# Synopsis on

# Design and Implementation of Intrusion Detection Framework for Mobile Wireless Sensor Network

**JULY-2020**

**Submitted for registration in the degree of**

**Doctor of Philosophy**

**DEPARTMENT OF COMPUTER SCIENCE**

**CHITKARA UNIVERSITY**

HIMACHAL PRADESH

**Submitted by**

Abha Sharma

PHDENG18055

**Under the supervision of**

**Dr. Prasenjit Das**
**Department of Computer Applications**
**Chitkara University, Himachal Pradesh**

**Dr. (Prof.) R.B. Patel**
**Department of Computer Science & Engineering**
**Chandigarh College of Engineering & Technology, Chandigarh**

# TABLE OF CONTENTS

**LIST OF FIGURES** ..... **i**

1. Introduction ..... 1

1.1 Wireless Sensor Network ..... 2

1.2 Advantages in WSN ..... 3

1.3 Challenges in WSN ..... 4

1.4 MANET ..... 5

1.4.1 MANET Types ..... 6

1.5 Intrusion in Network ..... 7

1.5.1 Specific Areas of Intrusion [11-12] ..... 7

1.6 Targeted Identified Attacks for N2N Communication ..... 10

1.7 Modern Day Frameworks of Security ..... 11

1.7.1 Swarm Intelligence [19] ..... 11

1.7.1.1 Cuckoo Search Algorithm ..... 12

1.7.2 Machine Learning / Artificial Intelligence ..... 12

2. Literature Review ..... 13

3. Justification for Research ..... 27

3.1 Motivation ..... 27

3.2 Research Gap ..... 28

4. Problem Statement ..... 28

4.1 Objectives ..... 30

4.2 Methodology ..... 30

5. Expected Outcomes ..... 32

6. Work Plan ..... 33

# LIST OF FIGURES

Figure 1 A General Architecture of M-WSN [2] .....1

Figure 2 Wireless sensor network architecture [58].....3

Figure 3 Basic Structural Design of MANET [59] .....6

Figure 4 For Route discovery and Routing .....9

Figure 5 Access Control and Monitoring .....10

Figure 6 Proposed Work.....31

# 1. Introduction

Mobile Wireless Sensor network (M-WSN), is a type of wireless sensor network (WSN), that consists of small mobile sensor nodes powered by battery. Compared with their predecessors, M-WSN is an emerging research field. M-WSN has more versatility compared to static sensor nodes because these nodes can be located in any situation and respond immediately to dynamic topology. M-WSN finds application in environmental monitoring, surveillance and many more [1]. The elements composed by M-WSN are shown in Figure 1.

The architecture of M-WSN is different from the static WSN network. In M-WSN, the sink node keeps on moving within the defined field whereas in WSN the sink node remains stable.

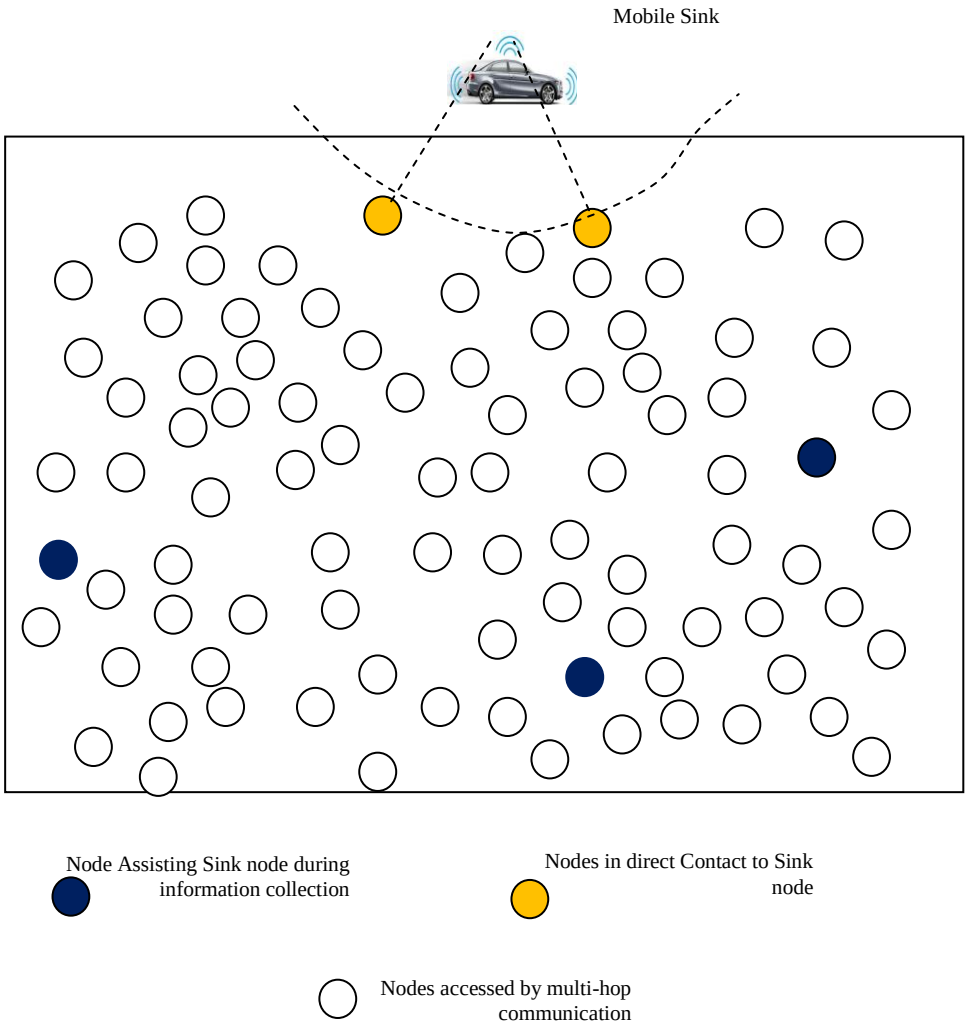


**Figure 1 A General Architecture of M-WSN [2]**

The architecture mainly consists of three types of nodes (i) Regular Nodes, (ii) Mobile Sink, and (iii) Sink Assistant Nodes. The detail description all is provided below.

