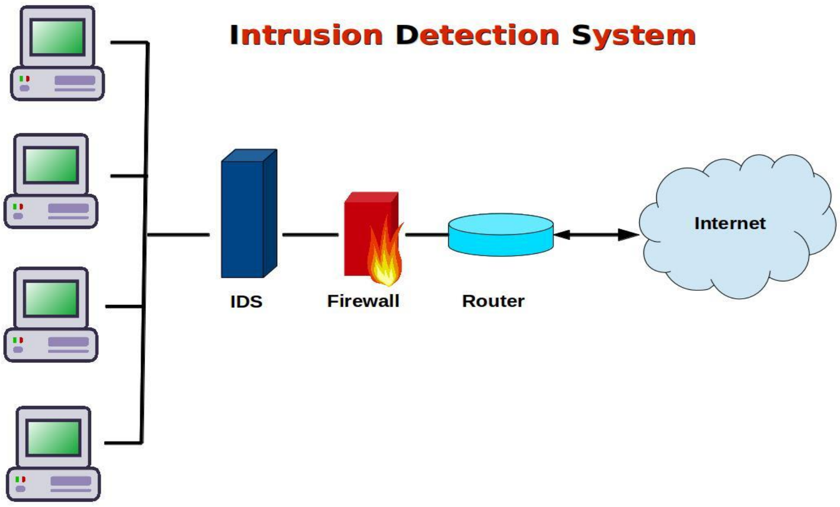


**Figure 3.2: Basics of Intrusion Detection System and classification**

In Figure 3.2 the Intrusion Detection System in a Wireless Sensor Network is to enhance the security and reliability of the network by timely detecting and responding to potential intrusions, minimizing the impact of attacks, and ensuring the integrity of the collected data. The main source of security breaches is intrusion, which poses a major security risk since it can quickly steal or destroy data from a PC and network system. An incursion may potentially harm a system's hardware. Additionally, penetration might impair IT core infrastructure and result in significant financial losses, which would make data inadequacy. Therefore, it is essential to identify intrusions and to prevent them. Although there are various intrusion detection systems, accuracy is still a problem because it depends on detection and the false alarm rate. The Intrusion Detection Systems (IDS) is a system that can identify hostile nodes and then quickly notify surrounding nodes to take the necessary precautions. The most common IDS is trust-based IDS, which utilises watchdog [4-5] to monitor network behaviour to find rogue nodes. A key element of the trust process in WSN safety is the watchdog. The watchdog, however, consumes a lot of energy, which reduces the network's lifespan. For existing security methods to identify intruders, more power and memory are needed. Therefore, they are not appropriate for networks with limited resources. The results show that the proposed methodology is focused.

The performance of EE-IDS is evaluated using AODV, STR, and OSTR as three different routing protocols. In addition, EE-IDSEP is developed to recognize DDOS attacks, and other IDSEP performance metrics are examined. The core of both EE-IDS and EE-IDSEP is the optimised watchdog system, a trust-based intrusion detection technique that identifies hostile nodes to watch over the behaviour of the nodes within its communication range. Due to their inherent qualities, such as being extraordinarily steady, the nodes chosen to serve as the watchdog node are the most reliable nodes. Like every other node in the network, these watchdog nodes are scattered at random. The detection time, False Positive Rate (FPR), average end-to-end latency, Packet Delivery Ratio (PDR), and energy consumption will be measured nodes.

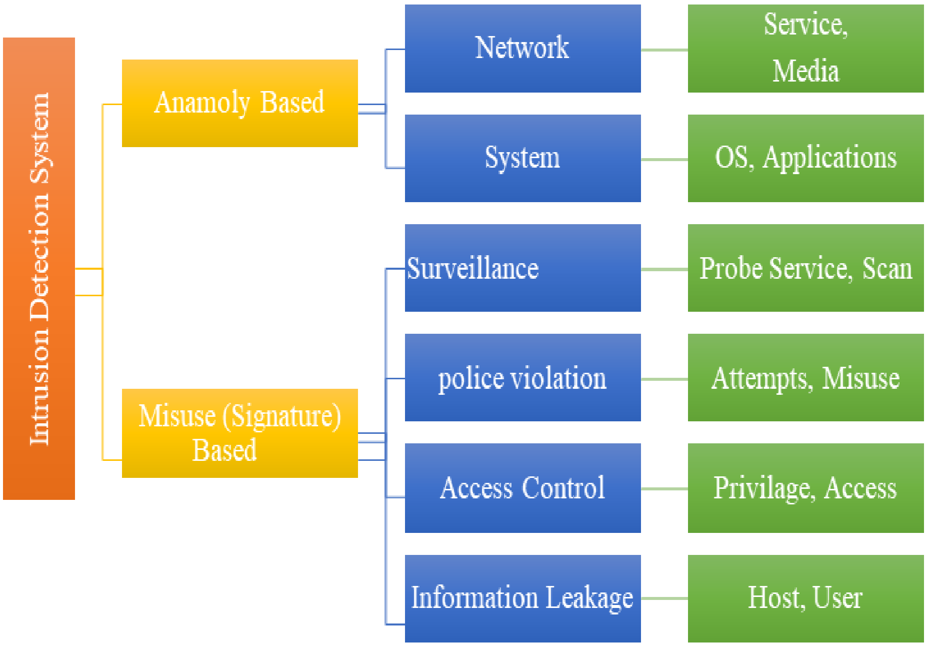


**Figure 3.3: Comprehensive framework of Intrusion Detection System`**

In Figure 3.3 the comprehensive IDS framework is to enhance the network and system's security posture by detecting intrusions, anomalies, and malicious activities promptly and accurately. It helps to protect sensitive data, prevent unauthorized access, and minimize potential damages caused by cyber threats. Additionally, a well-designed IDS contributes to incident response, threat intelligence analysis, and continuous improvement of the overall security infrastructure.

## 3.2 Overview of Intrusion Detection System

IDS is a term used to describe software or hardware systems that employ machinery to examine events occurring in a system or network and look for signs of security issues. A modern network security technique called intrusion detection is used to identify and stop unauthorized access to computer networks. Figure 3.4 illustrates the crucial function intrusion detection systems (IDS) play in ensuring a safe and secure system or networks [75]. A series of techniques known as anomaly-based intrusion detection systems make it challenging to assess whether network traffic is more anomalous than usual [10]. Performance of an intrusion detection system is dependent on how well it can maximize detection accuracy while minimizing false alarm rate [93]. To the fact that intrusion can also damage system hardware, it is a serious security concern and the most significant factor in security breaches. Additionally, intrusion can result in severe financial losses and compromise IT key infrastructure, which leads to inadequate data. However, accuracy is dependent on detection and the incidence of false alarms, leaving a problem with precision.

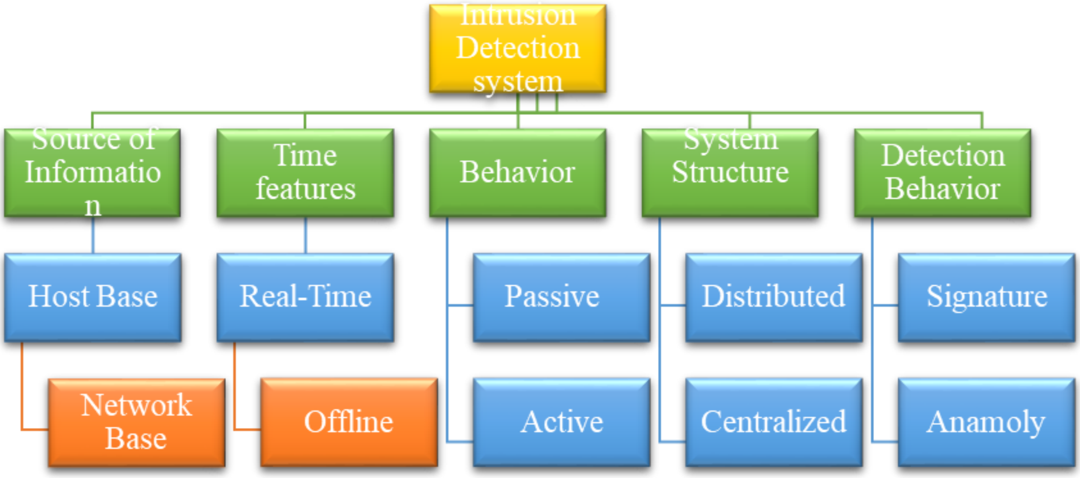


**Figure 3.4: Classification of Intrusion Detection System**

Investigative the bundles, IDS recognize anomaly practices and pieces malignant relations from attackers are shown in Figure 3.5. At the end, intrusion detection methods are arranged as abuse-based detection and abnormality construct location based on the analysis's design. An intrusion is distinguished by an abuse-based recognition framework by coordinating it with specified marks. As a result, when creating an abuse-based recognition system, attack profiles are necessary. It consistently detects existing system assaults with a low false alarm rate, but new attacks elude detection because of their masked signatures. In figure 3.4, the classifications provide a basis for understanding the different types of IDS used in Wireless Sensor Networks and help in selecting the appropriate intrusion detection strategy based on the specific requirements and constraints of the network environment.

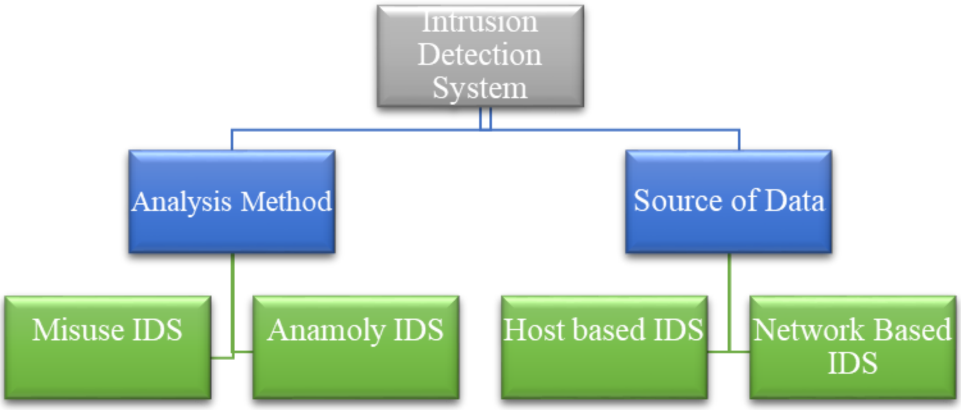


**Figure 3.5: Block Diagram of Basic Intrusion Detection System**

However, peculiarity-based location frameworks can identify an assault by spotting the departure from usual behavior. Contrary to abuse-based frameworks, consistency-based frameworks are likely to detect mysterious infiltration techniques. Despite the fact that they may suffer from a high false alert rate, irregularity-based, detection frameworks have become increasingly important in guaranteeing system security as new attack strategies keep emerging. Recently, with the enormous efforts of experts, Figure 3.5, irregularity construct detection frameworks based on information mining and proposed techniques have been suggested to provide accurate detection results.

## 3.3 Types of Intrusion Detection Systems

### 3.3.1 Network Intrusion Detection System– NIDS

NIDS, consistently known as Network based Intrusion detection system, are definitely not hard to make sure about and can be progressively difficult for an aggressor to detect [34]. Given the huge amount of data that arrange intrusion detection system need to analyze, they do have a reasonably lower level of identity [62]. This suggests they may miss attacks in progress, normally can't separate scrambled traffic on the computer system, and may require logically manual relationship from administrator. Figure 3.6 represents the NIDS may similarly be genuinely needy upon an excess of interest [35]. At the point when a NIDS is eagerly following an even on a system attempting to perceive whether it is an attack, various events may be permitted a lesser degree of consideration [38].

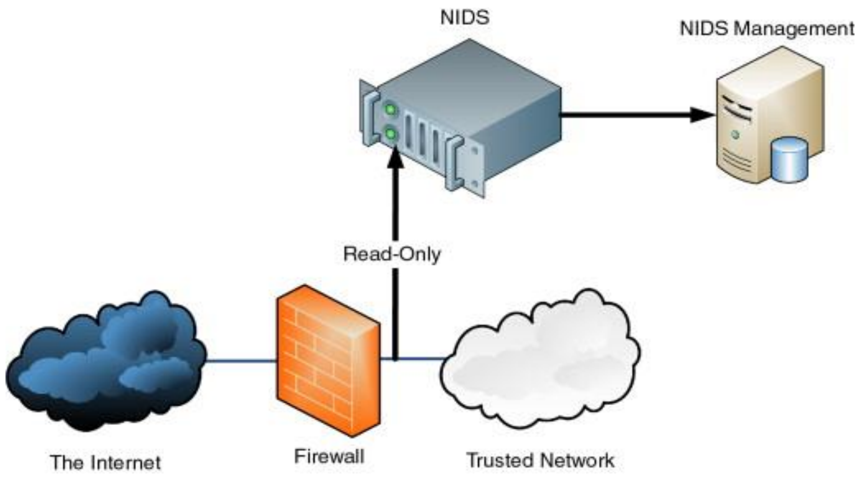


**Figure 3.6: NIDS architecture**.

### 3.3.2 Host-Based IDS

Similar to how a network-based intrusion detection system (NIDS) operates, a host-based intrusion detection system (HIDS) is capable of witnessing and analyzing a computer network's internal workings as the system parcels on its system interfaces [60]. The first objective system was the centralized server computer system, where outside collaboration was rare. This was the fundamentally structured type of intrusion detection software. Figure 3.7 represents the host-based Intrusion detection system is equipped for checking all or parts of the dynamic conduct and the condition of a computer network system, based on how it is designed. Other than such exercises as powerfully examining system bundles focused at this particular host, a HIDS may recognize which program gets to what assets and find that, for instance, a word-processor has abruptly and mysteriously began adjusting the framework secret key database. So also a HIDS may take a gander at the condition of a framework, its put away data, regardless of whether in RAM, in the file system, log records or somewhere else; and watch that the substance of these show up true to form, for example have not been changed by intruders [58].

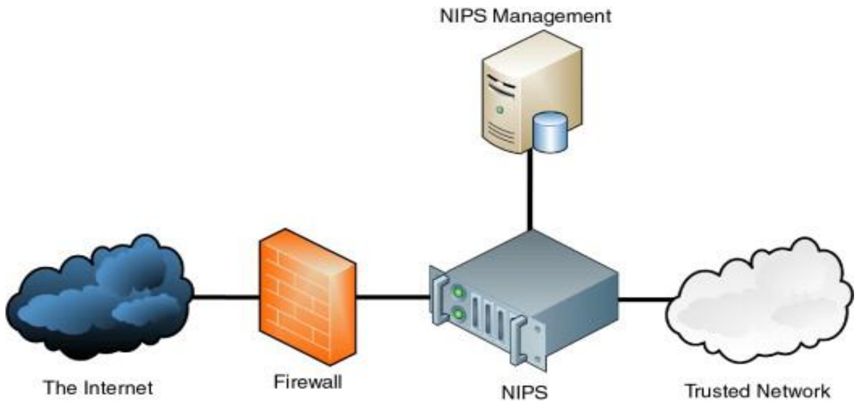


**Figure 3.7: NIPS architecture.**

Host-based Intrusion Detection  System (HIDS) are applications that work on data gathered from particular computer system. This vantage point permits a HIDS to break down behavior on the host it observe at an high level of feature; it be able to regularly establish out which forms as well as users are associated with malicious activities.

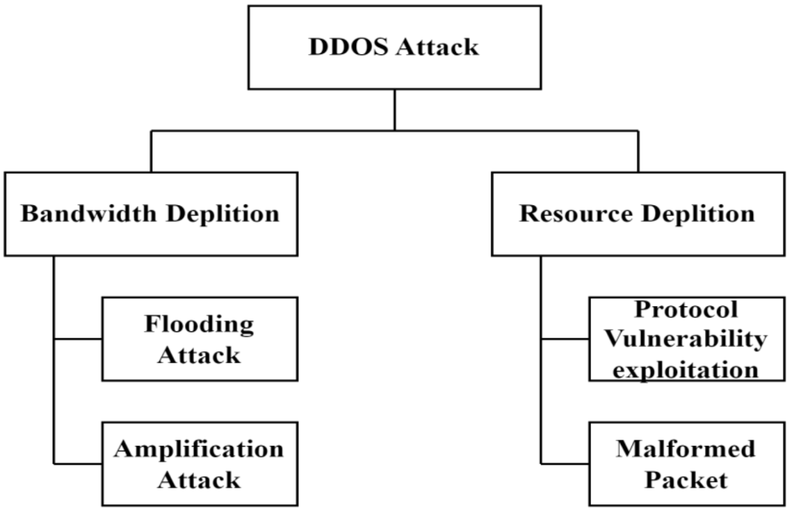


**Figure 3.8: Classification techniques of intrusion data.**

In the figure 3.8, the classification techniques should be optimized for low-complexity and power-efficient operations, while still providing effective DDoS detection capabilities. Additionally, a distributed approach to DDoS detection, where nodes collaborate and share information, can help improve the overall effectiveness of the intrusion detection system One that classifies system activity into normal and odd associations to decide on attacks [16], [83]. Since hybrid techniques, such hybrid classifiers, are superior to single order systems in terms of precision, they have become the de facto norm in the investigation of IDS.

## 3.4 Components of IDS

The three essential useful parts of any IDS they are Information source, Analysis and Response is shown in figure 3.9.

**Data Sources** –The several sources of event data that are utilized to determine whether an incursion has taken place. These sources can be derived from different system levels, with network, system, host, and application observing usual behavior.

**Analysis** – The component of the intrusion detection system that actually sorts through and understands the events obtained from the information sources, determining when those events indicate that an intrusion is occurring or has just happened. Misuse detection and anomaly detection are the two most well-known analysis techniques.

**Response** – The series of decisions the network makes after discovering intrusions. These are frequently combined into passive and active measures, with the passive measures involving disclosing IDS discoveries to people, who are then required to respond based on those reports, and the active measures including some robotized involvement with respect to the system.

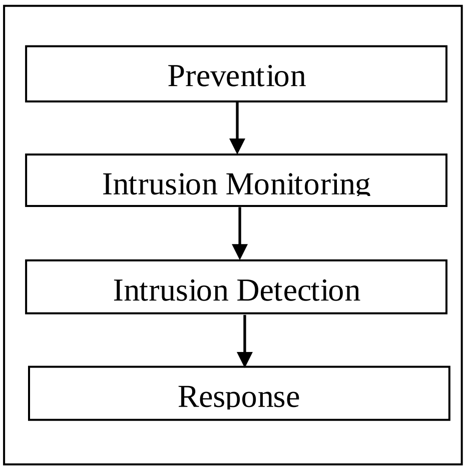


**Figure 3.9: Intrusion Detection System.**

In any event, some recent attempts have a few limitations. First off, accurate incursion data is not taken into account. Some intrusion detection techniques just determine the presence of attacks but do not reveal their nature. In fact, accurate intrusion data is necessary for corporate executives to take the proper security measures. The intrusion detection dataset is incredibly unbalanced, which is the cause [39].Therefore, understanding elite low-recurrence attacks is crucial for IDS. The final obstacle is a huge number of restrictions. The various intrusion detection techniques shown in Figure 3.10, primarily mixture models, contain several parameters. Setting values for such criteria is not straightforward.