Regular Nodes: These nodes are deployed in the field to sense some interesting phenomena. After collecting information, these nodes distribute their data to mobile receivers (mobile sink) in a supportive manner. Depending on the node's position in the sensor field, the node may act as a repeater, thus forwarding other data to the mobile receiver.

Mobile Sink(s): As per the application scenario, mobile sink nodes can be single or multiple. These nodes are used to collect information from the sensor field. Depending upon the availability of resources these nodes can be considered as un-constrained devices and can be implanted in robot, car or any moving device.

(Optional) Sink Assistants: Optional nodes can be implanted in some applications, that might help to the sink node during its data collection process. In static WSN, these nodes are called as intermediate nodes, as these nodes pass the collected information to the nearby node, so that the data can be transmitted from the source to the desired destination node. Whereas, in M-WSN, these nodes are designed to make sure that the entire sensor area is covered by these nodes during communication process performed for specific application.

## 1.1 Wireless Sensor Network

Wireless Sensor Network (WSN) offers a medium that can transmit signals, such as microwave, radio or satellite signals for communication process [3]. Wireless Sensors acts as a transceiver that is it receive the signal as well as transmit the signal to the destination.

WSN includes a group of nodes that are typically low in functionality. Collectively they collaborate alongside others to carry out activities during given surroundings. An invisible network of detectors may consist of a single or several drain nodes (Base Stations) to collect and share data from central nodes. Using the battery pack, each detector node is power-driven and could be classified into 3 primary functional products: the unit of understanding, the unit of contact and a processor device. Wi-Fi tools, in addition to optical computing, expanded the major event correlated with detector nodes, the new developments in micro-electro - mechanical systems development. It results in realistic viability for the specific prospect of flowering associated with WSNs [4].

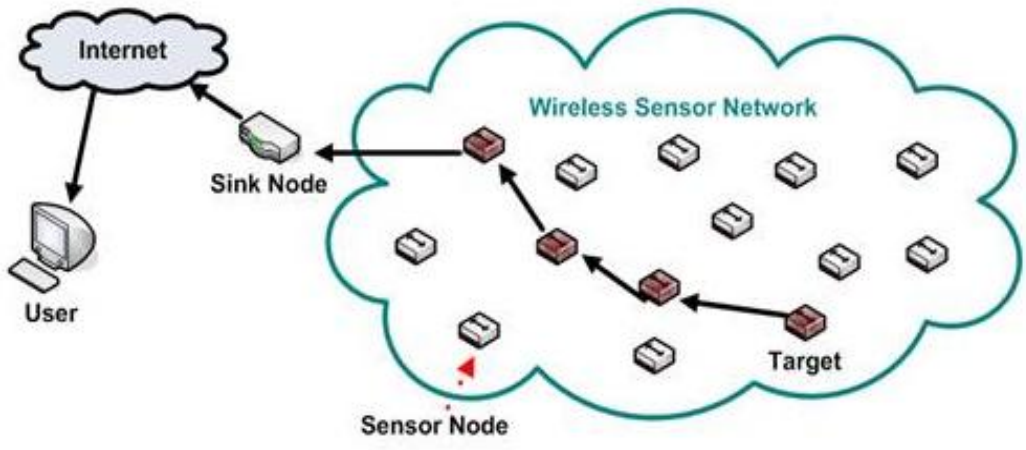


**Figure 2 A General WSN architecture [58]**

## 1.2 Advantages in WSN

Following are the advantages of wireless sensor network [5]:

i. **Energy-saving**: The Mobile Agent (MA) prevents the convergence of data as well as retrieval from the sensor to the server; information is ready when the server finally marge. This process will short the information targeted visitors from the network, help to conserve network bandwidth, decrease from one to other holdbacks and increase support responsiveness. Thus, the MA will efficiently minimize energy usage, as well as improve the longevity of the network.

ii. **Simplify network protocol;** Sensor Network is in essence a type of application-oriented network, which in turn involves simple security mechanisms, from the device layer to the network layer, as well as data communication layer to recognize the particular importance linked to different entities. Node protocols are distributed everywhere, minimizing the rates linked to node software systems, rendering complex protocols challenging to create and look after, so causing network breakdowns is an simple feat.

iii. **Flexibility and autonomy:** MA can be re-programmed; fresh agents can be inserted in the server at any time as well as redistributing duties; meanwhile, several operations may be carried out concurrently by one single sensor node. And instead, there's much more network efficiency, as well as flexibility. In fact, the mobile agent may probably recognize a different alteration of the natural world as well as easily establish reaction, and keep the device in great condition.

**Types of Network**

A network allows various systems to create link amongst themselves for communication, exchange data and share resources. Based on the needs and conditions we either need a wired network or a wireless network.

**i. Infrastructure Network**

Connection only occurs between the cellular nodes and the access points inside a network quartered around communication. The contact between wireless nodes is not clear. The access point is used here as a bridge between the wireless and wired networks to also handle the channel connection. This Network requires set base stations.

Once the node moves out of the control of one base station it comes into the control of every other base station. Cellular networks are one such example of a network dependent on the infrastructure. It's a centralized device that like a router is managed by the controller. The biggest issue with this method is that if the controller fails the whole program crashes.

**ii. Infrastructure-less Network**

In the most trivial networks (such as point-to - point links) any technique / approach is required to route the packets from the source to the final destinations. It often involves repairs along with related expenses, in addition to the exploration of roads. The routing job is assigned to trusty nodes known as Access Point. The AP architectures are slightly less complex than end-to - end nodes. Access points are somewhat like base stations which are used to map the identity of various nodes, links or dis-associations, etc., as well as to monitor traffic flow between their users which related access points. The connection point may even be connected to the Web, thereby supplying the consumers with internet connectivity.

## 1.3 Challenges in WSN

WSN faces vital issues regarding power consumption as the nodes are powered by tiny batteries. In order to reduce the power consumption the following issues have been addressed:

**a. Power management**

A wireless network consists of a large number of tiny nodes that are densely deployed inside as well as outside the environment. As the nodes are moveable and are deployed in remote or

hazardous environment. Therefore, power management becomes a serious issue in N2N communication.