Therefore, it's crucial to reduce the number of parameters in the intrusion detection model. The watchdog methodology is a trust-based intrusion detection system that monitors the nodes within its communication range for hostile nodes and their behaviors. The nodes selected as the watchdog nodes are the most trustworthy nodes because of their natural characteristics, such as being exceedingly steady. These watchdog nodes are dispersed randomly over the network, just like every other node. The watchdog can identify whether the data packet is being transmitted by the intermediate node, validating the nodes involved, if it is present within the communication range of both the intermediate node and the transmitting node. This occurs when a node sends a data packet to its target node through an intermediate node. This is due to the fact that when the source node sends this data packet to the targeted intermediary node, a sizable number of other neighboring nodes within the sender node's communication range also receive it.  All undesirable intervening nodes will immediately drop the data packet.

## 3.5 Evaluation Criteria

The effectiveness of the suggested method is evaluated in terms of packet delivery ratio, average end-to-end delay, energy consumption, detection rate, false positive rate, and average detection time by varying the number of wormholes, DDOS attacks, and node density. Finally, the simulation results of the proposed system (EE-IDS and EE-IDSEP) are compared to those of the existing systems (EE-TSW and EE-TS). Because different kinds of communication are required, illuminating various network threats is also difficult and expensive [15].

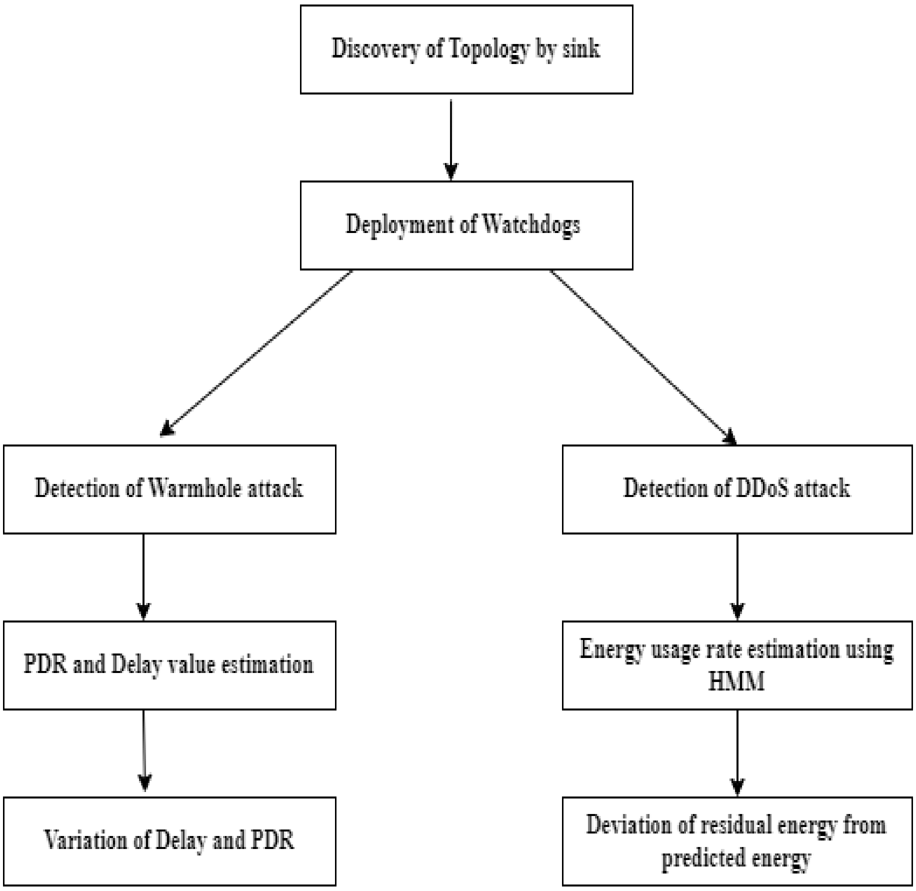

Discovery of Topology by sink
Deployment of Watchdogs
Detection of Warmhole attack
Detection of DDoS attack
PDR and Delay value estimation
Energy usage rate estimation using HMM
Variation of Delay and PDR
Deviation of residual energy from predicted energy

**Figure 3.10: Comprehensive framework of detection system for the proposed method.**

## 3.6 Pre-Processing

Pre-processing, which involves replacing or removing non-numeric or symbolic properties, is crucial. This method produces overhead, which lengthens the time required for setup, complicates the classifier's architecture, and wastes memory and processing power. Pre-processing is crucial since non-numeric or symbolic components have no real value in intrusion detection and must be eliminated or modified, but this method produces overhead, which lengthens the time required for setup, complicates the classifier's architecture, wastes memory and processing power. In order to enhance the effectiveness of intrusion detection systems, non-numeric features are eliminated from the raw information.

## 3.7 Classification

The primary goal of DDOS attacks is to overwhelm the network's resources, such as bandwidth, processing power, or memory, causing disruption or service degradation. Wormhole attacks is to redirect or intercept network traffic, allowing attackers to manipulate or eavesdrop on data transmissions. It's important to note that while DDOS attacks focus on overwhelming network resources, wormhole attacks exploit vulnerabilities in the routing and communication protocols to redirect or intercept traffic. Both types of attacks can have severe consequences for the WSN, but their objectives and techniques differ significantly.

## 3.8 Methodologies

EE-IDSEP is used to detect wormhole and DDOS assaults using the Ns2 simulator, and WSN performance is assessed by taking into account variables including PDR, typical end-to-end latency, and energy usage. The simulation's outcomes demonstrate that the suggested IDS outperforms the current system for a simulated duration of 60 seconds. It has been suggested to use the EE-IDS to identify wormhole attacks. It consists of three main phases. They are wormhole attack detection, optimized watchdog node deployment, and topology discovery. The routing path from each node to the sink is recorded separately in each node as part of the sink node's topology discovery phase. It makes use of the STR, OSTR, and AODV routing protocols.

### 3.8.1 Ad hoc On-Demand Distance Vector Routing

For sensor networks and mobile ad hoc networks (MANET), the AODV routing protocol [16] was created. Reactive routing is made possible by AODV. A route is only created using an on-demand method of route discovery when a source node needs it to send data packets. Route maintenance and route discovery are the two main AODV functions. The messages utilized by AODV for finding and following are Route Request (RREQ), Route Reply (RREP), and Route (ERR) or (RERR).

### 3.8.2 STR and OSTR

The STR method [17] was developed to use 1-hop neighbor information to solve the two issues with ZigBee Tree Routing (ZTR). When it is possible to reduce the number of necessary tree hops to reach the destination, the STR approach, which in essence is ZTR, chooses one of the neighboring nodes as the next hop node. A routing path cannot be changed since sender nodes (S) in STR choose the next hop node, even in the case of a link failure or traffic congestion. On the other hand, OSTR's [17] routing path can be altered depending on the volume of traffic and the state of the network. By dynamically involving neighboring nodes, OSTR can increase the dependability of PDR and the effectiveness of channel utilization.

### 3.8.3 Detection of DDOS Attack

Notations:

- E consumed: HMM estimates of the energy dissipation rate of different states
- E Collected residual: Energy was collected from the nodes that were being watched.
- E Calculated residual: Based on initial energy and spent energy, watchdog nodes calculated residual energy.

Step 1: Watchdog node uses an HMM filter to estimate E consumed.

Step 2: All of the monitored nodes' remaining energy (E Collected) is gathered by the watchdog.

Step 3: The difference between the original energy and the E utilised is calculated by Watchdog.

Step 4: Energy usage is usual if E Collected Residual is more than E Calculated Residual.

Step 5: The energy spent is abnormal if E Collected Residual exceeds E Calculated Residual.

Step 6: The attacker node's network link will be severed if the energy is anomalous; otherwise, move on to step 1.

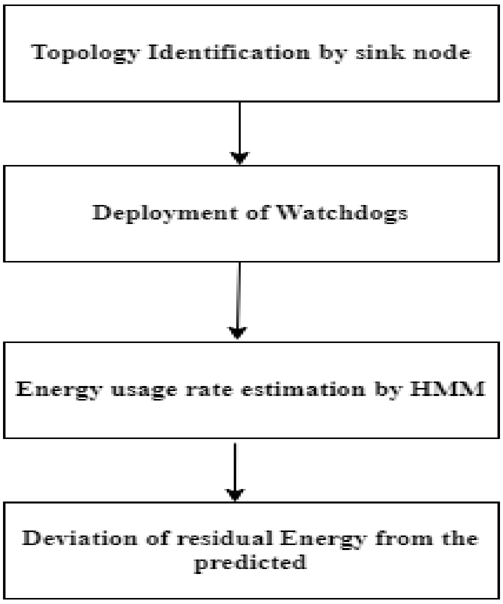

Topology Identification by sink node
Deployment of Watchdogs
Energy usage rate estimation by HMM
Deviation of residual Energy from the predicted

**Figure 3.11: The scheme of intrusion detection based on EE-IDSEP**

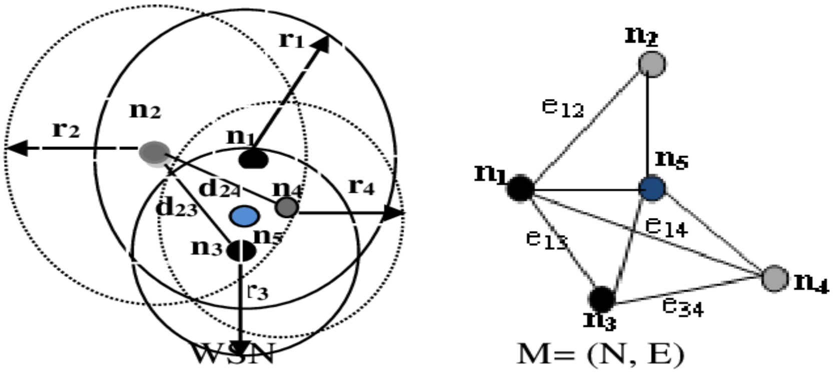


**Figure 3.12: WSN with System Model**

Figure 3.11 shows the proposed system's functional flow diagram, which comprises topology discovery by sink, watchdog deployment that is optimised, and DDoS attack detection. Consider a WSN with a flat topology and its system model M=(N, E), as shown in f igure 3.12. Here, nj N stands for a sensor node in the WSN, while ejk E denotes the neighborhood (i.e., the nodes that are present within each other's communication range) of nj and nk. Let djk represent the physical separation between nj and nk, and let rj represent the communication range of nj. Think about the statement, "E exists only if djk rj and djk rk." The set of nj's neighborhood nodes is defined by Bj=nk | ejk N= nj | djk rj & djk rj. While e23 and e24 do not exist (i.e., n3, n4), n3 and n4 exist inside the communication range of n2 (i.e., d23 r2 and d24 r2).

### 3.8.4 Using HMM to Estimate Energy

The typical Markov model's range is widened by the HMM. The Markov process is obscured or rendered invisible, leaving just the process' output visible. In HMM, only the final state is visible. Just a few of the several states in HMM include the starting state, the transition state, and the observed state. Each state's potential outcomes have a probability distribution. The outcome or the seeming state are not hidden, only the order in which they occurred during the process.

$$\boldsymbol{S = (s1, s2, s3, \ldots\ldots, sn)} \tag{3.1}$$

$$\boldsymbol{V = (v1, v2, v3, \ldots\ldots, vn)} \tag{3.2}$$

Let Q be the state sequence to the corresponding observations, with fixed length L.

$$\boldsymbol{Q = (q1, q2, q3, \ldots\ldots, ql)} \tag{3.3}$$

$$\boldsymbol{O = (o1, o2, o3, \ldots\ldots, ol)} \tag{3.4}$$

HMM is generally formulated as,

$$\boldsymbol{\lambda = (A, B, \pi)} \tag{3.5}$$

In contrast, B represents the array of observations and is not affected by the passage of time. As a result of the state j, it produces the likelihood of observation k, which is stored.

$$\boldsymbol{A = \left[a_{ij}\right], a_{ij} = P(q_t - s_j \left| q_{t-1} - s_j\right)} \tag{3.6}$$

$$\boldsymbol{B = [b_i(k)], b_i(k) = P(x_t = V_k | q_t = S_i)} \tag{3.7}$$

$\boldsymbol{\pi}$ Signifies the initial state probability

$$\boldsymbol{\pi = [\pi_i], \pi_1 = P\ (n_1 = l_i)} \tag{3.8}$$

**Algorithm 1** DDOS Attack Detection

**Input data:**

The Network connection *a*

**Result:** Class label of a

```
function detect DDOS Attack (packet Stream):
    initialize Watchdog()
    initialize HMM Model()
    for each packet in packet Stream:
        if watchdog Packet Received(packet):
            update Watchdog(packet)
        else:
            alert DDOS Attack()
        if is HMM Training Phase():
            train HMM Model(packet)
        else:
            if is DDOS Attack HMM State():
                alert DDOS Attack()
    return no DDOS Attack Detected()

function initialize Watchdog():
    // Initialize the watchdog parameters and variables
    // e.g., set thresholds, counters, and other necessary variables

function initialize HMM Model():
    // Initialize the HMM model parameters and variables
    // e.g., define states, transition probabilities, emission probabilities, and other
necessary variables

function watchdog Packet Received(packet):
    // Check if the packet is received from a watchdog node
    // Return true if the packet is from a watchdog, false otherwise

function update Watchdog(packet):
    // Update the watchdog parameters and counters based on the received packet
    // e.g., update counters for different packet types, source addresses, etc.

function alert DDOS Attack():
    // Trigger an alert indicating the detection of a DDOS attack
    // This could involve logging the event, notifying a central authority, or taking
appropriate action based on the deployment scenario.
```

```
function is HMM Training Phase():
    // Check if the current phase is the training phase of the HMM model
    // This can be based on time, packet count, or other predefined criteria

function train HMM Model(packet):
    // Train the HMM model using the observed packet information
    // Update the HMM model parameters, such as transition probabilities and emission probabilities, based on the training packets

function is DDOS Attack HMM State():
    // Use the trained HMM model to determine if the current state suggests a DDoS attack
    // This can involve computing the likelihood of the packet sequence given the HMM model or using other statistical measures

function no DDOS Attack  Detected():
    // Return a flag indicating that no DDOS attack is detected based on the analyzed packet stream
    // This can be used for further analysis or decision-making in the application
// Main execution
Packet Stream = receive Packet Stream From WSN()
Detect DDOS Attack (packet Stream)
```

### 3.8.5 Detection of Wormhole Attack

Node dependability, anomalous fluctuations in end-to-end latency, and Packet Delivery Ratio (PDR) are the major variables taken into account for the identification of wormhole assaults. The node with the most remaining energy and the most neighboring nodes serves as the network's watchdog. The amount of time it takes for a data packet to transit from one node to the next on its way to its destination is known as the hop-by-hop queuing delay. The node whose end-to-end latency is below the minimal threshold value is assumed to have a wormhole. In order to do wormhole verification on such dubious networks, the suggested approach then exchanges control packets [18] as HELLO request, HELLO rep, and probing packet. Figure 3.13

depicts the planned EE-IDS's functional block diagram for wormhole attack detection. There are three key phases in it. They are topology discovery, effective watchdog node deployment, and wormhole assault detection.

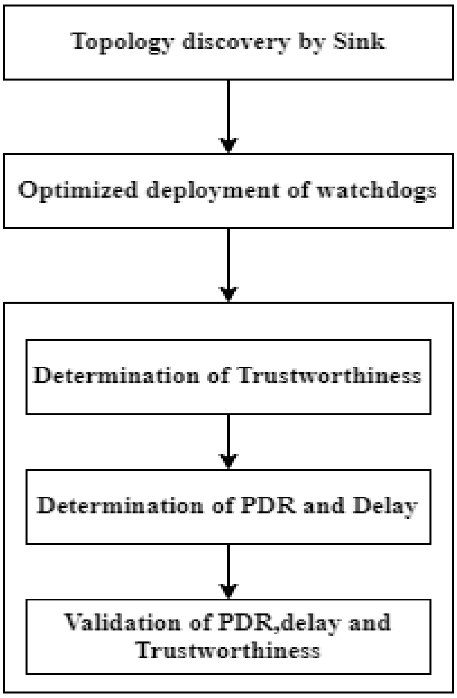

Topology discovery by Sink
Optimized deployment of watchdogs
Determination of Trustworthiness
Determination of PDR and Delay
Validation of PDR,delay and Trustworthiness

**Fig 3.13: Flow diagram of proposed EE-IDS**

Notations

| | |
|---|---|
| ❖ D | : End To End delay |
| ❖ SD | : Standard Deviation |
| ❖ TD | : Topology Discovery |
| ❖ WN | : Watchdog Node |
| ❖ $D_{Watchdog}$ | : End to end delay estimated by the watchdog |
| ❖ $PDR_{Watchdog}$ | : PDR estimated by the watchdog |
| ❖ $D_{Sink}$ | : End to end delay estimated by the sink |
| ❖ $PDR_{Sink}$ | : PDR estimated by the sink |

Network Topology Construction: Set up the WSN network topology by deploying sensor nodes and establishing communication links between them. Each node should be aware of its neighboring nodes.

1. Watchdog Mechanism:

    a. Node Monitoring: Each node continuously monitors the behavior of its neighbors and checks for any suspicious activities that might indicate a wormhole attack.

    b. Watchdog Timer: Nodes employ a watchdog timer mechanism, where each node periodically sends a beacon or heartbeat message to its neighbors. The timer is set to a specific interval, and if a node fails to receive a message from its neighbor within that interval, it raises an alarm.

2. Alarm Propagation:

    a. Local Alarms: When a node's watchdog timer expires due to a neighbor's failure to send a beacon, the node generates a local alarm to indicate a potential wormhole attack.

    b. Alarm Transmission: The local alarm is propagated to the neighboring nodes, indicating the possibility of a wormhole attack.

3. Hidden Markov Model (HMM):

    a. State Representation: Construct a Hidden Markov Model to model the system's behavior, considering both normal and wormhole attack states.

    b. Observation Generation: Define observations based on network-level features, such as packet rates, inter-arrival times, or transmission power levels.

    c. Training: Train the HMM using labeled data that differentiates between normal behavior and wormhole attacks.

    d. Inference: Apply the trained HMM to infer the current state of the system based on the observed network-level features.

4. Alarm Fusion:

    a. Combining Alarms: Combine the local alarms generated by individual nodes with the inference results from the HMM to make a collective decision regarding the presence of a wormhole attack.

    b. Thresholding: Set a threshold for the combined alarm score to distinguish between normal network behavior and a wormhole attack. If the score exceeds the threshold, trigger a wormhole detection alarm.

5. Response and Mitigation:

    a. Routing Path Reconfiguration: If a wormhole attack is detected, the network can reconfigure routing paths to avoid the affected nodes or channels.

b. Secure Neighbor Discovery: Enhance neighbor discovery protocols with authentication mechanisms to reduce the risk of wormhole attacks.

c. Cryptographic Techniques: Employ secure communication protocols and cryptographic mechanisms to prevent unauthorized access and data manipulation.

**Algorithm 2** Wormhole Detection Algorithm

**Input:** Training set for IDS

**Output:** The wormhole path detected

```
  function detect Wormhole():
    for each node in network:
      neighbors = get Neighbors(node)
      for each neighbor in neighbors:
        if is Wormhole(node, neighbor):
          report wormhole(node, neighbor)
function is wormhole(node, neighbor):
    packet = create Test Packet()
    send(packet, neighbor)
    start Time = get Current Time()

    while current Time – start Time < TIMEOUT:
      if packet Received(node):
        return true
    return false
function report wormhole(node, neighbor):
    # Take appropriate action, such as updating routing tables, notifying base station, etc.
    # You can also track the path and location of the wormhole for further analysis.
function get Neighbors(node):
    # Retrieve the list of neighboring nodes of 'node'
    # This can be obtained through neighbor discovery protocols or routing tables.
function create Test Packet ():
    # Create a test packet to be sent to the neighbor node
    # The packet can contain information for identification and timestamping.
```

```
function send(packet, neighbor):
    # Send the packet to the neighbor node
    # This can be done using the network's communication mechanisms.
function packet Received(node):
    # Check if the node has received a packet
    # This can be implemented by monitoring the network interface or listening to incoming packets.
function get Current Time():
    # Retrieve the current time
    # This can be obtained from the system clock or a timer mechanism.
```

## 3.9 Performance Evaluation

The efficiency of the proposed technique is assessed by adjusting the number of wormholes, DDOS assaults, and node density. This is done in order to examine the packet delivery ratio, average end-to-end latency, energy consumption, detection rate, false positive rate, as well as average detection time. The simulation results of the proposed system, EE-IDS and EE-IDSEP, are then contrasted with those of the current EE-TSW and EE-TS. Primarily assess the new protocol's performance in accordance with the following benchmarks. Comparing our proposed energy-efficient intruder detection system (EE-IDSEP) with the energy-efficient trust system (EE-TS) based on watchdog optimisation.

- Average PDR: This metric measures the proportion of successfully received packets to all packets transmitted.
- Average end-to-end delay: By averaging all of the data packets that successfully travelled from the sources to the destinations, this delay is determined.
- Packet drop: This term refers to the quantity of packets that were lost during data transfer.
- Energy usage: This refers to how much energy each node in the network uses on average.

$$T_{ij} = \frac{\Sigma_t \epsilon T v W_{ij\neq 0}^{t} K_{ij}^{t}}{\Sigma_t \epsilon T v W_{ij\neq 0}^{t} 1} \qquad (3.9)$$

The simulation findings show that the proposed EE-IDSEP beats the EE-TS by around 10% in terms of packet delivery ratio, 10% in terms of end-to-end latency, and 15% in terms of energy use when it comes to DDOS assaults. The EE-IDSEP beat the current EE-TS system in terms of the performance parameters of detection rate, false positive rate (FPR), and detection time.

In the table 3.1, the parameters play a crucial role in shaping the behavior of simulation and can have a significant impact on the results.

**Table 3.1: Simulation Parameters**

| | |
|---|---|
| No. of Nodes | 50, 100 |
| Area | 100 X 100 m$^2$ |
| MAC | IEEE 802.1 |
| Node Energy | 1 J |
| Propagation | Two Ray Ground |
| Antenna | Omni directional |
| Routing Protocol | AODV, STR, OSTR |
| Simulation Time | 100 seconds |
| Traffic Source | Poisson |
| Attackers | 5 &10 no’s |

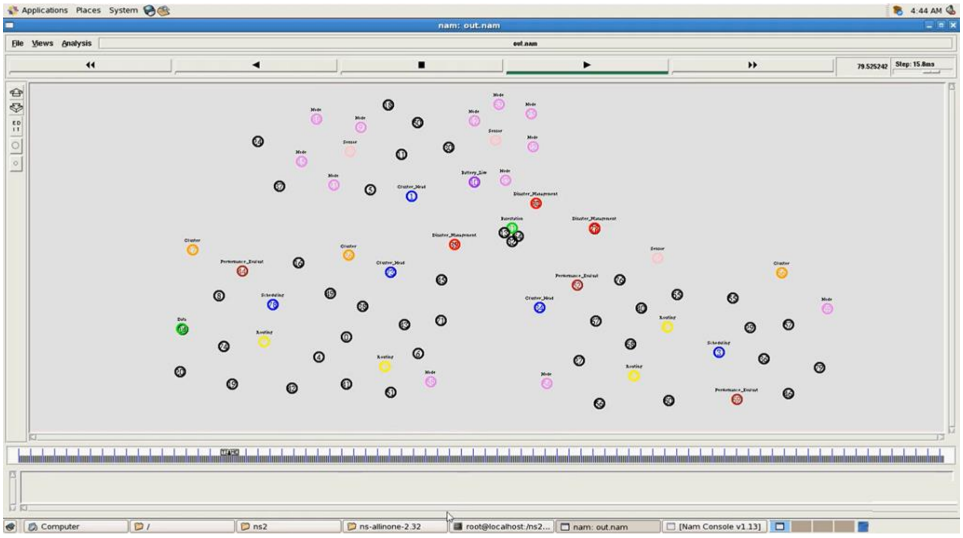


**Figure 3.14: DDOS attack in WSN**

In figure 3.14, the output of the DDOS attack simulation will provide insights into the impact of the attack on the WSN. It will demonstrate how the network's performance and stability are affected, the effectiveness of the IDS or mitigation strategies, and the vulnerabilities and limitations of the WSN under attack conditions. Based on the distinctive characteristic of a DDOS assault a significant energy consumption the attack is identified. The assault is therefore identified using the HMM approach and the energy used by the network nodes. Through the results of the simulation, it was demonstrated that EE-IDSEP performs better than EE-TS in terms of PDR, packet loss, and energy usage. In the table 3.2 and figure 3.15: it can be observed that Compared to the EE-TS, the suggested EE-IDSEP performs around 10% better in terms of packet delivery ratio.

**Table 3.2: Packet Delivery Ratio**

| Nodes | EE-IDSEP | EE-TS |
|---|---|---|
| 1 | 0.93 | 0.84 |
| 2 | 0.87 | 0.81 |
| 3 | 0.86 | 0.78 |
| 4 | 0.86 | 0.75 |
| 5 | 0.82 | 0.72 |

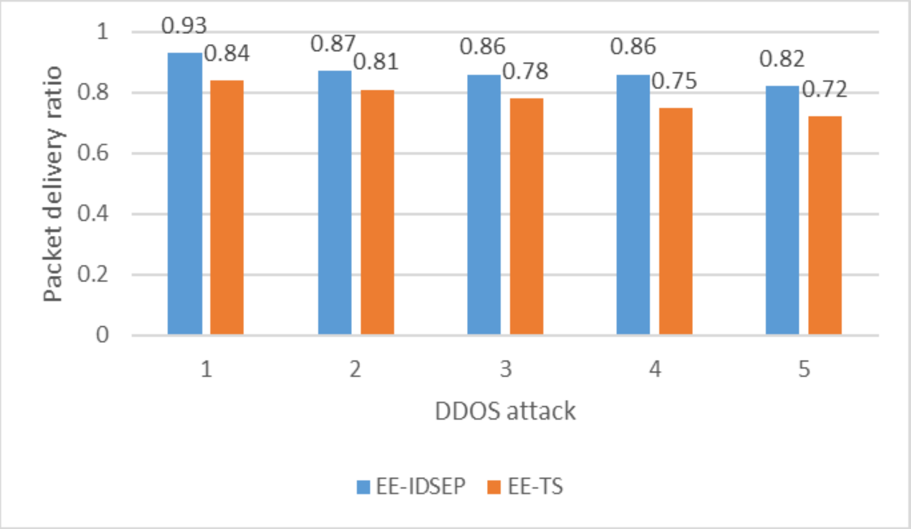


**Figure 3.15: Packet delivery ratio versus DDOS attacks.**

**Table 3.3: End to End delay comparison.**

| Nodes | EE-IDSEP | EE-TS |
|---|---|---|
| 1 | 20 | 23 |
| 2 | 26 | 28 |
| 3 | 31 | 34 |
| 4 | 34 | 38 |
| 5 | 38 | 44 |

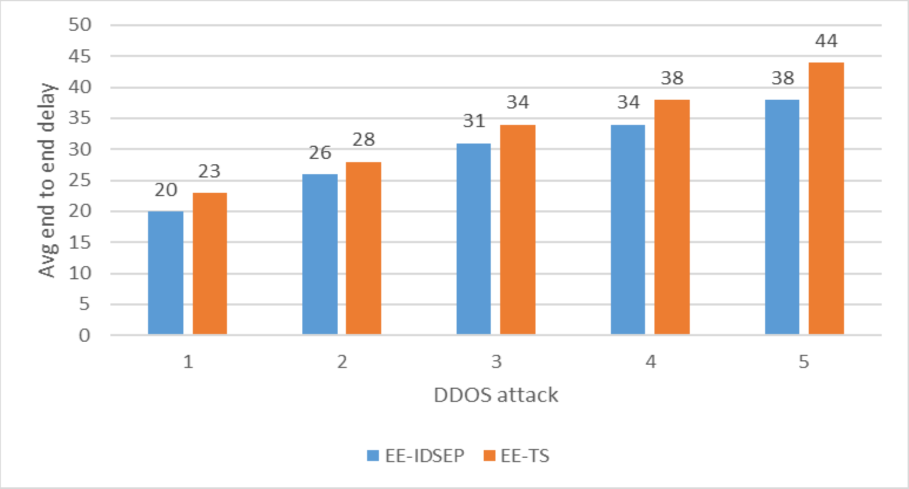


**Figure 3.16: Average End to End delay versus DDOS attacks.**

Observing the table 3.3 and figures 3.16, End-to-end latency is reduced by 10%, and energy consumption is reduced by 15%, as compared to DDOS attacks. Performance metrics such as detection rate, false positive rate (FPR), and detection time have shown that the EE-IDSEP outperforms the EE-TS system. The recommended system has been shown to have 0% FPR when compared to the current system. The proposed approach can detect wormhole assaults more quickly. The results from the simulation demonstrate that the proposed IDS with STR and OSTR protocol surpasses the EE-IDS with AODV and the existing EE- TSW protocols in terms of overall performance. From the table 3.4 and figure 3.17, it's essential to consider the energy consumption of the detection mechanisms to ensure the longevity and efficiency of the network. Here's a comparison of energy consumption in DDOS detection approaches.

Table 3.4: Energy consumption comparison

| Nodes | EE-IDSEP | EE-TS |
|---|---|---|
| 1 | 0.55 | 0.62 |
| 2 | 0.55 | 0.66 |
| 3 | 0.58 | 0.68 |
| 4 | 0.61 | 0.71 |
| 5 | 0.63 | 0.74 |

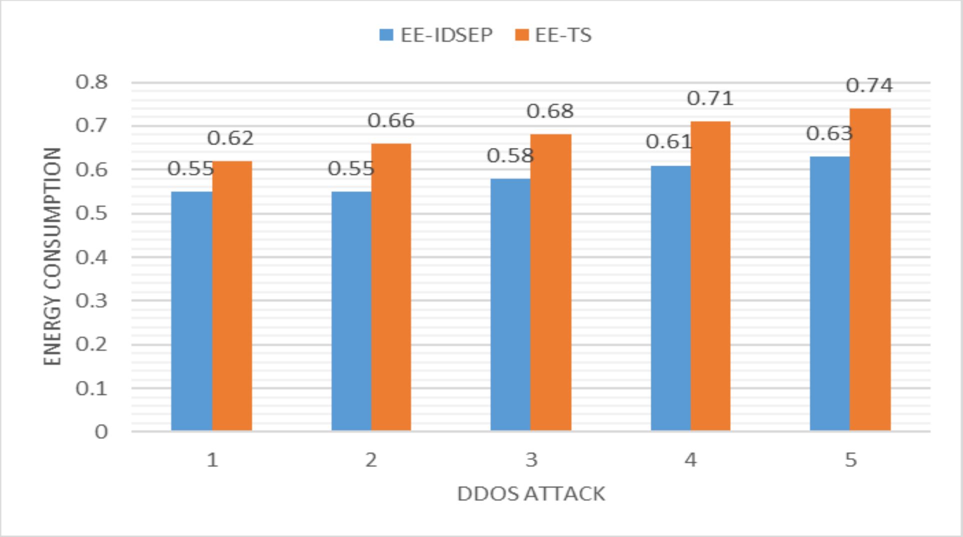
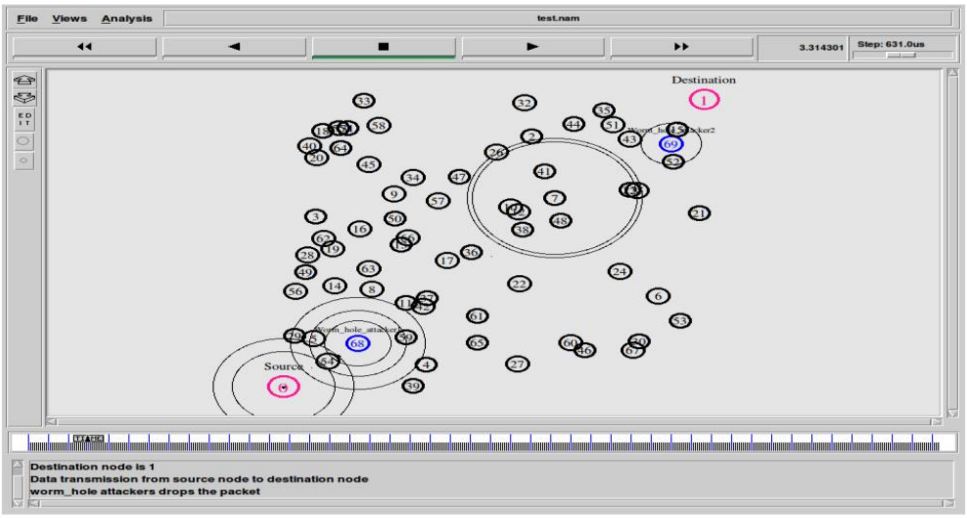


Figure 3.17: Energy Consumption.



Destination node is 1
Data transmission from source node to destination node
worm_hole attackers drops the packet

Figure 3.18: Detection of Wormhole attack on WSN.

**Table 3.5: Packet Delivery Ratio Comparison.**

| Nodes | EE-IDS | EE-TSW |
|---|---|---|
| 10 | 0.85 | 0.81 |
| 20 | 0.84 | 0.8 |
| 30 | 0.78 | 0.61 |
| 40 | 0.7 | 0.42 |
| 50 | 0.68 | 0.32 |

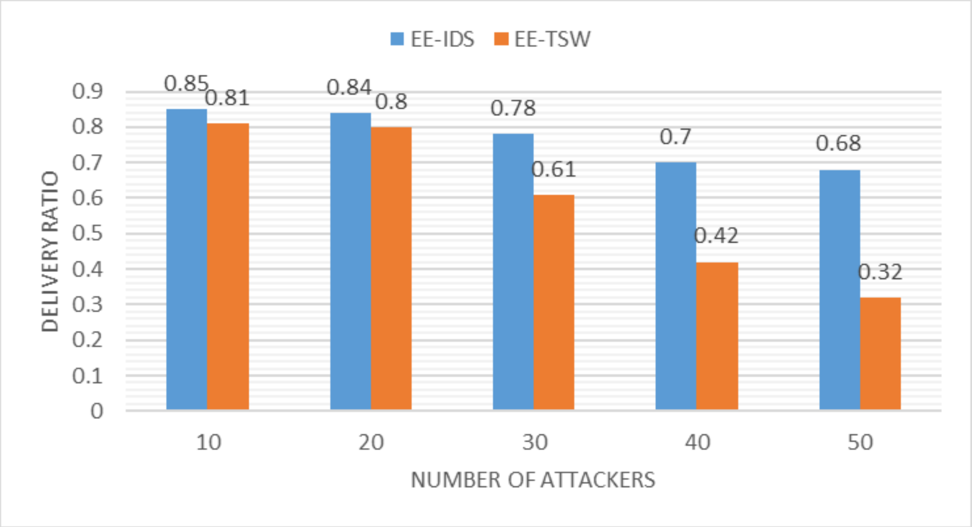


**Figure 3.19: Packet delivery ratio versus Wormhole attack.**

In the figure 3.18 and table 3.1, the output of the simulation will depend on the setup and configuration of the wormhole attack scenario and the performance metrics you chose to monitor. Analyzing the output is to understand the impact of the wormhole attack on the WSN's routing efficiency, data integrity, and overall network performance. In the table 3.5 and figure 3.19, it can be observed that the PDR decreases in relation to a rise in wormhole attacks. Additionally, it can be deduced from the results that the suggested IDS, EE-IDS-AODV, EE-IDS-STR, and EE-IDS-OSTR, perform better than the current EE-TSW by around 23%, 28%, and 33%, respectively. In the table 3.6 and figure: 3.20, it is evident With average end-to-end delays dropping by roughly 5.4%, 8.8%, and 6.6%, respectively, the proposed EE-IDS-AODV, EE-IDS-STR, and EE-IDS-OSTR have all shown improved performance. From the table 3.7 and figure 3.21, the goal is to ensure that communication paths are legitimate and not influenced by malicious actors, thus improving the overall energy efficiency of the WSN.