**b. Routing**

Routing in N2N communication is very challenging. Till now, no global routing scheme is available that can be applied to any communication network. The nodes generate data traffic with random packet size. Therefore, redundancy needs to be exploited by the routing mechanism to enhance the utilization of bandwidth as well as energy. Also, the nodes have limited power and hence need to be utilized carefully.

**c. Localization**

Localization problem is one of the foremost issues faced by the N2N communication networks that determine the location of the deployed nodes. The data related to the node's location essential for route the information packets using localisation aware routing protocols. Manual determination of node's location is not an easy task specifically for large networks. Also, the integration of hardware such as GPS is costly as well as power consuming.

## 1.4 MANET

Mobile Ad-hoc Network (MANET) is the type of device where a remote channel that requires an access point is used for communication [6]. Restricted to the framework of remote systems where every client straightforwardly corresponds with an access station or base point, a mobile specially appointed mechanism, namely MANET that is a sort of remote Ad-hoc network.

It is a self-arranging mechanism of movable routers joined by remote connections with no entry point. Each movable device in a system is self-governing as there is no central authority in the MANET. Every device is free to move independently in all directions at MANET (Mobile Ad-hoc Network). The biggest difficulty in the construction of a MANET is to equip each system to retain the knowledge that is required to properly route the traffic. A general architecture of MANET is shown in figure 3.

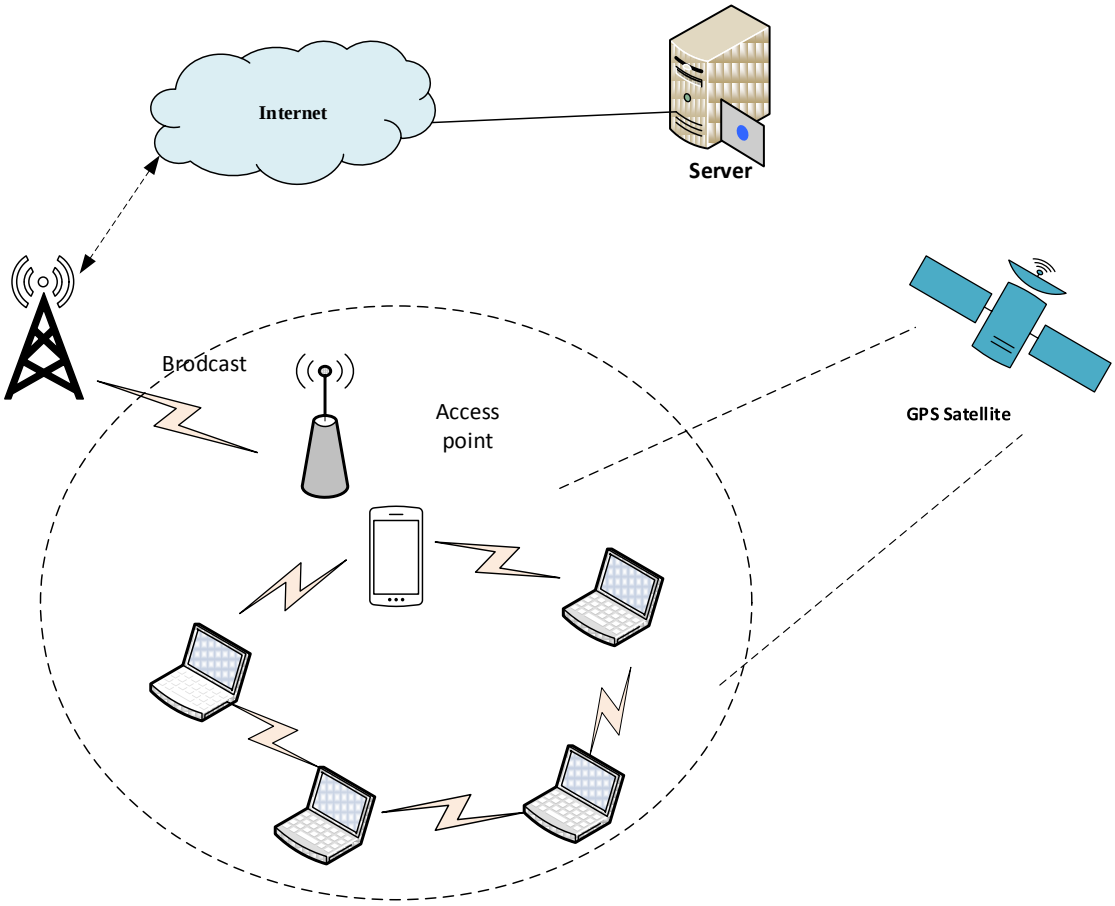


**Figure 3 Basic Structural Design of MANET [59]**

### 1.4.1 MANET Types

i. Vehicle Ad-hoc Networks (VANETs) used for connect with mobile vehicles. Therefore, the coordination is carried out even though the automobiles inside a defined region travel in separate directions [7].

ii. Intelligent Vehicular Ad-hoc Networks (IVANETs) are used in situations such as a automobile crash or some other accessibility issue.

iii. Internet-based post hoc communication networks (I-MANET) are ad hoc networks of fixed internet portal nodes linking cell nodes. Standard ad hoc routing algorithms do not directly refer to these types of networks [8].

iv. M-WSN is a combination of mobile and static wireless nodes. The mobile nodes support the static nodes in order to distribute the load in a linear procession. M-WSN can be benefited by the architecture of both WSN and MANETs, at one side WSN brings power stability into the network where as MANET bring adaptive routing strategies in order to increase the Packet Delivery Ratio (PDR).

## 1.5 Intrusion in Network

The intrusion comes into the act when false data packets are sent or received in any N2N communication. Thus, security and antivirus method are highly critical for any system or communication. Intrusions can quickly become dangerous because hubs in specific systems can guarantee many roles [9]. Some schemes are comparable to a common social network, but typically depend on different personality stereotypes that each single node relates to one individual character. Such problems usually occur when a reputational context (such as a specific reputation for record exchange on a particular system) is fooled through a disproportionately high effect on a confidence attacking node. Consistently, an attacker with a rich personality can use them for malicious behavior by acquiring information or interfering with communications. Initially described by Microsoft expert John Douceur, the intrusion depends on how the node system cannot guarantee that each processing component is an unambiguous physical node. The power is consumed during the usages of software (such as VeriSign) to establish the identity of a node on a system (or hub) using an IP location identification hub, password, and username. Intrusions occur in several situations and are widely used for trust, security, and health. Quite few companies are now utilizing Intrusions to boost Google Page Rank's enhanced evaluation. The aim of resource testing is to decide if the aggregation of identities is less frequent than when independent [10].

### 1.5.1 Specific Areas of Intrusion [11-12]

The definition of intrusion states that it is a disorder in the existing architecture which is designed to deliver the optimal solution as per requirement []. In case of MANET, WSN and M-WSN the network behavior may change due to lot of reasons as for example the battery failure of the node, routing overhead, inappropriate structure of data packet, delay in transmission etc. Some of these are briefed as follows:

i. **Routing:** Intrusions can disturb routing protocols in ad-hoc systems, particularly the multi-cast routing mechanisms. Another idea is Geographical routing, where vindictive hubs may show up at more than one spot at once.

ii. **Tampering with Voting and Reputation Systems:** In the event of any environment where there is a voting plan set up for purposes, for example, reporting and recognizing hub in the framework, intrusion may be especially unsafe. As a sample, an attacker may make enough malicious identities over and over-report. Then again,

these malicious hubs can shield themselves from constantly being evacuated as they are in a collision.

iii. **Fair Resource Allocation:** Intrusions might likewise be utilized to empower the attacker to get an excessively substantial offer of resources that were planned to be circulated amongst the interconnected nodes.

iv. **Distributed Storage:** File storage systems in shared networks and WSN networks can be traded off by the Intrusions. This is accomplished by creating the fragmentation and replication forms in the document.

v. **Data Aggregation:** Sensor network readings are processed by query protocols in a system. This is done for energy conservation. Sybil identities may have the capacity to report inaccurate sensor readings. A malicious client may have the capacity to change the destination address of data packets by its own packet address.

Ad-hoc networks like MANET, M-WSN faces significant issues in security. Many researchers have paid attention to both the fields, but due to the modern complexities of node architectures and behaviour, the work is not easy at all. Due to the mobilization factor, it becomes more sophisticated to trace the intruder in the network. To address this issue, several routing protocols have been established from time to time [13-15]. Based on the studied literature, the following fields are identified where improvisation can be done to make the data more secure.

a) Routing: The routing involves broadcasting request and selecting appropriate nodes for the transmission as shown in figure 5.
b) Node registration process: This process refers to the process of allowing a node to enter in the network in order to keep a safe routing process is referred as safe node registration process.
c) Network Monitoring: In order to run the network safe and secure, it is required to monitor the routing and the registration process. In addition to that, access control and access level grants are handled by the network monitor or the base station and the process is called network monitoring. This procedure is referred in figure 6.

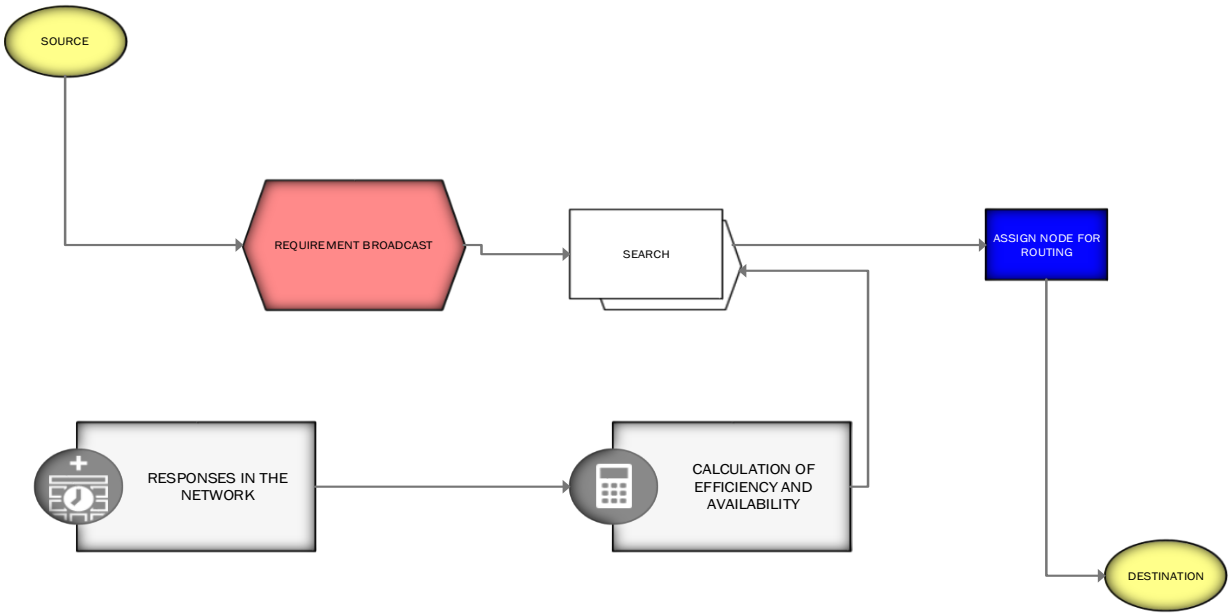


**Figure 4 Route discovery and Routing**

The routing mechanisms which are presented until now lacks in the adoption of node behaviour and also suffers from trust management issues. The routing process involves data communication from the source to the destination node. The routing mechanism majorly falls under the reactive and proactive categories. For reactive framework, it is difficult to respond to a node as per their request (RREQ) after checking all its credentials as this is a time and effort consuming. It is the role of the network manager to keep an eye over the trust issues of the network and to refresh the network after a certain time frame to register a new node or to dismiss the existence of a dead node in the network.