**Table 3.6: Delay comparison.**

| Nodes | EE-IDS | EE-TSW |
|---|---|---|
| 10 | 10 | 20 |
| 20 | 12 | 25 |
| 30 | 22 | 40 |
| 40 | 40 | 60 |
| 50 | 60 | 75 |

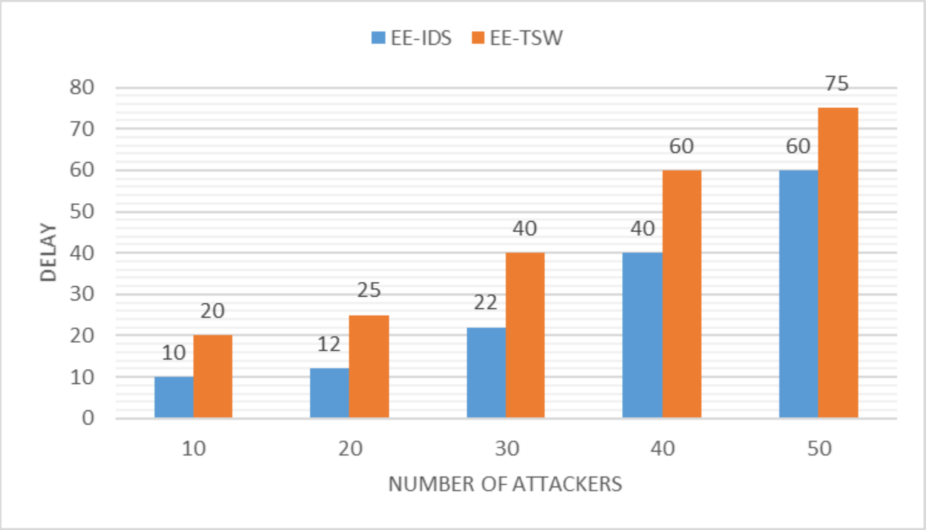


**Figure 3.20: Packet delay versus Wormhole attack.**

**Table 3.7: Energy Comparison in Wormhole attack.**

| Nodes Attackers | EE-IDS | EE-TSW |
|---|---|---|
| 10 | 1.5 | 2 |
| 20 | 3 | 4 |
| 30 | 4 | 4.3 |
| 40 | 5 | 6.5 |
| 50 | 6 | 8 |

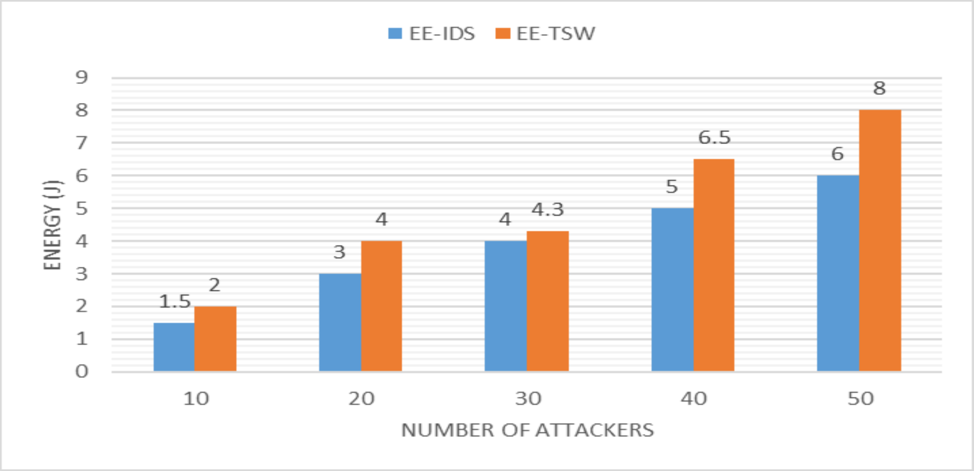


**Figure 3.21: Energy comparison in Wormhole attack**

## 3.10 Conclusion

Networks and information systems today and in the future both require solutions for intrusion detection and prevention. In this sense, intrusion detection systems have grown in importance over the past several years. In terms of packet delivery ratio, end-to-end latency, and energy consumption with respect to wormhole assaults, the EE-IDS with STR and OSTR protocol outperforms the present EE- TSW by around 29% and 34%, 8.8% and 6.7%, and 10.3% and 12.4%, respectively. It consumes 16% less energy as compared to DDOS attacks and improves packet delivery ratio, end-to-end latency, and energy use by around 10%, 10%, and 16%, respectively. This is similar to how recommended EE- IDSEP performs better than EE-TS. In terms of crucial performance metrics like detection rate, false positive rate, and average detection time, the recommended IDS has likewise excelled the current IDS detection systems.

# CHAPTER 4

# LOCALIZATION BASED CLONE NODE DETECTION IN WIRELESS SENSOR NETWORKS

## 4.1 Introduction

Wireless Sensor Networks (WSNs) consist of a large number of small, resource-constrained sensor nodes that collaborate to collect and process data from the environment. These nodes are vulnerable to various security threats, including clone node attacks. Clone nodes are malicious entities that illegitimately replicate the identity of legitimate nodes in the network. Clone node attacks can have detrimental effects on the integrity and reliability of WSNs. To impersonating legitimate nodes, clone nodes can disrupt the network's operations, compromise data confidentiality, launch various types of attacks, or manipulate the network behavior.

Clone identification in WSNs refers to the process of detecting and identifying these malicious clone nodes within the network. The goal is to differentiate between legitimate nodes and their illegitimate replicas to maintain the network's security and reliability. Clone identification techniques in WSNs typically rely on various characteristics and mechanisms to distinguish clone nodes from legitimate ones. These techniques can include physical, behavioral, or trust-based approaches. Replication attacks in wireless sensor networks might be referred to as application-independent attacks. The nodes added to the system will be given ids similar to those of the other nodes in the network, according to Parno B et al. (2005), in the replication attack where more than one node might be included or not included in the network. The phrase "clone attack" is another term for the replication assault. According to Alsaedi N. et al. (2017), the Sybil attack and the replication assault on the network are the same. A DOS attack happens when a node obtains several ids prior to attempting to attack the network system, according to Ramesh K et al. (2011). The replication assault is located using detection IDs.

Clone identification techniques aim to strike a balance between accuracy and efficiency, as they should be capable of effectively identifying clone nodes while minimizing false positives and false negatives. Additionally, the resource constraints of sensor nodes, such as limited processing power and energy, pose challenges in the design and implementation of clone identification mechanisms. The development and evaluation of clone identification techniques in WSNs involve simulation-based studies, mathematical modeling, and experimental evaluations. These techniques play a crucial role in enhancing the security and resilience of WSNs by mitigating the threats posed by clone node attacks and ensuring the authenticity and trustworthiness of network communications. Utilize a localization technique to estimate the physical locations of sensor nodes in the network. Common localization methods include GPS-based localization, range-based localization (such as using RSSI or time-of-flight measurements), and range-free localization algorithms (such as DV-Hop or Centroid-based localization). Analyze the neighborhood relationships between nodes based on their estimated locations. Based on physical proximity, each node should keep track of the nodes that are nearby. Clone nodes that have similar or overlapping sets of neighbors can be found by comparing the neighborhood lists of several nodes.

## 4.2 Problem Statement

Given a WSN with resource-constrained sensor nodes and the presence of potential clone nodes, the aim is to develop energy-efficient clone node identification techniques that accurately detect and differentiate between legitimate nodes and their malicious replicas while minimizing energy consumption. Designing clone node identification mechanisms that employ energy-efficient algorithms and techniques to minimize energy consumption during the detection process. This includes optimizing computation, communication, and data transmission activities to reduce the overall energy expenditure. Implementing adaptive thresholding techniques to dynamically adjust the detection thresholds based on the network's energy conditions. This allows the identification mechanism to balance detection accuracy with energy consumption, optimizing the trade-off between false positives and false negatives.

**Objective**

The objective is to develop clone node identification techniques that strike a balance between detection accuracy and energy consumption, ensuring the longevity and efficient operation of the WSN.  Addressing the energy consumption aspect of clone node identification, researchers and practitioners can contribute to the development of energy-efficient and sustainable security solutions for WSNs. In overlapping clusters, replica node discovery presents a significant issue. To find replicating nodes in overlapping clusters, two algorithms are used: the hybrid bat algorithm with differential equation (BA-DE) and the adaptive weighted clustering (AWC) algorithm. The second approach identifies a replica by locating it using triangulation and the RSSI (received signal strength) technology, whereas the first method uses RFID to uniquely identify the gadget. The effectiveness of these techniques—randomized multicast (RM), line-selected multicast (LSM), fault-tolerant virtual backbone tree (FTVBT), and K-coverage WSN—is tested in comparison to multicast and non-clustered systems. RDBRFID is seen to have a higher detection rate and less transmission overhead due to its deterministic technique.

## 4.3 System Model

A node's MAC address may be used to uniquely identify it in wired networks [15]. The MAC addresses of the nodes in a WSN, however, are easily duplicable or spoof able [16]. It is challenging to uniquely identify every node in a WSN. With the help of the existing addressing method, it is possible to provide nearby nodes addresses, and those nodes will then give their own close nodes addresses [17]. However, there is no structure in place to guarantee the exclusivity of the address given. As a result, the replication identification problem is not solved by this. The suggested method, RDBRFID, employs a novel replica identification technique for overlapping clusters in WSN based on RFID-based unique addressing [18]. The node may be uniquely identified by the system's RFID-based addressing mechanism only if it has an RFID tag inside of it. The permanent and specific RFID address is [18].RDBLT, a different recommended approach, locates nodes in a network using a localization technique based on RSSI and the triangulation algorithm [19].

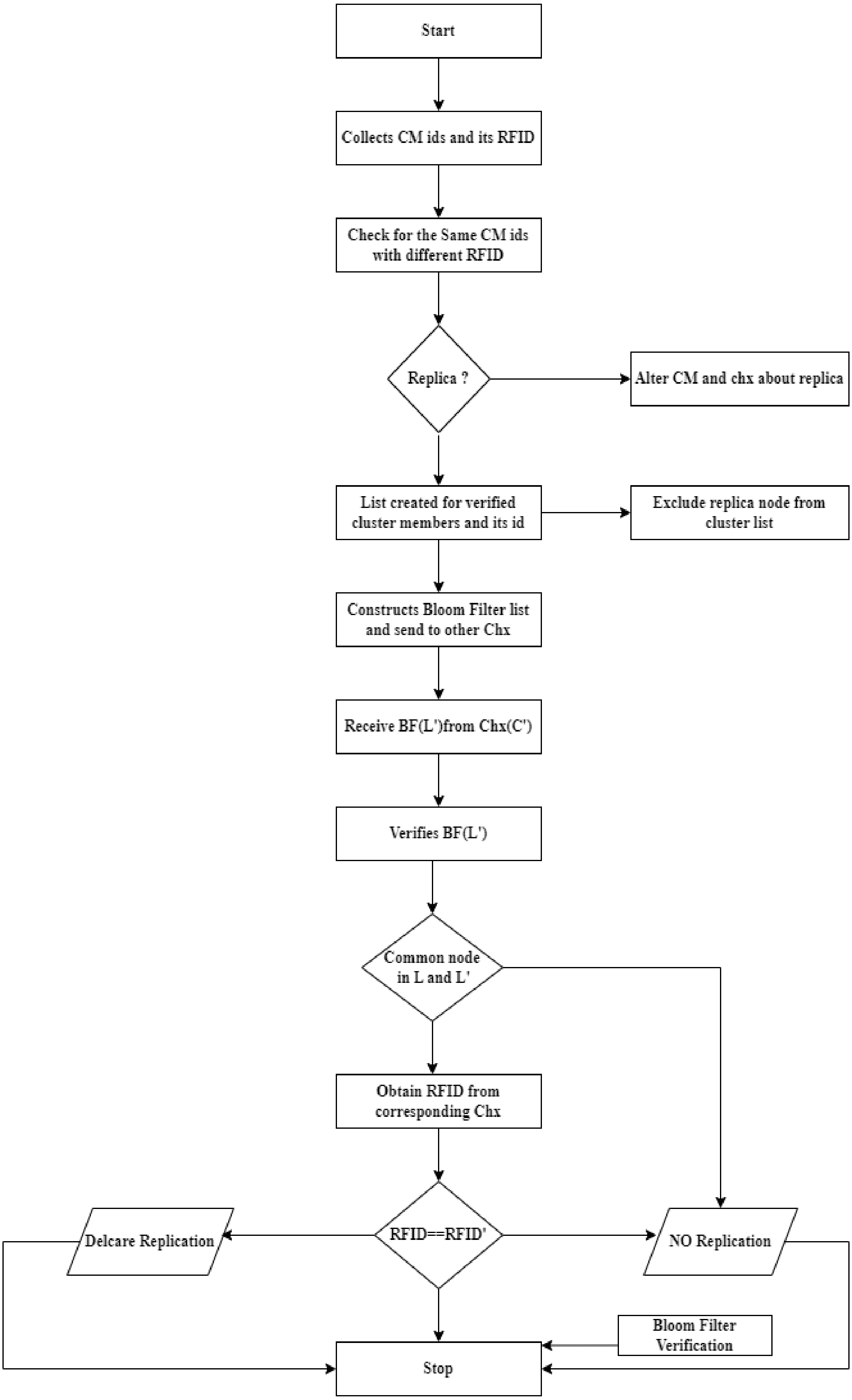

Start
Collects CM ids and its RFID
Check for the Same CM ids with different RFID
Replica ?
Alter CM and chx about replica
List created for verified cluster members and its id
Exclude replica node from cluster list
Constructs Bloom Filter list and send to other Chx
Receive BF(L')from Chx(C')
Verifies BF(L')
Common node in L and L'
Obtain RFID from corresponding Chx
RFID==RFID'
Delcare Replication
NO Replication
Bloom Filter Verification
Stop

**Figure 4.1: Proposed system flow**

In the figure 4.1, the unique identity and localization-based replica node detection architecture enhances the security and reliability of data in hierarchical WSNs. By using a combination of unique identities and localization information, the system can detect and prevent replica nodes from compromising the integrity of data and ensuring the authenticity of the collected information.

### A) Intrusion Detection System

Network-based and radio signal-based replication detection approaches fall under these two basic groups [15]. The radio signal based detection techniques in WSN employ the radio signal strength indicator (RSSI) or radio fingerprint based on the received signals to identify node replications. [17] in hostile situations and geographically extensive WSN, this strategy is ineffective [30]. The networks-based detection techniques are divided into two groups: mobile and static. Mobile-based and static-based detection techniques are further divided into centralized and distributed techniques.

### B) Classification

Static centralized detection- After being deployed in static networks, WSN nodes stay stationary. Strong base stations are key to centralized detection methods decision making. The following section lists the various static centralized method detection techniques. The simplest method is the most popular in the static centralized method [35]. Static distributed detection refers to the use of distributed algorithms and techniques to detect the presence of clone nodes in the network [37]. Unlike centralized approaches where a single entity is responsible for clone detection, static distributed detection involves collaborative efforts among multiple sensor nodes to identify and differentiate clone nodes from legitimate ones.

### 4.3.1 Bloom Filter for Member List Creation

It's important to note that Bloom filters are primarily used for efficient membership queries and are not designed for precise detection or identification of specific intrusions. They provide a trade-off between memory efficiency and accuracy. Therefore, in combination with a Bloom filter, other techniques such as anomaly detection algorithms, signature-based detection can be employed to enhance the effectiveness of an IDS in WSN. The CM stands for the cluster member. The CM from cm1, cm2, cmn that was owned by CH. The cluster head for each CM determined the hash value. The output of a bloom filter is viewed as n bits. In the bloom filter to include CMi, the value of the cluster members' hash, CMs, with H-Hash [h1, h2, hn], is established. The applicable bloom filter bit will receive the value one. Bits from extra bloom filters will be zero in value. Verify the bit's location in the bloom filter to see if any cluster members are present, then calculate the value of H to CM.

$$p = \left(1 - (1 -\ 1/m)^{kn}\right)^{k} \quad (4.1)$$

No CM will be left behind in BF in relation to the idea of the insertion method. This was cited as the cause of the absence of any false negatives in BF. Possibility of marking non-CM as CM in bloom filters. This demonstrates the potential for false positives.

$$p = \left(1 - (1 -\ e^{-kn/m})\right)^{k} \quad (4.2)$$

K-hash function sum is referred as

$$k = \frac{m}{n} ln2 \quad (4.3)$$

Substituting k in (4.2)

$$p = \left(1 -\ e^{(\frac{m}{n} ln2)n/m}\right)^{\frac{m}{n} ln2} \quad (4.4)$$

Eq. (4) is further simplified as

$$lnp = -\frac{m}{n}(ln2)^2 \quad (4.5)$$

From (5), m can be obtained as

$$m = \left|-\frac{nlnp}{(ln2)^2}\right| \quad (4.6)$$

#### 4.3.2 Location computation using Triangulation and RSSI.

Localization is used by the BA-DE technique to locate nodes in clusters. Triangulation and RSSI are used to determine the distance between the unknown and the known nodes. The location of the unknown node may be found using the measured distance. To find the unknown node, three anchor nodes are required. The three anchor nodes in the triangulation technique, which are separated by the unknown node's Euclidean distance, allow for the exact identification of the system's nodes. Precise node placement in the system is made possible by the three anchor nodes in the triangulation approach, which are Euclidean distances from the unknown node. The distance between the nodes is computed using RSSI.

Step 1: Begin

Step 2: KN = known nodes [a1, a2, and a3]

Step 3: In [n1, n2, nn], where n1, n2...nn are KN neighbor nodes, obtain RSSI values.

Step 4: From nodes n1, n2, and so on, the node with the highest RSSI in the KN is chosen as node u.

Step 5: Using RSSI, distance d1, d2, and d3 are calculated.

Step 6: It is found using the node u's x1, y1, x2, y2, x3, and d1, d2, d3 coordinates.

Step 7: Include you in KN.

Step 8: Steps 4 through 8 should be repeated until all nodes in [n1, n2, nn] have their coordinates calculated.

Step 9: stop

### 4.3.3 Communication Complexity

Since both techniques employ a broadcasting strategy to find replicas, communication complexity is O (n2). A node in LSM passes a location claim to a chosen node. Fake routing serves as the basis for the node selection. Conflicting claims can be found at the spots where the path intersects as the location claim is transmitted along it. In the LSM, the communication complexity is O (nn). The nodes in N2NB, DM, and LSM are required to send the received node ids and location assertions. The bloom filter is used by both of the mentioned techniques, RDBRFID and RDBLT. A single list of bits containing the entire node id of a cluster is transferred between cluster chiefs.

$$\boldsymbol{n^2}(|\boldsymbol{id}|) > \boldsymbol{n\sqrt{n}}(|\boldsymbol{id}|) > \boldsymbol{c^2}(\boldsymbol{m}) \qquad (4.7)$$

The number of nodes is N, the id and location claims are |id|, and the communication complexity between N2NB and DM is n2 |id|. The term nn |id| can be used to represent the communication complexity of the LSM. The suggested tactics For RDBLT and RDBRFID, the communication complexity is c2 (m), where m is the number of bloom filter bits and c is the number of cluster heads. Equation (4.6) may be used to compute M. Where n is the total number of nodes and |id| is the collection of id and location claims.

$$m = \left|-\frac{nlnp}{(ln2)^2}\right| \tag{4.8}$$

### 4.3.4 AODV (Ad hoc On-Demand Distance Vector) routing.

AODV uses a reactive routing system, routes are built as they are needed. Nodes can utilize AODV to dynamically find and maintain routes in order to connect with other nodes in the network.

**Route Discovery:** When a node has to send data to a destination node but does not yet have a route, it initiates a route discovery method. The Route Request (RREQ) message that the source node broadcasts includes both the destination address and a unique sequence number.

**Route Request Propagation**: Each intermediary node that receives the RREQ message decides if it has already received the RREQ based on the sequence number. If a node has not already seen the RREQ or if the RREQ has a higher sequence number, the node broadcasts the RREQ to its nearby nodes.

**Route Reply:** After receiving the RREQ, the destination node generates a Route Reply (RREP) message. The RREP contains the source address, the sequence number, and the destination address. To unicast the RREP back to the source node, the RREQ's reverse route is taken.

**Route Maintenance:** As it travels back to the source node, each intermediate node changes its routing table with the information from the RREP. The source node may then be reached through reverse pathways. As long as there is ongoing connection between the nodes, the routes are kept up to date.

**Route Error Handling:** A node notifies the other nodes along the impacted route of a link failure or route breakage by sending them a Route Error (RERR) message. The impacted nodes make the necessary updates to their routing tables.

**Route Expiration:** Nodes in AODV frequently check for route expiration because routes have a finite lifespan. An entry in the routing table is deleted and the route is designated as expired if it is not utilized for a predetermined amount of time. When data needs to be transferred to that location, route discovery is started once more.

### 4.3.5 Adaptive Weighted Clustering Algorithm

It involves forming clusters of sensor nodes and assigning weights to the nodes based on their behavior or characteristics. The objective is to detect the presence of clone nodes by identifying abnormal or inconsistent behavior within the clusters.