A node that is not responding to node requests or did not actively participate in any process is referred to as dead. The first gained attention of this research work is to develop a trustworthy network route mechanism utilizing modern-day algorithms which can well utilize the time frame while keeping the trust management on a high note.

The security factor is at risk again when a new node attempts to enter in the network. The interpolation methods are made to tackle such scenarios, but what if multiple nodes aim to register at one time from other networks. The interpolation mechanism has no such answer to this question other than verifying each node one by one. The research work considers this matter as a serious issue and attempts to solve the problem of multiple interpolations through a single calculation.

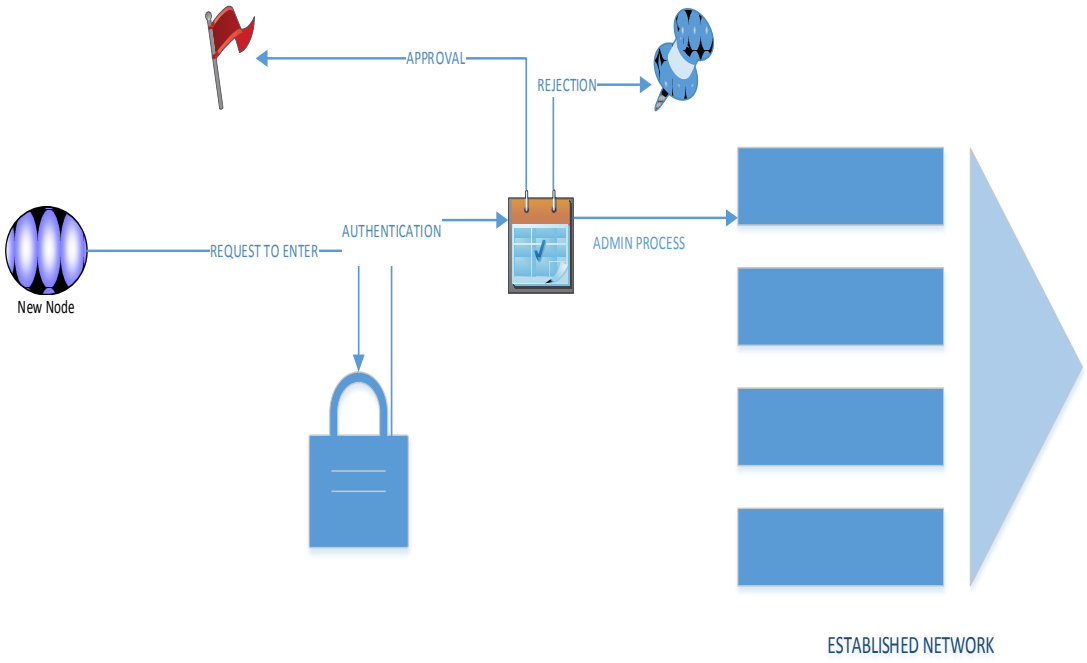


**Figure 4 Access Control and Monitoring**

## 1.6 Targeted Identified Attacks for N2N Communication

Safe transmission of data packets over the network in a secure way is need of the hour. A network is always prone to attacks which affect the performance of the network. This section discusses various attacks which are prone to end to end communication.

a) Black Hole Attack [16-17]: It is one of the most consistent and smart types of attack in any N2N or mobile communication. It slowly grabs the network and dumps the data packet in a slow and steady manner. The detection process of this attack faces a similar kind of issue as that of DDoS and replay attack. A rule-based architecture system becomes quite complex, and hence adaptive mechanism is required

b) Gray Hole Attack: A gray hole attack is an extension of a black hole attack. In this that data packet is carefully selected and dropped during the transmission over the network. Originally, the attacking nodes act as a normal node and send authentic sequence number to be a part of route. But once they are part of the route they change their behaviour during transmission.

c) Distributed Denial of Service (DDoS): This attack sends false packet information to the receiving or to the transferring node. The location of the intruder is mobile, and hence it becomes a little difficult to identify the intruder through normal rule-based architecture [18].

d) Replay Attack: Following the trend of the DDoS attack, this attack also replicates the packet information, increases the overload and delay in the network.
e) Sybil Attack: It adds a malicious node in the network which acts as a legitimate node and creates multiple identities to attract traffic towards itself, hence causing disruption in network operations [32].
f) Sink Hole Attack: This attack initiate new attacks in the network once the faulty node manage to take position in the network. The faulty node tries to pull all the traffic towards itself and tries to disturb network performance [53].

## 1.7 Modern Day Frameworks of Security

### 1.7.1 Swarm Intelligence [19]

Nature has always showed their contribution for humans to solve complex problems. Throughout the past, biology-inspired approaches have emerged in other areas of study, such as electronics, computer science, economics, medicine and social sciences. Similarly, other biologically based strategies for detecting harmful behavior inside the network have been suggested. One such approach is swarm intelligence.

Swarm Intelligence is a study of the behavior of the elements that exist in nature, for example, Particles, Cuckoo, Chicken, Firefly Buffalo, etc. Some of the recent studies have focused on cuckoo search is a swarm-based intelligence algorithm, which allows a reduction in population size of the sample data. Unique egg comparison algorithm architecture demonstrates the collection and rejection of eggs of the cuckoo bird. The surprising fact of this algorithm is that selection threshold may or may not vary from one nest to another [20]. This architecture boosts the categorization of intrusion.

The approaches, strategies, and algorithms used in this research field was influenced by the nature of humans, birds, and fish, and their unique capacity to overcome complicated challenges in communities, while at the human level it seems difficult to do so. It is true that individual ants, bees and even birds and fish as individuals seem to have very little intellect, yet when they communicate with each other and the natural world, they seem to be able to perform challenging tasks, such as seeking the shortest food route. As a result, origins coordinate their colonies, synchronize their flight, and fly at high speed as a single cohesive force. This feat would become much more significant if one realizes that, in the presence of a central organization, they have accomplished such activities without guiding any other

actions. The application of this method can be found in the NP hard optimization problem, such as detecting intruder, to select best pixel in image processing, vehicle routing, etc. In this researcher we will plan to use Cuckoo search (CS) as a swarm intelligence approach. The detail description of CS is provided below.