**Algorithm:**

```
function Adaptive Weighted Clustering():
    // Initialization
    for each node in network:
     node. weight = Calculate Initial Weight(node .attributes)
    Cluster Heads = Empty List ()
    // Adaptive Weight Update and Cluster Head Selection
    for round in range(1, total Rounds + 1):
    for each node in network:
    node. Update Weight() // Update the weight based on network conditions
      if node. weight > threshold and node .weight > Max Neighbor Weight(node
.neighbors):  node.is Cluster Head = true
        cluster Heads.append (node)
// Cluster Formation
    for each non Cluster Head Node in network:
        best Cluster Head = Find Best Cluster Head(non Cluster Head Node. neighbors)
 best Cluster Head. Cluster Members. append (non Cluster Head Node)
    // Cluster Maintenance
    for each cluster Head in cluster Heads:
    if cluster Head .energy Level < threshold:
    cluster Heads .remove(cluster Head)
    eligible Nodes = Find Eligible Nodes(cluster Head. Cluster Members)
     new Cluster Head = Select New Cluster Head(eligible Nodes)
     for each cluster Member in cluster Head cluster Members:
```

Cluster Member .Join Cluster (new Cluster Head)

Adaptive weighted clustering for clone node detection in WSNs leverages the collective intelligence of sensor nodes within clusters to identify clone nodes exhibiting abnormal behaviour or characteristics. By assigning weights to nodes and analysing their behaviour, this approach can enhance the detection of clone nodes and improve the overall security and reliability of the WSN. To calculate the energy level (E) of each sensor node. Assign weights (W) to the nodes based on their energy levels, using a function such as: W = f(E), where f(E) is a mapping function. Once weights are assigned to the nodes within each cluster, perform weighted aggregation to obtain a collective representation of the cluster's behaviour. This can be achieved through techniques such as weighted averaging or weighted summation. For example, if Wi represents the weight of the node in the cluster, and Xi represents a characteristic or behaviour of the node, the aggregated value (A) can be calculated as:

$$\boldsymbol{A} = \frac{(\boldsymbol{\Sigma}(\boldsymbol{W_i} * \boldsymbol{X_i}))}{\boldsymbol{\Sigma W_i}} \tag{4.9}$$

Where Σ denotes the summation.

### 4.4 Results and Discussion

The findings are achieved, and the h-value is between one and two. The replica nodes can be CH or regular mote. All of the cloned devices were initially distributed around the network at random. Over a range of time periods, the BA-DE approach offers a larger detection chance of more than 96%. As the number of duplicated nodes increases, the likelihood of discovering the predicted strategies decreases. This is brought on by the network's restricting characteristics. The adaptive weighted clustering (AWC) methodology and BA-DE methods are more commonly found, the number of replica nodes rises, and the median rate of replica identification is found. The communication overhead dropped together with the CH volume.

**Table 4.1: Communication overhead of existing and forecasted method**

| No of Nodes | LSM | RM | RDBRFID | RDBLT | FTVBT-RDBRFID | FTVBT-RDBLT | K-COVERAGE-RDBRFID | K COVERAGE – RDBLT |
|---|---|---|---|---|---|---|---|---|
| 100 | 0.8 | 0.96 | 0.78 | 0.98 | 0.89 | 0.86 | 1 | 0.98 |
| 200 | 0.8 | 0.94 | 0.78 | 0.96 | 0.92 | 0.88 | 1 | 0.96 |
| 300 | 0.7 | 0.85 | 0.68 | 0.91 | 0.94 | 0.89 | 1 | 0.96 |
| 400 | 0.7 | 0.86 | 0.68 | 0.92 | 0.94 | 0.92 | 1 | 0.94 |
| 500 | 0.8 | 0.96 | 0.7 | 0.94 | 0.92 | 0.86 | 1 | 0.97 |

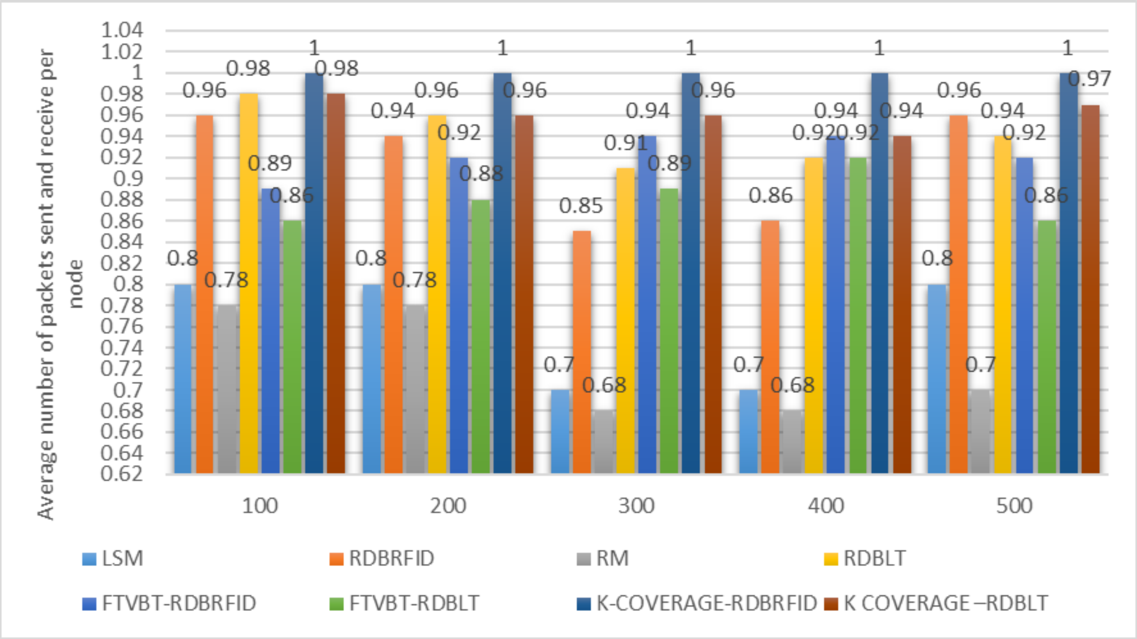


**Figure 4.2: Communication overhead for existing and forecasted method**

The projected approaches adaptive weighted clustering (AWC) algorithm and BA-DE's detection potential are demonstrated in table 4.1 and figure 4.2 for various numbers of replica nodes. The CH or regular mote might be the replica nodes. The results are obtained because the h-value is between one and two. At the beginning of the simulations, all of the replicated devices were distributed randomly around the network. The BA-DE approach for varying h offers a better detection chance of more than 96%. As the number of replicate nodes increases, the likelihood of discovering the intended approaches decreases. This is because throughout the authentication process, the duplicate nodes were chosen with BF loss confirmation. The article noted that when the CH or regular mote might be the replica nodes.

**Table: 4.2 Detection Probability of clone node device**

| No of Nodes | RDBRFID-1 HOP | RDBRFID-2 HOP | RDBLT 1 HOP | RDBLT 2HOP |
|---|---|---|---|---|
| 100 | 0.998 | 0.993 | 0.981 | 0.981 |
| 200 | 0.996 | 0.992 | 0.981 | 0.978 |
| 300 | 0.995 | 0.992 | 0.972 | 0.961 |
| 400 | 0.994 | 0.991 | 0.972 | 0.958 |
| 500 | 0.994 | 0.990 | 0.972 | 0.956 |

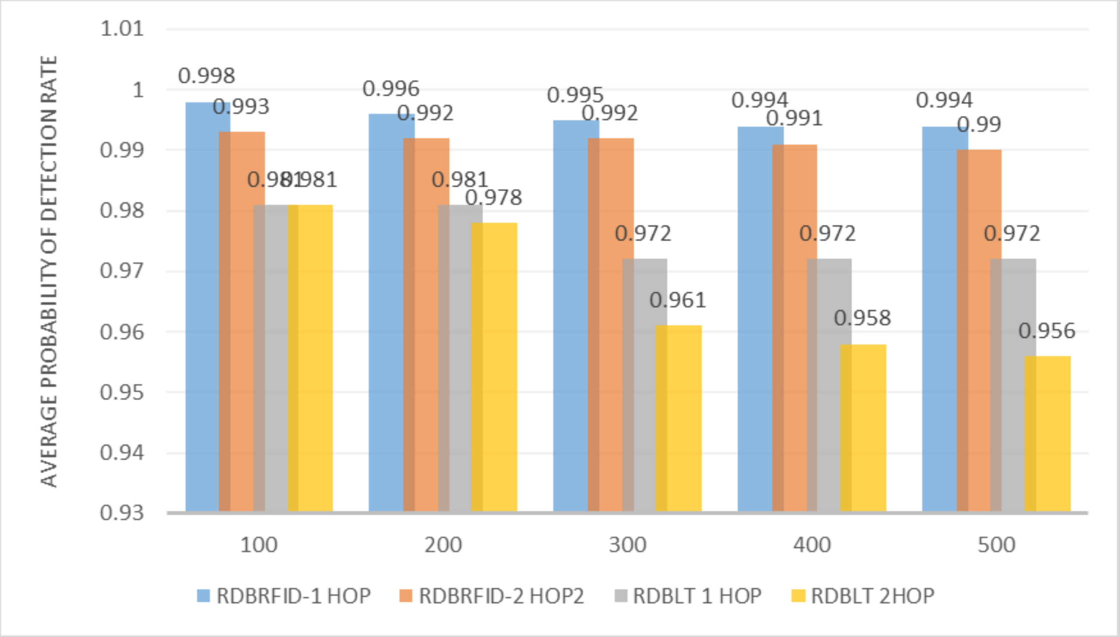


**Figure 4.3: Clone node detection probability of 10 cloned devices**

The results are obtained because the h-value is between one and two. At the beginning of the simulations, all of the replicated devices were distributed randomly around the network. The BA-DE approach for varying h offers a better detection chance of more than 96%. As the number of replicate nodes increases, the likelihood of discovering the intended approaches decreases. This is because throughout the authentication process, the duplicate nodes were chosen with BF loss confirmation.

**Table 4.3: Average possibility of rate replica node detection using forecasted method**

| No of Replica Nodes | RDBRFID-1 HOP | RDBRFID-2 HOP | RDBLT 1 HOP | RDBLT 2HOP |
|---|---|---|---|---|
| 5 | 0.988 | 0.98 | 0.98 | 0.97 |
| 10 | 0.988 | 0.98 | 0.98 | 0.96 |
| 15 | 0.988 | 0.985 | 0.965 | 0.961 |
| 20 | 0.986 | 0.985 | 0.965 | 0.961 |
| 25 | 0.986 | 0.985 | 0.965 | 0.958 |

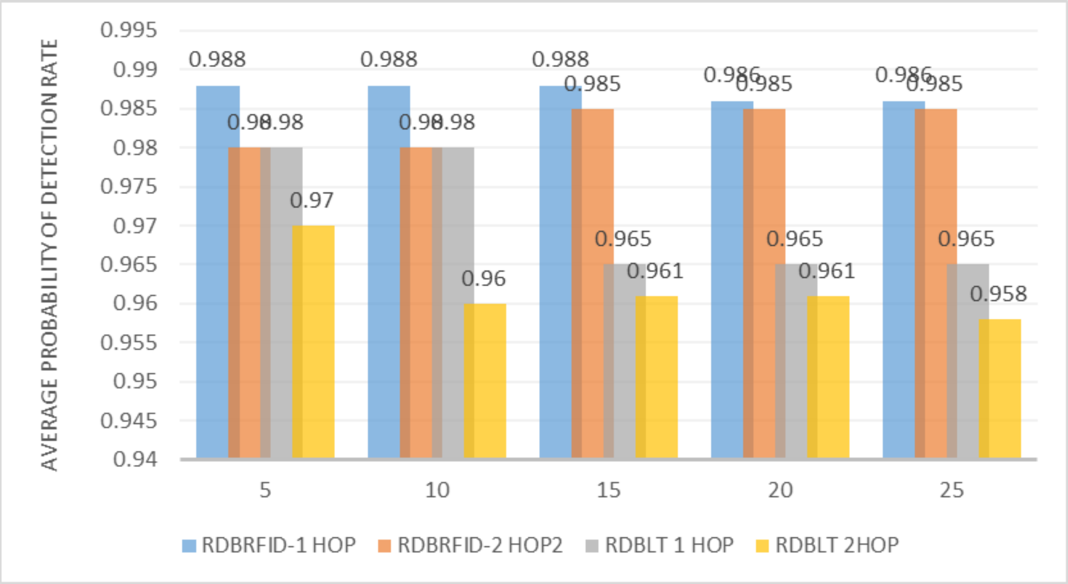


**Figure 4.4: Average possibility for rate of replica node detection**

It claimed that when the cluster size increased along with the h-value, the amount of CH decreased. As replica nodes increase, the median rate of detection of the predicted techniques adaptive weighted clustering (AWC) algorithm and BA-DE is found, and is displayed in table 4.2 and figure 4.3. The communication overhead also lowers when CH levels drop. There are 100 total devices, a hop count between 2 and 1, and between 6 and 35 duplicate nodes. The probability gain for comparing the two forecasting methods, adaptive weighted clustering (AWC) algorithm and BA-DE, is shown in table 4.3 and figure 4.4. The results were found for different hop counts of 2 and 1. The adaptive weighted clustering (AWC) method outperforms BA-DE with a probability gain that ranges between 1.02% and 1.03%. It is understood that this variation results from the predicted technique's adaptive weighted clustering (AWC) algorithm's determinative character as opposed to the BA-DE approach. From the table 4.4 and figure 4.5, the probability gain is used to assess the improvement in the accuracy or reliability of node localization achieved by a forecasted algorithm compared to a baseline approach.

**Table 4.4: Probability gain**

| Nodes | Probability gain over RDBLT -1 HOP | Probability gain over RDBLT -2 HOP |
|---|---|---|
| 100 | 1.021 | 1.024 |
| 200 | 1.022 | 1.025 |
| 300 | 1.021 | 1.024 |
| 400 | 1.022 | 1.028 |
| 500 | 1.02 | 1.03 |

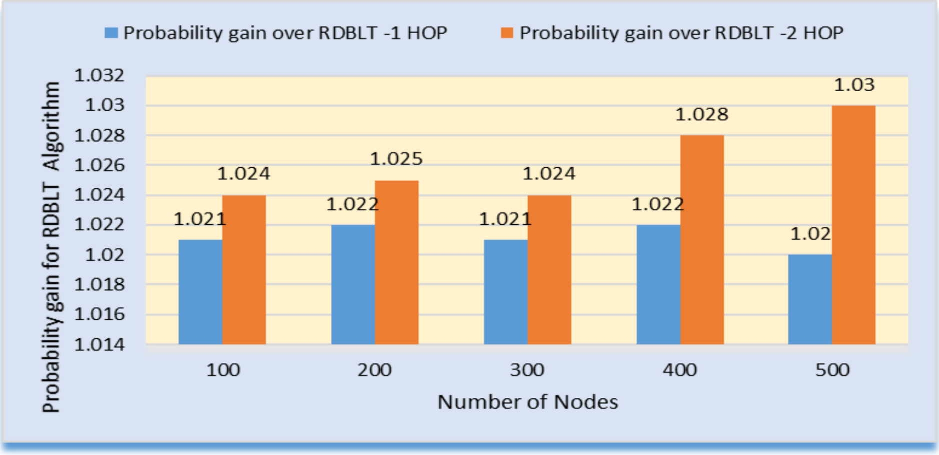


**Figure 4.5: Probability gain of a forecasted algorithm**

## 4.5 Conclusion

The most difficult operation in overlapping clusters is replica node discovery since cluster members are dispersed throughout the clusters. Adaptive weighted clustering (AWC) method and BA-DE approaches use localization and RFID to solve the issue. The effectiveness of the techniques is assessed and contrasted with LSM and RM systems. The methodologies are also discovered in non-cluster settings using K-coverage and FTVBT Wireless Sensor Network in order to evaluate the efficacy and make conclusions. When compared to the current approaches, the adaptive weighted clustering (AWC) algorithm and BA-DE are reported to have the lowest communication overhead. The proposed process, which will be used in accordance with the AODV protocol, is thoroughly compared with the existing approaches to assure its effectiveness.

# CHAPTER 5

# ENERGY EFFICIENT DDOS ATTACK DETECTION AND DEFENSE APPROACH

## 5.1 Introduction

DDOS (Distributed Denial of Service) attack detection in Wireless Sensor Networks (WSNs) using the Sleep/Wake algorithm involves leveraging the energy-efficient scheduling approach to identify anomalous traffic patterns caused by potential DDOS attacks. It is designed to efficiently manage the communication and operation of sensor nodes by alternating between active (wakeup) and inactive (sleep) states [52]. The algorithm aims to strike a balance between maintaining network connectivity and minimizing energy consumption. During the sleep state, nodes turn off their radio and remain inactive. This allows them to conserve energy by minimizing power consumption. While in sleep mode, the node is effectively disconnected from the network and does not participate in any communication or sensing activities. In the wakeup state, nodes activate their radio and become active. During this phase, nodes engage in various activities such as data sensing, processing, and communication with other nodes in the network. The wakeup state allows nodes to establish connectivity, exchange data, and perform necessary tasks. To alternating between sleep and wakeup states, the Sleep/Wake algorithm enables energy-efficient communication and operation in WSNs. It helps to minimize energy consumption during idle periods when no data transmission or processing is required. This energy conservation technique significantly extends the network's lifetime and enables long-term monitoring and data collection in resource-constrained environments. Each sensor node in a WSN may collect all the data aggregation also known as clustering information, which produces precise results. They are then divided into smaller groupings, such as clusters [62], [64]. Each cluster has a C-H-designated head. Finally, the Base-Station as well as C-H packet transfer will occur. In order to prevent DOS attacks, each sensor node has a Digital Signature ID. As a result, the sensor (source) node can transfer the data information to the base station with the digital signature ID. This has the ability to sense information with a digital signature ID before receiving data information.

This approach was introduced by Vaibhav God bole [59] and uses a competitive threshold value to pick a temporary C-H between 0s and 1s. Based on their energy and distance from the base station, one static C-H can be chosen among these temporary C-Hs. Fuzzy logic has been employed in the Fuzzy Clustering Algorithm to eliminate the uncertainties in the C-H radius calculation. Employ the sleep & wakeup protocol [60] as a routing protocol to increase energy efficiency and achieve a high packet delivery ratio (PDR). This method has established a path between C-Hs and the base station. The sensor nodes become awaken nodes if they are in the path. Sleep nodes are the rest of the nodes. In this case, only the wake-up node can communicate its data information to the base station in accordance with the parameters. In the context of Wireless Sensor Networks (WSNs), fuzzy logic is applied to handle the inherent uncertainties in sensor data, network conditions, and environmental factors. It provides a flexible and effective method for making decisions and reasoning in WSNs, where traditional binary logic may not be suitable due to the imprecise and uncertain nature of the data. Fuzzy logic can assist in decision-making processes by considering multiple factors and assigning degrees of importance to each factor based on their relevance and uncertainty. To defend against assaults on the wireless sensor node, a cooperative multi-agent based fuzzy artificial immune system (Co-FAIS) is being developed. This is a fresh approach to the IDS issue. The Low Energy Adaptive Clustering Hierarchy (LEACH) protocol uses Co-FAIS.

## 5.2 Problem Statement

The identification and defense against DDOS (Distributed Denial of Service) attacks in Wireless Sensor Networks (WSNs) utilizing the Sleep/Wake algorithm and fuzzy logic-based defense system is the research subject addressed. The availability and performance of WSNs are seriously threatened by DDOS assaults, which disrupt legitimate communication by flooding the network with large amounts of malicious traffic. The Sleep/Wake algorithm is an energy-efficient technique that optimizes node activity by alternating between sleep and wakeup states. Integrating the Sleep/Wake algorithm with fuzzy logic-based defense mechanisms can enhance the WSN's ability to detect and mitigate DDOS attacks while conserving energy resources.

**Objective:**

Utilizing the energy-efficient scheduling method, DDOS (Distributed Denial of Service) attack detection in Wireless Sensor Networks (WSNs) with the Sleep/Wake algorithm identifies aberrant traffic patterns brought on by probable DDOS assaults. A multi-hop sensor network may experience the hotspot problem because the base-station (sink) is sometimes overlooked. Analyze the sleep & wakeup technique in this work to help prevent the hot spot (WLAN) issue. This strategy tries to improve packet delivery while also lengthening the network lifetime through energy conservation. The choice of C-H (cluster-head) for this approach depends on the distance to and energy level of the base station. The Cooperative Decision Making Modules (Co-DMM) combine the danger detector module with the fuzzy Q-learning vaccine module to provide the best possible defense tactics. The Low Energy Adaptive Clustering Hierarchy (LEACH) was used to assess the performance of the suggested model. By effectively grouping sensor nodes into clusters and enabling data aggregation and transmission inside those clusters, it aims to reduce energy consumption and extend the network lifetime.

## 5.3 Methodologies

The fuzzy clustering method is a distributed, competitive algorithm [56]. Using a threshold value, the temporary cluster heads were chosen. Random rotation (number between 0 and 1) has selected the temporary C-H for each round. Based on energy consumption and base-station distance, the permanent C-H was chosen from these temporary C-H utilizing the Mamdani technique [57] of fuzzy inference approach using fuzzy if-then rules with linguistic variables. To find the path and determine its base station destination n, the FCA uses an algorithm. The Base-Station, like the centralized Clustering Algorithm [59], has access to all of the network's clustering data and may choose new precise C-Hs based on energy and C-H radius distance. After that, C-H sent the data packet to the base station. Assume that, the fuzzy logic condition if there is a problem with the C-H radius estimation. In figure 5.1, the effectiveness of the system architecture depends on the choice of anomaly detection techniques, the accuracy of the models used, the level of collaboration among sensor nodes, and the security measures implemented to protect the WSN against various intrusion attacks.

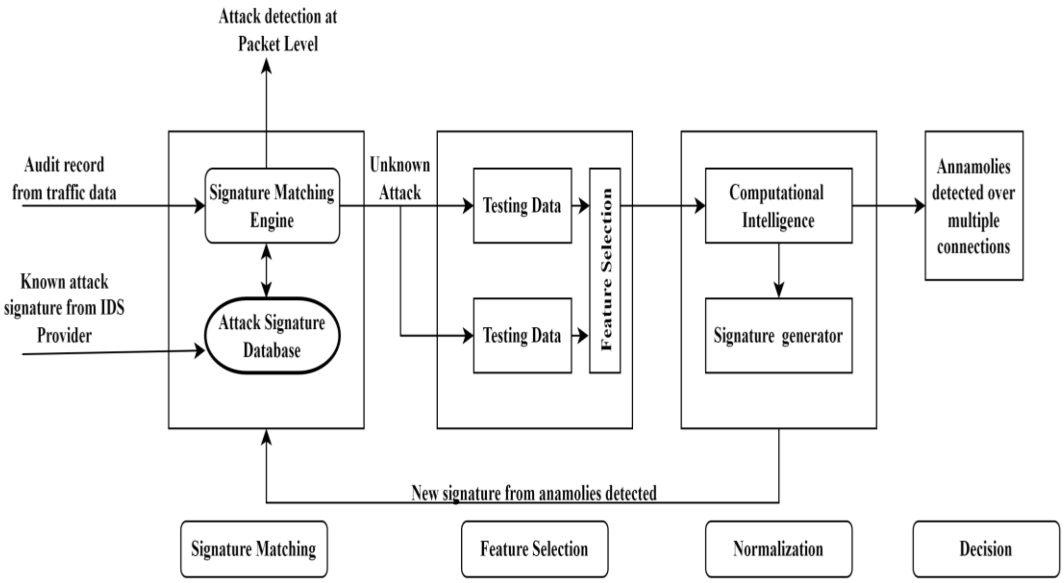


**Figure 5.1: System architecture for intrusion attacks detection**

### 5.3.1 Sleep and Wakeup Approach

The C-H has been chosen as a mobile node in this instance. The C-H could map out a path to the base station while on the go. The WORK_REQUEST message can then be sent from the base station to C-H. The C-H can transmit the WORK message if the sensor nodes are present along the path. As a result, that specific sensor node is converted to a wake up node. The base station will then receive the data packet transmission. The C-H can transmit the sleep message even if the nodes are off the route. As a result, the sleep node does not transmit the data packet to the base station. The sleep nodes keep the WORK_REQUEST message for C-H after the data packet transmission is complete because they practice excellent energy saving. After that, the C-H might move to a new area and carry on with this process. Any packet loss will stop the transmission of packets. Using this packet loss, create a parameter for the FND (first node dead) and HNA (half of the nodes alive) circumstances.

Energy Efficiency: The primary objective of the LEACH protocol is to improve WSN energy efficiency. This is accomplished by using a clustering strategy in which sensor nodes are grouped together under the leadership of a selected cluster head (CH). The CHs rotate on a regular basis to evenly balance energy use among nodes, preventing any one node from rapidly exhausting its energy supply. The overall amount of energy is reduced by this clustering technique.

Load Balancing: LEACH aims to balance the energy load among nodes by periodically selecting a new CH within each cluster. By distributing the role of CH across different nodes, the protocol prevents energy depletion in specific nodes, thus prolonging the network's operational lifetime.

- Data Aggregation: LEACH enables efficient data aggregation within clusters, which reduces the amount of data transmission and saves energy. Sensor nodes in a cluster aggregate data from multiple sources before transmitting it to the CH. This aggregation reduces redundancy and minimizes the number of transmissions, resulting in lower energy consumption.

- Scalability: Due to the scalability of the LEACH protocol, the network may support several sensor nodes. By forming clusters and utilizing the CHs, LEACH avoids direct communication between all nodes in the network. This clustering structure enables efficient data collection and communication even in large-scale WSNs.

- Self-Organization: LEACH promotes self-organization among sensor nodes. The protocol does not require any centralized control or infrastructure, allowing nodes to autonomously form clusters and elect CHs based on predefined rules. This self-organization capability simplifies network deployment and management.

- Fault Tolerance: LEACH provides a level of fault tolerance in WSNs. Since each cluster has multiple sensor nodes, the failure of a single node does not cause the entire cluster to be compromised. The clustering structure allows the network to continue functioning even in the presence of node failures or attacks.

In the figure 5.2, flow diagram will be tailored to the specific requirements and algorithms used in the DDoS attack detection system.

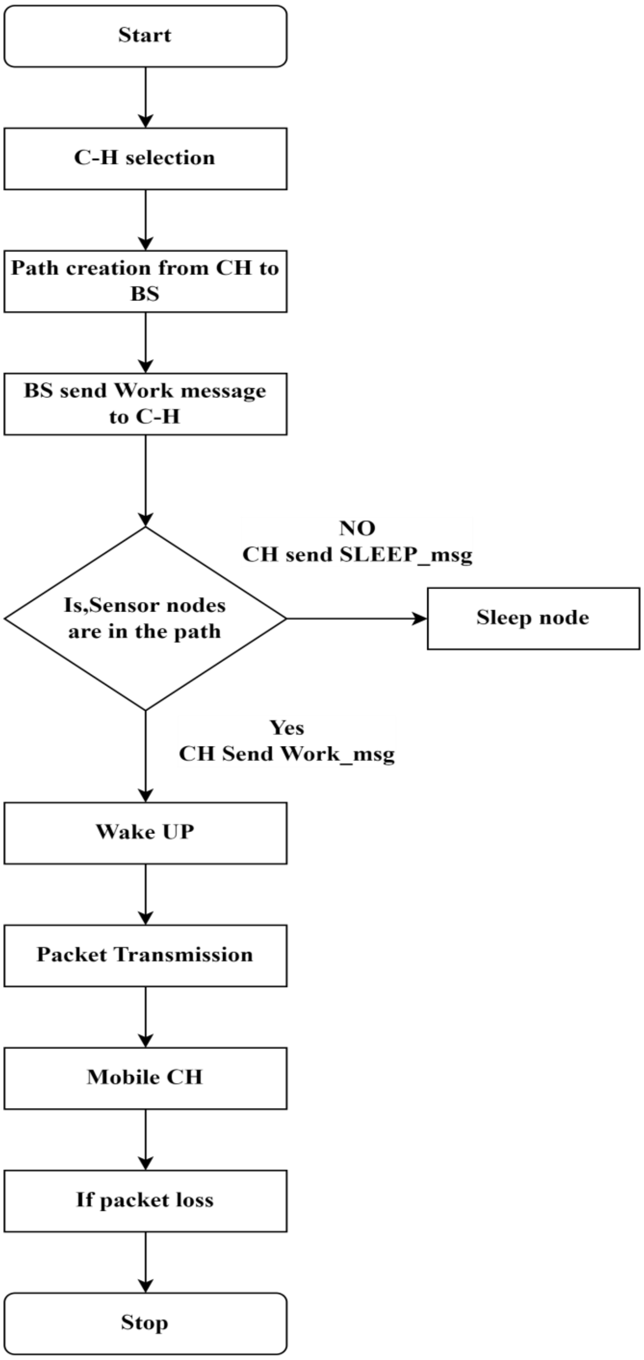


**Figure 5.2: Flow diagram of Sleep Wake approach**

**Algorithm**

```
shared variable flag = false
shared variable queue = empty
function sleep():
    if flag is true:
        add current process to queue
        block current process
    else:
        set flag to true
function wake():
    if queue is not empty:
        remove a process from queue
        unblock the process
    else:
        set flag to false
```

## 5.3.2 LEACH Routing Technique

### A. Network Lifetime

- Reset as soon as the first sensor node (FND) expired.
- Round when a certain percentage of sensor nodes (some nodes) stopped functioning as whole nodes.
- Round when last number of node expired (LND).

### B. Network Throughput

The quantity of information a system can process in a certain amount of time is known as throughput. The entire amount of data packets transferred to the BS is referred to as throughput in a WSN system.

$$E_{TX}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2 & d < d_0 \\ kE_{elec} + k\varepsilon_{amp}d^4 & d \geq d_0 \end{cases} \tag{5.1}$$

$$E_{RX}(k) = kE_{elec} \tag{5.2}$$

Where ERX is the energy response of all k bits in the direction of distance d, and ETX is the energy transmission. Electronic energy is required for filtering, coding, and modulation. Energy-consuming EDA is required for data accumulation. Efs and ampere the energy of amplification

To find the $E_{avg}$ per round.

$$E_{avg} = \frac{Total\ energy\ consumption\ of\ 1^{st}\ node\ expired}{Number\ of\ rounds\ before\ the\ 1^{st}\ node\ expired} \tag{5.3}$$

The selection of the node that will become the next CH is the primary task of the first phase. The CH is chosen using a random integer that must fall between 0 and 1, which is equal to a T (n), which is evaluated by equation (4).

$$\boldsymbol{T(n)} = \begin{cases} \frac{P}{1-P\,(r \bmod 1/P)} & \textit{if } n \in G \\ 0 & \textit{Otherwise} \end{cases} \tag{5.4}$$

Master nodes regularly collect data and deliver it to the CH during the second phase. The steady state process is now split into a number of frames, each of which is split into a number of time slots within the same period. Master sensor nodes relay the data they have collected to the relevant CH during their allotted communication.

### 5.3.4 Cooperative-FAIS

A multi-agent artificial immune system that provides defense against a lone attacker is the cooperative-FAIS model. It gives one more self-assurance and establishes a solid reputation for discovering an intruder quickly and successfully defending the system. In order to overcome the attacker, this cooperative immunity system based on tactics adapts to ongoing self-learning from prior attacks and the behavior in the fuzzy Q-learning decision-making process. According to Co-FAIS, regular interaction fosters cooperation, confidence, and reputation as supplements by offering incentives for cooperative behavior and disincentives for fraudulent behavior. The next generation of complex heterogeneous computer and networking systems is better protected against sophisticated attacks and attackers using cooperative theory-based fuzzy Q-learning artificial immune system, a technique in IDS. To further enhance its capacity to make decisions that would repel existing or upcoming assaults, the recommended Co-FAIS mechanism should be enhanced in the future to incorporate information from various attack types and sources.

**Algorithm:**

```
Initialize the population of antibodies
Initialize the population of sensors
Repeat until termination condition is met:
   for each sensor in the population:
      Measure the local environment and collect sensor data
      If the sensor detects an intrusion:
        Generate a danger signal based on the severity of the intrusion
        for each antibody in the population:
            Calculate the affinity between the antibody and the danger signal
            Update the antibody's activation level based on the affinity
        Select the antibodies with the highest activation levels as response units
        for each response unit:
            Determine the appropriate action based on the response threshold and activation level
            if the action is defense:
                Trigger a defensive mechanism in the sensor
            else if the action is communication:
                Broadcast a warning message to neighboring sensor.
            Update the response unit's activation level based on the performed action
    Update the antibody population based on the feedback received from sensor
    Evaluate and update the fitness of each antibody in the population
    if termination condition is met:
        break
```

***Steps:***

1. Initialize the system:

Initialize sensor nodes, each with unique IDs and positions.

Initialize the AIS parameters and variables.

2. Main Loop:

while (not terminated) do:

2.1. Sensing Phase:

Each sensor node monitors the network traffic and measures various metrics

Calculate the local anomaly score for each sensor node based on the collected metrics. Share the local anomaly scores with neighboring nodes.

2.2. Cooperation Phase:

Each sensor node receives the anomaly scores from its neighboring nodes.

Combine the local and received anomaly scores using fuzzy logic.

Determine the overall anomaly score for each sensor node.

2.3. Decision Phase:

Each sensor node compares its overall anomaly score with a predefined threshold.

If the score exceeds the threshold, the node is considered as a potential attacker.

Mark the potential attackers and broadcast the information to neighboring nodes.

2.4. Response Phase:

Nodes receiving the information about potential attackers evaluate the trustworthiness of the information based on the reputation of the sender.

Formulate a response plan based on the trustworthiness and the severity of the attack.

Implement the response plan, which may include filtering suspicious traffic or isolating the attacker nodes.

2.5. Adaptation Phase:

Depending on how well the system is performing, dynamically adjust the AIS parameters.

Adapt the fuzzy logic system's weights and thresholds in accordance with the Success of the defense plan. Keep an eye on the network and Adjust the defense appropriately.

3. Termination -

Terminate the system based on predefined termination conditions

Create a set of fuzzy rules that map the combinations of fuzzy sets in the state and action spaces to the corresponding fuzzy sets in the Q-value space. Calculate the weighted average of the consequent values using the firing strengths as weights.

Update the current state-action pair's Q-value using the Q-learning update equation using the defuzzified Q-value:

$$Q(s,a) = Q(s,a) + \alpha * (R + \gamma * Qmax - Q(s,a)) \qquad (5.5)$$

Q(s, a) is the current Q-value for state s and action a.

$\alpha$ is the learning rate.

R is the immediate reward received after taking action an in state s.

$\gamma$ is the discount factor.

Q_max is the maximum Q-value among all possible actions in the next state.

## 5.4 Result and Discussion

To optimize the sleep and wakeup algorithm for PDR in DDOS detection, it is important to consider factors such as network traffic patterns, packet delivery requirements, and energy constraints.

**Table 5.1: Comparison of Packet Delivery Ratio**

| Nodes | S & W | FCA |
|---|---|---|
| 1 | 0.72 | 0.42 |
| 2 | 0.76 | 0.45 |
| 3 | 0.86 | 0.47 |
| 4 | 0.89 | 0.54 |
| 5 | 0.93 | 0.61 |

In the table 5.1 and figure 5.3, it is observed that the PDR will depend on the coordination and synchronization of the sleep and wakeup cycles among the nodes. Proper synchronization ensures that the nodes are awake at the same time, enabling efficient packet forwarding and minimizing packet loss.

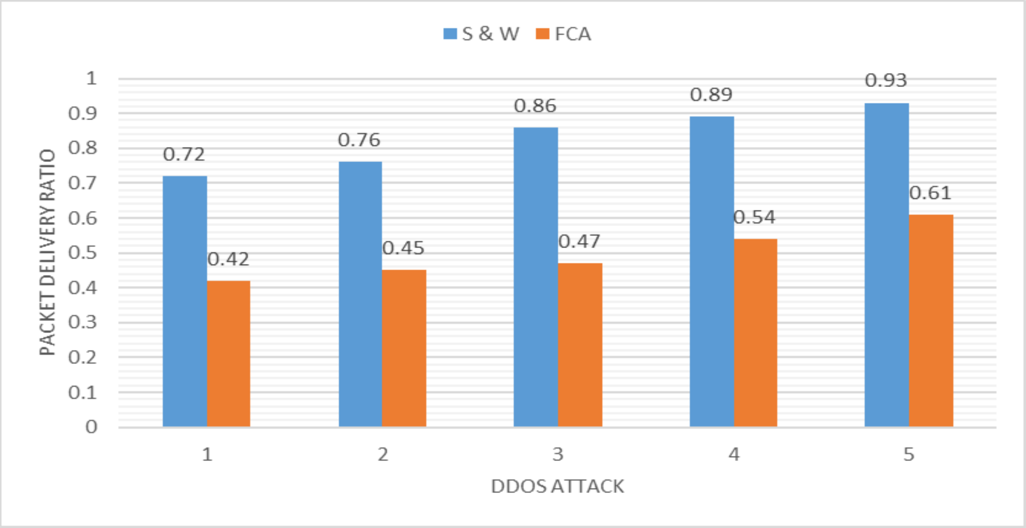


**Figure 5.3: PDR comparison S & W and FCA**

Monitoring the PDR in real-time during network operation and compare it with the established baseline PDR. Deviations from the baseline can indicate the presence of DDOS attacks. Analyze the magnitude and duration of PDR deviations to distinguish between normal fluctuations and attack-induced variations. In the table 5.2 and figure 5.4, it is observed that the algorithm should balance the sleep and wakeup durations to avoid excessive energy consumption while maintaining an acceptable PDR. If the wakeup durations are too short, the nodes may not have sufficient time to forward packets, resulting in reduced PDR. Conversely, longer wakeup durations may lead to higher energy consumption. However, as compared to FCA, PDR can save up to 63% more energy. Fine-tuning the wakeup durations and coordination among nodes can help strike a balance between energy conservation and achieving a desirable PDR for DDOS detection in the WSN. Perform data aggregation at the network level to reduce redundant transmissions. Instead of sending individual sensor readings, nodes can aggregate data from multiple sensors and transmit summarized information. This reduces the number of packets transmitted, thereby saving energy.