#### 1.7.1.1 Cuckoo Search Algorithm

This algorithm is inspired from the behavior of cuckoo bird. The eggs lay in the nest of cuckoos represents the solution to the defined problem. Each cuckoo lay eggs in the nest and each egg represents a specific solution for the defined problem. The aim of this algorithm is to provide a new solution, by replacing the worst solution present in the nest. The steps followed by CS algorithm are listed below.

a) ***Initialization Phase:*** Initially, random population of eggs ($e_n = 1,2,3, \dots \dots n$) is generated.
b) ***Generating new Cuckoo:*** In this phase, new levy flight is utilized for the generation of new cuckoo. The evaluation of objective function is performed to determine the quality of solution.
c) ***Fitness Function Evaluation:*** In this phase, the evaluation of fitness function is performed to identify the optimal solution.
d) ***Update Phase:*** in this phase, a novel solution is formed.
e) ***Discard Worst Solution:*** In this phase, the worst solution is rejected, and the best one value is considered as optimal solution.
f) ***Stop Criteria:*** In this phase, the rejection process is repeated until the maximum recurrence is completed. Additional processing in the algorithm is performed by selecting the optimal solution [21].

### 1.7.2 Machine Learning / Artificial Intelligence

Machine Learning is an adaptive method that learns from the environment and its behavior. This architecture can be applied in any field. Generally, it comprises of three layers

i. Input Layer: Intakes the data
ii. Hidden Layer: Converts the data into an environment which can be processed in the learning mechanism
iii. Output Layer: Provides the conclusion of Input and Hidden Layer

The good part of this architecture is that it can be trained to utilize any feature of the network. Although providing multiple suitable features can enhance classification accuracy. The entire process is categorized into two sections, namely Training and Classification [22].

## 2. Literature Review

In N2N communication, data is transmitted from one node to another node. In such scenario, the nodes are communicated with different coordinate positions. Therefore, the node deployment, routing of data packet to the desired node is necessary. In this section, the work performed by various researchers focussing to save energy, develop techniques to protect network from intruder and management through interpolation is presented.

In [23], the author discussed a predictive model to estimate the mobility as well as the remaining energy of the nodes positioned in the M-WSN. Here, the network is designed in MATLAB tool that consists of a BS with 21 number if SN that were clustered in an area of $150 \times 60m^2$. The designed model has analysed the effect on remaining energy of SN with respect to the transmission distance. Also, the effect of inter and intra-cluster movement has been analysed against the mobility factor of SN.

In [24], the authors have focused on to resolve the problem of packet loss in MWSN network using LEACH-MT2FL clustering approach. This approach is the enhancement of Type-2 Fuzzy logic approach. In this approach route is formed using a well-known LEACH approach, and the selection of CH has been performed using Fuzzy logic. From the results it has been observed that the proposed approach performed with better performance parameters evaluated in terms of PDR, network lifetime, and energy consumption [24].

In [25], the researchers have proposed an enhanced mobility-based GA (Genetic Algorithm) approach that helps to resolve the difficulty of PDR in MWSN and hence enhance the network stability time. Here, GA has been used to find the best location of CH along with the total CH's present in the network. Time allotment has been performed by the mechanism using Time division Multiple Access (TDMA) scheme for those nodes that were moving out from the network. From results an enhanced performance has been obtained in terms of network parameters.

In [26], the authors have used game theory in addition to clustering algorithm. The proposed algorithm, utilized energy in an optimized manner in heterogeneous mobile sensor network. An energy efficient clustering approach has been used for the selection of appropriate CH and later on examined the performance. The proposed approach has been able to lessen the hot spots in the network, that results in minimization of delay. Overall, the authors have concluded that the performance of the proposed work is improved against the baseline methods.

In [27], the authors have presented an enhanced Artificial Bee Colony as a swarm inspired approach applied for the detection of intruder in WSN system. Later on, the author has used SVM as a machine learning approach to distinguish normal and intruder node with reduced false alarm rate. The author has divided the entire network in different cluster each contained a single Cluster Head (CH) as a master node. The clusters are also dived into two types normal and abnormal. The cluster, whose CH distance is larger than the other existing clusters, is categorized as abnormal cluster. Based on this, SVM is trained and tested during communication process.

In [28], the scholars have discussed an integrated approach using Artificial Immune System (AIS) for anomaly detection in WSN. Here, Tissue Growing Algorithm is used to detect anomalies and then a secure data transmission takes place. The selection of nodes in the route has been performed by predicting the tissue with higher capacity cell. The nodes, which includes week cell are ignored and considered as intruder. The designed algorithm performed well compared to the existing approach by detecting intruder with better performance parameters.

In [29], the authors explored the problem of implementing clustering in M-WSN has been resolved using mobility aware hierarchical approach. The mechanism is based on three-layer clustering architecture that includes mobility aware centralized and hybrid clustering algorithms. The results show that an improved M-WSN performance has been determined in terms of determined parameters.

In [30], the researchers proposed Restricted Boltzmann computer-based clustered IDS (RBC-IDS) to undertake comparative study of the usage of IDS deep and machine learning applications in wireless sensor networks (WSNs). RBC-IDS output is analysed as opposed to current adaptive IDS focused on machine learning called as the Adaptively Controlled and Clustered Hybrid IDS (ASCH-IDS). And the findings obtained indicate that RBC-IDS and

ASCH-IDS deliver the same accuracy performance by the time RBC-IDS is identified nearly twice that of ASCH-IDS. The scheme proposed developed detection rate (99%) and accuracy (99.9%) for three secret layers.

In [31], the authors presented a solution to resolve the issues related to the coverage in M-WSN by presenting two sensor development mechanisms named as blind-zone centroid-based scheme (BCBS), and disturbed centroid-based scheme (DCBS) respectively. The aim of these approaches is to determin the destination location of SN so that the coverage holes can be heals effectively. Here, BCBS have used blind Zone polygon mechanism to find out the position of the source node with its nearby nodes. The centre point of the polygon method is considered as target location with respect to other sensor nodes. On the other side, DCBS technique, finds the coverage holes in every round from using the centroid based approach.

In [32], the researchers explored a dynamic scheme to identify sybil node in M-WSN. The information regarding to the malicious node has been observed during the distinct time slot using J-SIM simulator. The algorithm is processes into two parts. The first part includes traffic monitoring whereas, the attack detection has been performed into the second part of the algorithm.

In [32], the authors presented a new deep learning technique for the identification of intrusion was presented in this paper. An unsupervised feature learning scheme with a non-symmetric deep autoencoder (NDAE) has been used. The design has been implemented using the Graphical Processing Unit (GPU) that utilized KDD Cup 99 & NSL KDD dataset. The results have been found improvement compared to the existing work.

In [34], the authors presented a scheme to minimized the problem of high energy consumption in M-WSN using Cross-layer Energy Efficiency scheme. The scheme utilized three layers of the network model including MAC layer, physical layer and information of node location in the network. The results prove that the proposed scheme perform well with reduced energy consumption and high network performance [34].

In [35], the researchers have presented an auto organised and dynamic clustering approach to monitor relays in the M-WSN. The mechanism split the entire network into a set of clusters known as service zone. This helps to minimize the routing overhead, delay by utilizing bandwidth in an optimized way. The clustering mechanism also helps to manage load in the network. The cluster formation in small network reduces the buffer overflow and energy

depletion problem. From the experiments, it has been proved that the PDR, delay, energy consumption has been improved by 10 %, 15%, and 53% respectively. The improvement in the life of the network has been increased by 53 % with an energy balance of 51 %.

In [36], the researchers have given lightweight algorithm to identify the mobile sybil attacker node in M-WSN. The researchers have used two kinds of sensor nodes, Watchdog Nodes (WNs), and sensor Nodes (SNs) that are distributed randomly in the network area, in order to detect the sybil nodes. SNs function is to collect data, and send that data to the base station. Whereas, WNs is used to monitor the traffic of network and responsible for sybil node detection. From the simulation results, the network offers detection accuracy against sybil attack is 94 % [36].

In [37], the authors presented alow cost communication scheme has been applied to localize nodes in M-WSN. In wsn, the information related to the location of nodes is very essential to detect the attacker node or to collect information. Here, two types of monte Carlo schemes have been used to determined the location of nodes one scheme obtained information through anchor node and other is used both normal as well as anchor scheme. The utilization of both schemes anchors as well as normal enhances the accuracy but also increases the communication cost.

In{13], the authors have proposed a new fault-tolerant routing procedure in order to lower the data packet lost caused due to route breakage. The proposed mechanism discovers alternate routes to successfully transmit data whenever the ability of any intermediate node gets challenged. The simulation studies of the designed system were done in NS2. The network was tested against variable traffic levels and a variety of flows in terms of latency time, packet decline, packet transmission ratio, and energy usage calculated against. The suggested concept has been seen to have outperformed the current research in terms of measured output matrices.

In [10], the researchers have demonstrated a Hybrid Intrusion Detection System (IDS) for clustered WSNs on the basis of functional reputation and the rule of misuse. The main principle is that each sensor node determines its neighbors' credibility values by monitoring their behaviors. Base Station (BS) identifies hostile nodes by combining possible integrity values with harassment laws. The simulation result shows that the proposed solution enhances the network lifetime and strengthens sensed data freshness by centralizing the identification of malicious nodes by increasing energy consumption.

In [11], the researchers have addressed confidence-based intrusion detection utilizing multi-attribute assurance measures to improve detection accuracy. The confidence of sensor networks (SNs) is evaluated through cluster heads (CHs) and the confidence of CHs is analyzed through neighboring CHs whereby the difficulty of the evaluation was reduced without any evaluation through the network's various overall CHs.

In [17], the scholars explored a novel successful group-based scheme for detecting and avoiding massive black hole attacks in WSNs has been introduced. Here, all WSNs are classified into different groups, and each cluster has a fixed high-level sensor node known as the cluster head, which is responsible for detecting nodes attacked by a black hole. This mechanism achieved in the term of detection rate of 90% and an improved false-positive rate of 3.75% compared to the previous study.

In [38], the authors described the wireless Ad-hoc routing protocol's interoperability. Interoperability operates in the same manner as it will transmit messages to a neighbouring network in case of more than two different networks, even if they use distinct routing protocols. This work focused exclusively on the constructive Strip Interoperability process, which has proved to cross numerous networks through layer 3 protocols. Use IPv6 and several other related protocols, the testbed of this research carried out on Ubuntu Linux and wireless Ad-hoc routing protocols, and the implementation of OSLR and BMX6.

In [39], the researchers have proposed a routing protocol to detect and prevent from selective black hole named as Modified Dynamic Source Routing (MDSR) protocol. A selective black hole attack is a type of black hole attack that has packets dropped in a way that is selectively dropped by malicious nodes. If any kinds of the anomaly are detected, the adjacent IDS node informs all nodes of the network to remove this defected node from the network.

In [40] the autors explored a well-known routing protocol Ad-hoc On-demand Distance Vector (AODV) has been presented in this paper that works in addition with Artificial Neural Network (ANN) for MANETs. To measure AODV's reactive routing protocol's Hello message frequency to boost the efficiency of the MANETs. The researchers also defined an ANN 's design and modeling through Verilog Hardware Descriptive Language (VHDL) and implemented ANN 's hardware using Field Programmable Gate Arrays (FPGA).

In [41], the scholars have focused on to analyses the performance of sensor networks while the nodes were deployed for environmental monitoring. The main purpose of this paper is to

connect the effect of separation the malicious nodes in those networks. The authors have focused on routing protocols that are rely on tree dependent topology in which the data is sent through the sensor node towards sink node via tree rooted on the sink. The routing tree was believed to be established by hop-distance towards the sink. Protocols, namely, RESIST-1 as well as RESIST-0, are analyzed for increasing network resilience by means of whole sink attacks. The risk factor is introduced for measuring the selective forwarding impact.