**Table 5.2 :Comparison of energy spent on each algorithm**

| Time(Sec) | S & W | FCA |
|---|---|---|
| 2 | 2.66 | 16.75 |
| 4 | 11.22 | 17.75 |
| 6 | 11.8 | 17.91 |
| 8 | 12.34 | 18.48 |
| 10 | 12.91 | 19.07 |

S&W can be utilized to detect the first dead node in a WSN. By periodically waking up and checking for responses from all nodes, the absence of a response from a particular node indicates that it may be the first dead node. S&W allows for energy-efficient monitoring and identification of the first node that becomes unresponsive or fails. FCA can be used to detect alive nodes in a WSN by analyzing data collected from the sensor nodes. FCA clusters the data points based on similarity and assigns membership degrees to determine the degree of belongingness to a particular cluster. By analyzing the membership degrees, FCA can identify nodes that are alive and actively contributing to the network. In the figure 5.5 and figure 5.6, the energy efficiency and adaptability are critical, S&W is used, accurate data clustering and analysis are essential.

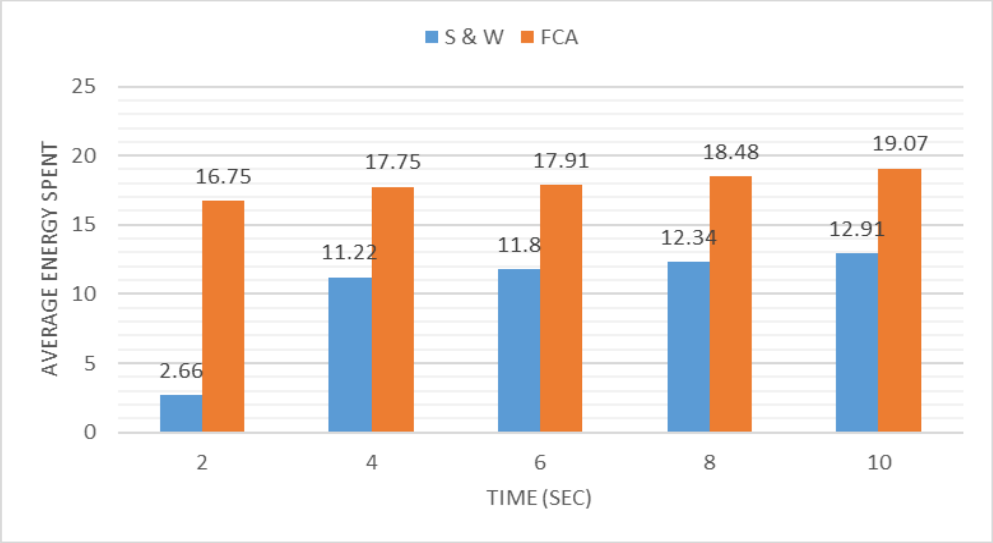


Figure 5.4 : Average energy spent on time

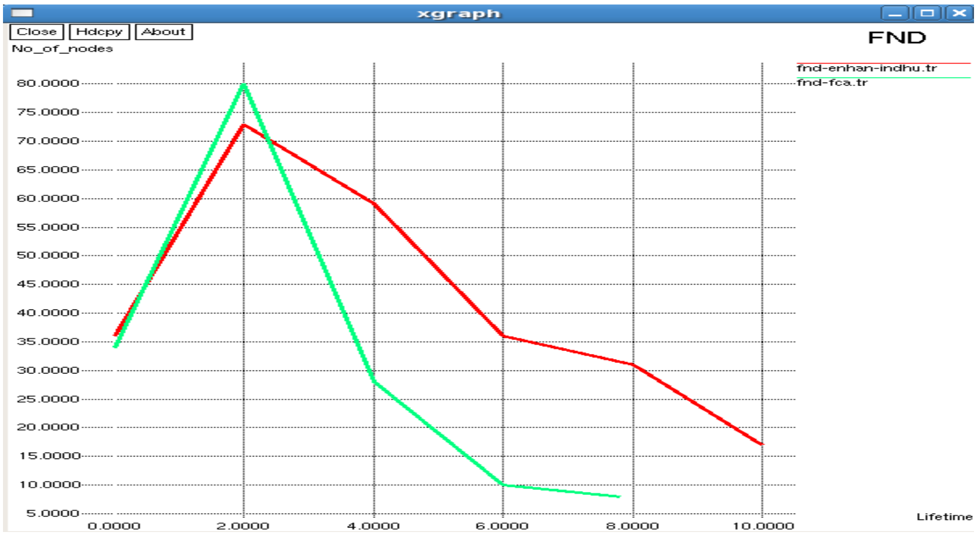


Figure 5.5 : Comparison of S&W and FCA in FND

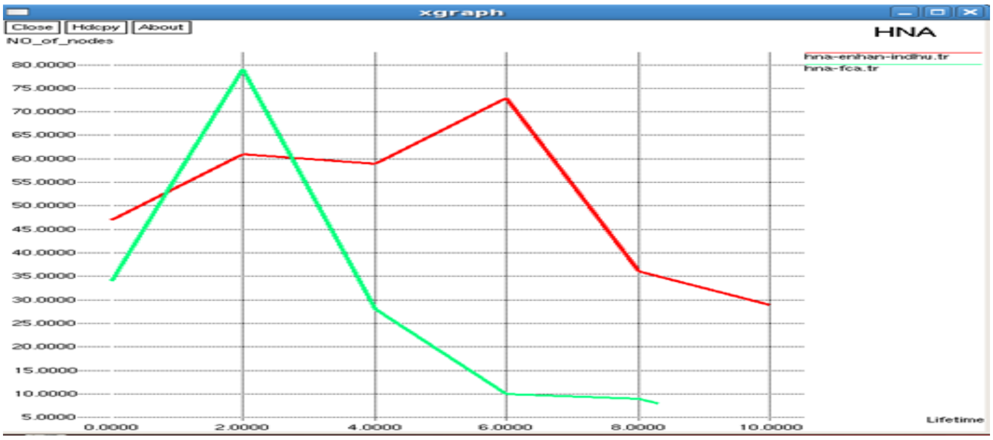


**Figure 5.6: Comparison of S&W and FCA in HNA**

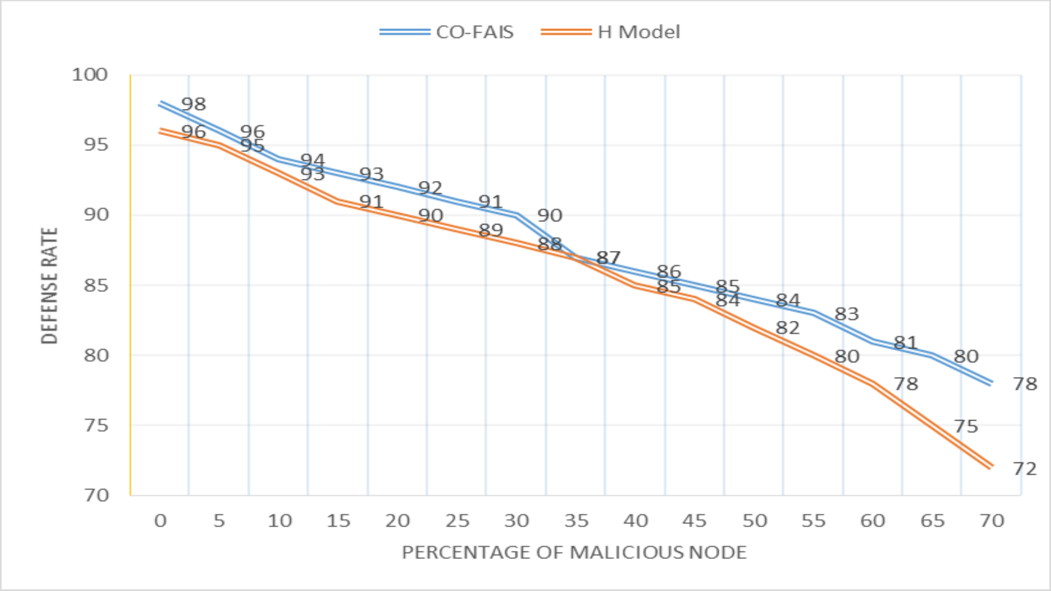


**Figure 5.7: Comparison of defense rate**

As seen in Figure 5.7, the Fuzzy Q-learning IDS assigns the sink node and base station a complementary reward/incentive functional value that is maintained. The shifting fuzzy state of a node may therefore be tracked and measured using the fuzzy reward function. The base station evaluates the essential information to modify the artificial immunity FQL settings in the case that a node is attacked or gets an anonymous communication.

The base station receives messages and evidence regarding alarm occurrences with the appropriate severity from the sink node. The base station assesses the data from the sink nodes to determine whether or not to defend nodes based on whether or not they are being attacked or in danger. A severity alert event threshold rate, V, had previously been set by the base station. After a node obtains the severity alert value exceeds v, the Co-FAIS strengthens its defenses to defend the cluster region where the node is detected at the associated base station, assuming the node to be exposed or under attack.

## 5.5 Conclusion

Discussed both the Sleep & Wakeup Technique and the FCA. When compared to the Sleep & Wake up Technique, the FCA during this work expends a lot of energy while having a low PDR and DDOS attack detection. To prolong the network lifetime, we have boosted the energy efficiency, packet delivery ratio (PDR) to improve the detection rate, and FND of HNA characteristics. Also compared to FCA, PDR can save energy up to 63%. Once the anomalous percentage grew, the recommended approach dropped from 100% to 87%. However, compared to Huang's lower success rate, the suggested technique had a greater percentage of malicious nodes discovered, giving it a better success rate for successful defense. Thus, it can be concluded that performance is superior to that of any other individual defense strategy when the fuzzy Q-learning method and the cooperative artificial immune theory are combined.

# CONCLUSION

## CONCLUSION

To address the security attacks, specifically focusing on DDOS attack identification, clone node detection, and fuzzy-based attack detection and defense in Wireless Sensor Networks (WSNs). The objective was to develop a comprehensive approach that combines fault tolerance, energy minimization, and advanced attack detection mechanisms to enhance the security and resilience of WSNs.

In this Work, for detecting wormhole assaults and DDOS attacks in wireless sensor networks, the EE-IDS and EE-IDSEP are advised. The outcomes of the simulation serve as evidence. According to the available data, EE-IDS with the STR and OSTR protocols performs better than the current EE- TSW in terms of packet delivery ratio by roughly 29% and 34%, end-to-end latency by 8.8% and 6.7%, and energy usage by 10.3% and 12.4% about wormhole assaults. When DDOS assaults are present, it performs better than EE-TS and consumes 15% less energy overall. Additionally, it raises the packet delivery ratio by 10%, the end-to-end latency by 10%, and the energy consumption by 15%, respectively. The recommended IDS has also exceeded the current IDS in terms of important IDS performance metrics including detection rate, false positive rate, and average detection time. The EE-IDS and EE-IDSEP can thus be used in a range of applications that require strong security and low energy consumption.

The most difficult operation in overlapping clusters is replica node discovery since cluster members are dispersed throughout the clusters. Adaptive weighted clustering (AWC) method, BA-DE approaches use localization and RFID to solve the issue. The effectiveness of the techniques is assessed and contrasted with LSM and RM systems. The methodologies are also discovered in non-cluster settings using K-coverage and FTVBT Wireless Sensor Network in order to evaluate the efficacy and make conclusions. When compared to the current approaches, the adaptive weighted clustering (AWC) algorithm and BA-DE are reported to have the lowest communication overhead. The proposed process, which will be used in accordance with the AODV protocol, is thoroughly compared with the existing approaches to assure its effectiveness.

In contrast to the Sleep & Wake up Technique, the FCA uses a lot of energy while having a poor PDR and DDOS attack detection. In order to extend the lifetime of the network, boosted energy efficiency, packet delivery ratio (PDR) to increase detection rate, and FND of HNA features. But compared to FCA, PDR can save up to 63% more energy. The recommended action went from 100% to 87% as the anomalous proportion grew. However, the recommended method had a higher proportion of malicious nodes found, giving it a better success rate for successful protection compared to Huang's lower success rate. Therefore, it can be said that performance when the fuzzy Q-learning is used to defend is better than that of any other individual defense technique.

## Future Enhancement

Given the spread nature of denial-of-service attacks, it is difficult to identify such malicious behavior in Wireless Sensor Networks (WSNs) using conventional intrusion detection systems. Provide a cooperative game-theoretic method called G-FQL (Game-based Fuzzy Q-learning). G-FQL combines the game theoretic approach with the fuzzy Q-learning method in WSNs. Situations involving combination defense and counterattack are examined using a game theory methodology. The base station and sink node are shown as actors with the capacity to reason. To assess the effectiveness of the approach, the Low Energy Adaptive Clustering Hierarchy (LEACH) was simulated using the NS-2 simulator.

# REFERENCES

[1] Mingjian Cui, Jianhui Wang, Meng Yue “Machine Learning Based Anomaly Detection for Load Forecasting Under Cyberattacks” IEEE TRANSACTIONS ON SMART GRID, 2018, DOI 10.1109/TSG.2018.2890809, IEEE, PP:1-11.

[2] C. Balarengadurai and S. Saraswathi, “Fuzzy Based Detection and Prediction of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network”, *International Journal of Computer Science Issues*, Vol.10, Issue 6, No. 1, pp. 293-301, 2013.

[3] Colin Urquhart, Bellekens,Xavier,Christos Tachtatzis, Robert Atkinson, Hanan Hindyand Amar Seeam “Cyber-Security Internals of a Skoda Octavia vRS:A Hands on Approach” Volume 7, 2019, Digital Object Identifier 10.1109/ACCESS.2019.2943837.

[4] Chen Peng, Hongtao Sun, Mingjin Yang, and Yu-Long Wang “A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, 2168-2216 @ 2018 IEEE.

[5] G. Jegan and P. Samundiswary “Wormhole Attack Detection in Zigbee Wireless Sensor Networks using Intrusion Detection System” *Indian Journal of Science and Technology,* Vol.9, No. 45, pp. 1-10, 2016

[6] Ying Wan, Jinde Cao, Guanrong Chen, and Wei Huang” Distributed Observer-Based Cyber-Security Control of Complex Dynamical Networks” IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS–I: REGULAR PAPERS, 1549-8328 © 2017 IEEE.

[7] Chen Zhong, John Yen, Peng Liu and Robert F. Erbacher “Learning From Experts’ Experience: Toward Automated Cyber Security Data Triage” IEEE SYSTEMS JOURNAL, 1937-9234 © 2018 IEEE.

[8] Paul M. Beach, Logan O. Mailloux, Brent T. Langhals, and Robert F. Mills” Analysis of Systems Security Engineering Design Principles for the Development of Secure and Resilient Systems” Digital Object Identifier 10.1109/ACCESS.2019.2930718, volume 7, 2019, 2169-3536, IEEE.

[9] Sukumara T, S.D. Sudarsan, Janne Starck, Timothy R. Vittor" Cyber security – security strategy for distribution management system and security architecture considerations" ISSN 2515-0855, DOI: 10.1049/oap-cired.2017.0936, June 2017, Vol. 2017, Issue. 1, pp. 2653–2656

[10] Ho JW, Liu D, Wright M, Das SK. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks. J Ad Hoc Network 2009;7(8):1476.

[11] B. Parno, A. Perrig, and V. Gligor, Distributed Detection of Node Replication Attacks in Sensor Networks, In: IEEE International Conference on Security and Privacy. 1(1) (2005) 49–63.

[12] Nasser R. Sabar, Xun Yi and Andy Song "A Bi-objective Hyper-heuristic Support Vector Machines for Big Data Cyber-Security" IEEE ACCESS, 2169-3536 (c) 2018 IEEE.

[13] S. Ramesh, C. Yaashuwanth, K. Prathibanandhi, Adam Raja Basha and T. Jayasankar, An Optimized Deep Neural Network-Based DosAttack Detection in Wireless Video Sensor Network, Journal of Ambient Intelligence and Humanized Computing (2021).

[14] Fardin Abdi, Chien-Ying Chen, Monowar Hasan, Songran Liu, Sibin Mohan and Marco Caccamo " Preserving Physical Safety Under Cyber Attacks" IEEE INTERNET OF THINGS JOURNAL , VOL. XX, NO. XX, AUGUST 2018, DOI 10.1109/JIOT.2018.2889866.

[15] LU-XING YANG, PENGDENG LI, XIAOFAN YANG AND YUAN YAN TANG "Security Evaluation of the Cyber Networks Under Advanced Persistent Threats" Digital Object Identifier 10.1109/ACCESS.2017.2757944, VOLUME 5, 2017, 2169-3536 2017 IEEE.

[16] Haris M. Khalid, Jimmy C.-H. Peng, "A Bayesian Algorithm to Enhance the Resilience of WAMS Applications Against Cyber Attacks" 1949-3053 (c) 2015 IEEE, DOI 10.1109/TSG.2016.2544854, IEEE.

[17] Guohua Wang1, Shangda Xie, Xun Zhang, Jinggeng Gao, Feng Wei, Bo Zhao, Chunying Wang and Shichao LV "An Effective Method to Safeguard Cyber Security by Preventing Malicious Data" Digital Object Identifier 10.1109/ACCESS.2017.

[18] Jianing Li, Conghuan Yang, Dechao Kong, Stuart Mann, Xiao-Ping Zhang "Methodology for P&C cyber security studies using real-time digital simulation" eISSN 2051-3305, doi: 10.1049/joe.2018.0273.

[19] C. Ramesh, C. Yaashuwanth, K. Prathibanandhi, Adam Raja Basha and T. Jayasankar, An Optimized Deep Neural Network-Based DosAttack Detection in Wireless Video Sensor Network, Journal of Ambient Intelligence and Humanized Computing (2021)..

[20] Md Masud Rana Li, and Steven W. Su "Cyber Attack Protection and Control of Microgrids" IEEE/CAA JOURNAL OF AUTOMATICA SINICA, VOL. 5, NO. 2, MARCH 2018.

[21] YU AN, DONG LIU, "Multivariate Gaussian-Based False Data Detection Against Cyber-Attacks" Digital Object Identifier 10.1109/ACCESS.2019.2936816, VOLUME 7, 2019.

[22] Jiankun Hu, Athanasios V. Vasilakos "Energy Big Data Analytics and Security: Challenges and Opportunities" IEEE TRANSACTIONS ON SMART GRID, VOL. 7, NO. 5, SEPTEMBER 2016.

[23] K. Cho, M. Jo, T. Kwon, H. H. Chen, and DH. Lee, Classification and Experimental Analysis for Clone Detection Approach inWireless Sensor Networks, IEEE Syst J. 7(1) (2013) 26–35.

[24] Ahmadi A, Shojafar M, Hajeforosh S, Dehghan M, Singhal M. An efficient routing algorithm to preserve k-coverage in wireless sensor networks. J Super computing 2013:1–25.

[25] HOON KO, LIBOR MESICEK , JONG YOUL HONG, SOON SIM YEO, SUNG BUM PAN, and PANKOO KIM "Blog Reliability Analysis With Conflicting Interests of Contexts in the Extended Branch for Cyber-Security" Digital Object Identifier 10.1109/ACCESS.2019.2942075, VOLUME 7, 2019.

[26] Kuai Xu, Zhi-Li Zhang, and Supratik Bhattacharyya "Internet Traffic Behavior Profiling for Network Security Monitoring" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 16, NO. 6, DECEMBER 2008, Digital Object Identifier 10.1109/TNET.2007.911438.

[27] Saurabh Amin, Xavier Litrico, Shankar Sastry, and Alexandre M. Bayen "Cyber Security of Water SCADA Systems—Part I: Analysis and Experimentation of Stealthy Deception Attacks" IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, VOL. 21, NO. 5, SEPTEMBER 2013, Digital Object Identifier 10.1109/TCST.2012.2211873.

[28] Yingshuai Hao, Meng Wang, Joe H. Chow "Likelihood Analysis of Cyber Data Attacks to Power Systems with Markov Decision Processes" 1949-3053 (c) 2016 IEEE, DOI 10.1109/TSG.2016.2628522, IEEE.

[29] Nong Ye, Yebin Zhang, and Connie M. Borror "Robustness of the Markov-Chain Model for Cyber-Attack Detection" IEEE TRANSACTIONS ON RELIABILITY, VOL. 53, NO. 1, MARCH 2004.

[30] Gideon Creech, Jiankun Hu "A Semantic Approach to Host Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns" IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 4, APRIL 2014, pp 807-819.

[31] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, Mostafa M. Fouda "Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks" IEEE Network, May/June 2013 0890-8044/13/$25.00 © 2013 IEEE.

[32] IZHAR AHMED KHAN, DECHANG PI, ZAHEER ULLAH KHAN, YASIR HUSSAIN, AND ASIF NAWAZ "HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems" Digital Object Identifier 10.1109/ACCESS.2019.2925838, VOLUME 7, 2019.

[33] Chunjie Zhou, Shuang Huang, Naixue Xiong, Shuang-Hua Yang, Huiyun Li, Yuanqing Qin, and Xuan Li “Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, 2168-2216, 2015 IEEE.

[34] Jiong Zhang, Mohammad Zulkernine, and Anwar Haque “Random-Forests Based Network Intrusion Detection Systems” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, APPLICATIONS AND REVIEWS, VOL. 38, NO. 5, SEPTEMBER 2008

[35] Weiming Hu, Wei Hu, and Steve Maybank, “AdaBoost-Based Algorithm for Network Intrusion Detection” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, VOL. 38, NO. 2, APRIL 2008, pp: 577-583

[36] Song Han, Miao Xie, Hsiao-Hwa Chen, and Yun Ling “Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges” IEEE SYSTEMS JOURNAL, VOL. 8, NO. 4, DECEMBER 2014, pp: 1049–1059.

[37] Hichem Sedjelmaci, Sidi Mohammed Senouci, Nirwan Ansari, “Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks “IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, 2168-2216, 2017 IEEE, pp:1-13.

[38] Dimitrios Papamartzivanos, Félix Gómez Mármol, and Georgios Kambourakis “Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems” DOI 10.1109/ACCESS.2019.2893871, IEEE Access

[39] Khalil El-Khatib “Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 8, AUGUST 2010, pp:1143-1149

[40] Nikos Tsikoudis†, Antonis Papadogiannakis*, Evangelos P. Markatos “LEoNIDS: a Low latency and Energy-efficient Network-level Intrusion Detection System” DOI 10.1109/TETC.2014.2369958, 2168-6750 (c) 2013 IEEE.

[41] HONGYU YANG AND FENGYAN WANG "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network" 2169-3536 2019 IEEE., VOLUME 7, 2019.

[42] Ai-min Yang, Yun-xi Zhuansun, Chen-shuai Liu , Jie Li, Chun-ying Zhang "Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network" Digital Object Identifier 10.1109/ACCESS.2017.Doi Number, 2169-3536 © 2017 IEEE.

[43] Saurabh Amin, Xavier Litrico, Shankar Sastry, and Alexandre M. Bayen, "Cyber Security of Water SCADA Systems—Part I: Analysis and Experimentation of Stealthy Deception Attacks IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, VOL. 21, NO. 5, SEPTEMBER 2013,pp: 1963-1970

[44] Hyun Jin Kim, Hong-Sik Kim, and Sungho Kang "A Memory-Efficient Bit-Split Parallel String Matching Using Pattern Dividing for Intrusion Detection Systems" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 11, NOVEMBER 2011 Digital Object Identifier no. 10.1109, pp:1904-1911.

[45] WAJDI ALHAKAMI, ABDULLAH ALHARBI, SAMI BOUROUIS, ROOBAEA ALROOBAEA,NIZAR BOUGUILA "Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection" Digital Object Identifier 10.1109/ACCESS.2019.2912115, VOLUME 7, 2019, 2169-3536, 2019 IEEE.

[46] IFTIKHAR AHMAD, MOHAMMAD BASHERI, MUHAMMAD JAVED IQBAL, and ANEEL RAHIM "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection" Digital Object Identifier 10.1109/ACCESS.2018.2841987, VOLUME 6, 2018, 2169-3536 2018 IEEE.

[47] Rossouw von Solms, Johan van Niekerk "From Information security to cyber security" Elsevier computer and Security, 2013, http://dx.doi.org/10.1016/j.cose.2013.04.004, pp:97-103

[48] E. Kritzinger, S.H. von Solms “Cyber security for home users: A new way of protection through awareness enforcement” Elsevier computer and Security, 2010, doi:10.1016/j.cose.2010.08.001, pp:840-847.

[49] Kaikai Pan, Andre Teixeira, Milos Cvetkovic, and Peter Palensky “Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation” DOI 10.1109/TSG.2018.2817387, IEEE Transactions on Smart Grid pp:1-13.

[50] LONGJIE LI, YANG YU, SHENSHEN BAI, YING HOU, and XIAOYUN CHEN “An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and k-NN” Digital Object Identifier 10.1109/ACCESS.2017.2787719, 2169-3536, 2017 IEEE, VOLUME 6, 2018

[51] Yihan Xiao 1 (Member, IEEE), Cheng Xing 1, Taining Zhang 2, and Zhongkai Zhao “An intrusion detection model based on feature reduction and convolutional neural networks” DOI 10.1109/ACCESS.2019.2904620, IEEE Access, 2169-3536 (c) 2018 IEEE.

[52] WALEED BULAJOUL, ANNE JAMES, AND SIRAJ SHAIKH “New Architecture for Network Intrusion Detection and Prevention” Digital Object Identifier 10.1109/ACCESS.2019.2895898VOLUME 7, 2019.

[53] Xiujuan Wang, Chenxi Zhang, Kangfeng Zheng “Intrusion Detection Algorithm Based on Density Cluster Centers, and Nearest Neighbors” NETWORK CODING AND ALGORITHM, China Communications • July 2016, pp.24-31.

[54] Fangyu Li, Yang Shi, Aditya Shinde, Jin Ye, WenZhan Song “Enhanced Cyber-Physical Security in Internet of Things through Energy Auditing” IEEE INTERNET OF THINGS JOURNAL, 2019.

[55] Fangjun Kuang, Weihong Xu,∗, Siyang Zhang “A novel hybrid KPCA and SVM with GA model for intrusion detection” Elsevier - Applied Soft Computing, (2014) http://dx.doi.org/10.1016/j.asoc.2014.01.028 , pp.178–184.

[56] Abdulla Amin Aburomman, Mamun Bin Ibne “A novel SVM-kNN-PSO ensemble method for intrusion detection” Elsevier, Applied Soft Computing, http://dx.doi.org/10.1016/j.asoc.2015.10.011 1568-4946/© 2015, pp.1-13

[57] Majjed Al-Qatf, Yu lasheng, Mohammed Alhabib, Kamal Al-Sabahi "Deep Learning Approach Combining Sparse Autoen-coder with SVM for Network Intrusion Detection" 2169-3536 (c) 2018 IEEE. DOI 10.1109/ACCESS.2018.2869577, IEEE Access.

[58] Nong Ye, Senior Member, IEEE, Syed Masum Emran, Qiang Chen, and Sean Vilbert "Multivariate Statistical Analysis of Audit Trails for Host-Based Intrusion Detection" IEEE TRANSACTIONS ON -COMPUTERS, VOL. 51, NO. 7, JULY 2002, pp.810-820.

[59] "A Cyber Security Detection Framework for Supervisory Control and Data Acquisition Systems" DOI 10.1109/TII.2016.2599841, IEEE Transactions on Industrial Informatics, 1551-3203 (c) 2016 IEEE.pp.1-10.

[60] Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi "A Deep Learning Approach to Network Intrusion Detection" IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE, VOL. 2, NO. 1, FEBRUARY 2018, pp.41-50.

[61] ADEL BINBUSAYYIS, THAVAVEL VAIYAPURI "Identifying and Benchmarking Key Features for Cyber Intrusion Detection: An Ensemble Approach" Digital Object Identifier 10.1109/ACCESS.2019.2929487, VOLUME 7, 2019, IEEE Access.

[62] HAITAO HE, XIAOBING SUN, HONGDOU HE, GUYU ZHAO, LIGANG HE, and JIADONG REN "A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection" Digital Object Identifier 10.1109/ACCESS.2019.2959131, VOLUME 7, 2019.

[63] Lin Wang, Todd Mander, Helen Cheung, Farhad Nabhani, Richard Cheung "Security Operation Modes for Enhancement of Utility Computer Network Cyber-Security" 2007 IEEE, pp.1-8.

[64] Selcuk Cevher "Multi Topology Routing Based Failure Protection For Software Defined Networks" IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2018 IEEE, pp.1-5.

[65] Gan Xu-sheng, Duanmu Jing-shun, Wang Jia-fu, Cong Wei “Anomaly intrusion detection based on PLS feature extraction and support vector machine” Elsevier, Knowledge-Based Systems, (2013) pp. 1–6.

[66] Muhammad Shakil Pervez, and Dewan Md. Farid “Feature Selection and Intrusion classification in NSL-KDD Cup 99 Dataset Employing SVMs” 2014 IEEE, pp.1-6.

[67] Junaid Akram, Luo Ping “How to build a vulnerability benchmark to overcome cyber security attacks” ISSN 1751-8709, doi: 10.1049/iet-ifs.2018.5647, Vol. 14 Iss. 1, pp. 60-71 The Institution of Engineering and Technology 2019.

[68] Dr. Tariq Mahmood, Uzma Afzal “Security Analytics: Big Data Analytics for Cybersecurity” ISBN: 978-1-4799-1288-9/13/$31.00 ©2013 IEEE, pp.129-134.

[69] Martin Husak, Jana Komarkova, Elias Bou-Harb, and Pavel Celeda “Survey of Attack Projection, Prediction, and Forecasting in Cyber Security” DOI 10.1109/COMST.2018.2871866, IEEE Communications Surveys & Tutorials, 1553-877X (c) 2018, pp.1-21.

[70] Rafał Kozik, Michał Choras, Witold Hołubowicz “Packets tokenization methods for web layer cyber security” Vol. 25 No. 1, The Author 2016. Published by Oxford University Press, doi:10.1093/jigpal/jzw044, pp. 103-113.

[71] Gaoqi Liang, Steven R. Weller, Junhua Zhao, Fengji Luo and Zhao Yang Dong “A Framework for Cyber-topology Attacks: Line-switching and New Attack Scenarios” 1949-3053 (c) 2017, DOI 10.1109/TSG.2017.2776325, IEEE Transactions on Smart Grid

[72] Guohua Wang, Shangda Xie, Xun Zhang, Jinggeng Gao, Feng Wei, Bo Zhao, Chunying Wang and Shichao LV “ An Effective Method to Safeguard Cyber Security by Preventing Malicious Data” Digital Object Identifier 10.1109/ACCESS.2017., IEEE Access, pp.1-10.

[73] Arsalan Mosenia, Susmita Sur-Kolay, Anand Raghunathan, Niraj K. Jha “DISASTER: Dedicated Intelligent Security Attacks on Sensor-triggered Emergency Responses” DOI 10.1109/TMSCS.2017.2720660, IEEE Transactions on Multi-Scale Computing Systems, 2332-7766 (c) 2016 IEEE, pp.1-15.

[74] Fan Zhang, Hansaka Angel Dias Edirisinghe Kodituwakku, J. Wesley Hines, and Jamie Coble "Multi-Layer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data" IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, DOI 10.1109/TII.2019.2891261, pp.1-8

[75] Ansam Khraisat, Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman "Survey of intrusion detection systems: techniques, datasets and challenges" https://doi.org/10.1186/s42400-019-0038-7, Springer: Cyber security, 2019, pp.1-22.

[76] Jianing Li, Conghuan Yang, Dechao Kong, Stuart Mann, Xiao-Ping Zhang "Methodology for P&C cyber security studies using real-time digital simulation" The Journal of Engineering, eISSN 2051-3305, doi: 10.1049/joe.2018.0273,pp.1130-1133

[77] Xindong Liu, Mohammad Shahidehpour, , Zuyi Li, Xuan Liu, Yijia Cao, Zhiyi Li, "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems" DOI 10.1109/TSG.2016.2545683, IEEE Transactions on Smart Grid, 2015, pp.1-8.

[78] Limei He, Zheng Yan, Senior Member, Mohammed Atiquzzaman "LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A Survey" Digital object Identifier 10.1109/ACCESS.2017.Doi Number, 2169-3536 (c) 2017 IEEE., pp.1-23.

[79] Ahmed S. Musleh, Haris M. Khalid, S. M. Muyeen and Ahmed Al-Durra "A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications" IEEE SYSTEMS JOURNAL, 1937-9234 © 2017 IEEE, Digital Object Identifier 10.1109/JSYST.2017.2741483,pp.1-10.

[80] FARHAN ULLAH, HAMAD NAEEM, SOHAIL JABBAR, SHEHZAD KHALID, MUHAMMAD AHSAN LATIF, FADI AL-TURJMAN, AND LEONARDO MOSTARDA "Cyber Security Threats detection in Internet of Things using Deep Learning approach" Digital Object Identifier 10.1109/ACCESS.2017.Doi Number, pp.1-12.

[81] HADIS KARIMIPOUR, ALI DEHGHANTANHA, REZA M. PARIZI, KIM-KWANG RAYMOND CHOO AND HENRY LEUNG “A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids” Digital Object Identifier 10.1109/ACCESS.2019.2920326, 2169-3536 2019 IEEE., VOLUME 7, 2019, pp.80778- 80788.

[82] JONGHOON LEE, JONGHYUN KIM, IKKYUN KIM, and KIJUN HAN “Cyber Threat Detection based on Artificial Neural Networks using Event Profiles” DOI 10.1109/ACCESS.2019.2953095, IEEE Access, pp.1-20.

[83] YU AN, AND DONG LIU “Multivariate Gaussian-Based False Data Detection Against Cyber-Attacks” Digital Object Identifier 10.1109/ACCESS.2019.2936816, IEEE Access, VOLUME 7, 2019, PP. 119804-119812.

[84] T.T. Teoh, Graeme Chiew, Yeaz Jaddoo, Michael H. A. Karunakaran, Y.J. Goh “Applying RNN and J48 Deep Learning in Android Cyber Security Space for Threat Analysis”PP.1-5.

[85] Emna Bahri, Nouria Harbi and Hoa Nguyen Huu “Approach Based Ensemble Methods for Better and Faster Intrusion Detection” CISIS 2011, LNCS 6694, Springer-Verlag Berlin Heidelberg 2011, pp. 17–24.

[86] Claude Fachkha and Mourad Debbabi “Darknet as a Source of Cyber Intelligence: Survey, Taxonomy and Characterization’ DOI 10.1109/COMST.2015.2497690, IEEE Communications Surveys & Tutorials, 1553-877X (c) 2015 IEEE., pp.1-32.

[87] WALEED MUGAHED AL-RAHMI, NORAFFANDY YAHAYA, MAHDI M. ALAMRI,NADA ALI ALJARBOA, YUSRI BIN KAMIN, AND MUHAMMAD SUKRI BIN SAUD “How Cyber Stalking and Cyber Bullying Affect Students' Open Learning” Digital Object Identifier 10.1109/ACCESS.2019.2891853, VOLUME 7, 2019, 2169-3536 2019 IEEE, pp. 20199-20210.

[88] Yumei Li, Holger Voos, Mohamed Darouach, and Changchun Hua “An Algebraic Detection Approach for Control Systems under Multiple Stochastic Cyber-attacks” IEEE/CAA JOURNAL OF AUTOMATICA SINICA, VOL. 2, NO. 3, JULY 2015, pp.258-266.

[89] PATRICIO ZAMBRANO , JENNY TORRES, LUIS TELLO-OQUENDO, RUBÉN JÁCOME, MARCO E. BENALCÁZAR , ROBERTO ANDRADE , and WALTER FUERTES “Technical Mapping of the Grooming Anatomy Using Machine Learning Paradigms: An Information Security Approach” Digital Object Identifier 10.1109/ACCESS.2019.2942805, VOLUME 7, 2019, pp. 142129-142146.

[90] Tomoya Enokido, Makoto Takizawa “Purpose-Based Information Flow Control for Cyber Engineering” IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 58, NO. 6, JUNE 2011, pp.2216-2225.

[91] Randy C. Paffenroth, Chong Zhou “Modern Machine Learning for Cyber-defense and Distributed Denial of Service Attacks” 0360-8581 (c) 2019 IEEE. DOI 10.1109/EMR.2019.2950183, IEEE Engineering Management Review, pp.1-11.

[92] HONGYAN LI 1,2, FENGJUN XIAO 3, AND NAIXUE XIONG “Efficient Metadata Management in Block-Level CDP System for Cyber Security” Special Section On Advanced Communications And Networking Techniques For Wireless Connected Intelligent Robot Swarms, Digital Object Identifier 10.1109/Access.2019.2948097, Volume 7, 2019,pp. 151570- 151578.

[93] Amol Borkar, Akshay Donode, Anjali Kumari “A Survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System (IIDPS)” Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017), ISBN: 978-1-5386-4031-9, pp.949-953.

[94] Gong Shang-fu, Zhao Chun-lan “Intrusion Detection System Based on Classification” ISBN: 978-1-4673-1332-2/12/$31.00 ©2012 IEEE, pp.78-83

[95] Ahmad W. Al-Dabbagh, Yuzhe Li, and Tongwen Chen “An Intrusion Detection System for Cyber Attacks in Wireless Networked Control Systems” 1549-7747 (c) 2016 IEEE., pp.1-5.

[96] Hichem Sedjelmaci, Sidi Mohammed Senouci, and Nirwan Ansari “A Hierarchical Detection and Response System to Enhance Security against Lethal Cyber-Attacks in UAV Networks” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, pp.1-13.

[97] WAJDI ALHAKAMI, ABDULLAH ALHARBI, SAMI BOUROUIS , ROOBAEA ALROOBAEA,AND NIZAR BOUGUILA "Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection" Digital Object Identifier 10.1109/ACCESS.2019.2912115,, VOLUME 7, 2019,pp. 52181- 52190

[98] Antonia Nisioti, Alexios Mylonas, Paul D.Yoo, Vasilios Katos "From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods" DOI 10.1109/COMST.2018.2854724, IEEE Communications Surveys & Tutorials, pp.1-23.

[99] ADEL BINBUSAYYIS, THAVAVEL VAIYAPURI "Identifying and Benchmarking Key Features for Cyber Intrusion Detection: An Ensemble Approach" Digital Object Identifier 10.1109/ACCESS.2019.2929487, VOLUME 7, 2019, pp. 106495-106513.