Inspired by the tremendous applications of random-walk proximity and to decrease the counts of the process related to the calculation of proximity, genuine efforts have been made. Structural and numerical attributes of the problem are used to lessen process counts. Based on speeding up the convergence of the underlying iterative process, the authors used an alternative approach of Chebyshev polynomials names as Chopper. Traditional iterative procedures used the outcome of the previous iteration to calculate the next iterate. When convergence is observed, the iterations are stopped, i.e., when the proximity vector does not show any significant change between two operations, convergence halts there. Chopper outperforms existing methods significantly by computing the coefficients of linear combination, making converging faster than iteration in the original formula. This reflects significant promptness in the calculating scores of random walk-based proximities.

**Table 1 Some literature cited works and their outcomes**

| **Reference** | **Proposed Work** | **Technology** | **Study Outcomes** | **Handled attacks** | **Drawback** |
|---|---|---|---|---|---|
| **Zardari et al. (2019) [42]** | Proposed a prominent method for MANETs called black and gray hole attacks dual attack detection (DDBG). | The proposed DDBG method selects an interference detection scheme (IDS) with two additional features. | The proposed DDBG method is an effective approach to detecting black and gray hole attacks. | Greyhole and Blackhole attack | Developed mode is only applicable for the detection of black and gray hole attacks during the simulation but need to prevent the network from other attackers also and to make a environmental free WSN model to |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | sense the data for all applications. |
| **Muhammad et al. (2019) [43]** | Demonstrated two types of MANET protocols which belong to different routing protocol categories; as a reactive protocol and as a proactive protocol based on energy consumption and quality of service (QOS). | Destination-Sequenced Distance-Vector (DSDV) Optimized Link State Routing (OLSR) Ad Hoc On-Demand Distance-Vector (AODV) and Dynamic Source Routing (DSR) | Proactive protocols perform better in a static network. | N/A | The drawback is that proactive protocol consumes more power than reactive protocol. |
| **Gorine et al. (2019) [44]** | Three different types of attacks, such as self-centered, gray hole, and black hole attacks, were proposed. | AODV and DSR | The results shows that AODV performed better than DSR under selfish nodes but under blackhole attack DSR performed better than AODV. | Grayhole and Blackhole attack | N/A |
| **Gurung & chauhan (2019) [45]** | Proposed a new methodology that justifies the effects of the | Mitigating the Gray hole Attack Mechanism | In this network, the key assumption is that all nodes are | Grayhole Attack | N/A |

| | | | | | |
|---|---|---|---|---|---|
| | gray hole attack. | (MGAM) implemented Various special nodes called G-IDS nodes placed in MANETs. | confidential but in actual circumstances, some nodes can be malicious node. | | |
| **Singh et al. (2019) [46]** | Discussed some significant method used to identify black hole attacks in MANETs using AODV routing protocol. | AODV Protocol | The simulation result shows that the data packet loss increase if number of blackhole increases linearly. | Blackhole, grayhole Attack | **N/A** |
| **Saudi et al.(2019) [47]** | Investigated about the performance of four MANET protocols', namely the Ad Hoc On-Demand Distance Vector (AODV), Destination-Sequenced Distance-Vector (DSDV), Dynamic Source Routing (DSR) and Ad Hoc On-Demand Multipath Distance | AODV, DSR, AOMDV techniques | The simulation result shows that the AOMDV and DSDV protocols show better results in terms of throughput and packet delivery ratio. | N/A | **N/A** |

| | | | | | |
|---|---|---|---|---|---|
| | (AOMDV). | | | | |
| **Abdel-Azim et al. (2018) [16]** | A model to mitigate the effect of a black hole attack. | Genetic Algorithm in Integration to Fuzzy with a neural network (NN). | In the case of a black hole attack, it was concluded that the PDR was less than the PDR obtained with the application of the proposed IDS. | Blackhole Attack | It is observed that attacks significantly reduces PDR to 56% that shows that the system demonstrated poor performance in presence of black hole, gray hole attacks and high-speed mobility. |
| **U. Ghugar et al. (2018) [48]** | They have proposed an IDS to measure degree of trust in WSN. | The implemented method has proved successful in detecting abnormal nodes (DoS attack) within WSNs. They also used the periodic jamming assault to observe PL-IDS results. | The result shows that accuracy of detection at density 20 is 84% and false detection rate is 15.8% and followed by density at 40 is 88.6% and false detection rate is 11.4% and density at 60 is 94.2% and false alarm rate is 5.8% respectively. | Jamming Attack, DoS Attack | The IDS has been designed only for physical layer not for another network protocol layers. |
| **S. Otoum et al. (2017) [49]** | The authors introduced a hybrid | The presented architecture had | The study shows that sensor nodes with a sensitivity | N/A | False Negatives may occur when it is solely employed |

| | | | | | |
|---|---|---|---|---|---|
| | architecture to detect disruptive activity between network sensors that monitor systems such as climate, medical, and intelligent networking. | implemented the Enhanced Density-Based Spatial Clustering of Applications with Noise (E-DBSCAN) and Random Forest (RF) scheme. | of 99.73% and a total accuracy of 98.95% are described. | | as intrusion detection method |
| **R. Singh et al. (2017) [12]** | Researchers have proposed an advanced hybrid intrusion detection system (AHIDS) to automatically detect WSN attacks. | AHIDS uses a cluster-based architecture with an improved LEACH protocol to reduce the power consumption of sensor nodes. Together with the Multilayer Perceptron Neural Network, AHIDS utilizes anomaly identification and abuse identification based on | The results covered the various kinds of attacks such as Sybil attack, wormhole attack, and hello flood attack with different accuracy and false-positive rate. | Sybil Attack, Hello flood Attack, Wormhole Attack | Detailed simulation of various attack scenarios was not given to assess the efficiency of the proposed work. |

| | | | | | |
|---|---|---|---|---|---|
| | | fuzzy rule sets. | | | |
| **X. Jin et al. (2017) [50]** | Authors had presented an intrusion detection system to accomplish a higher rate of detection and low false-positive rate | To achieve this goal, they built a multi-agent model both at the cluster heads and at ordinary sensor nodes. In the process, trust value of the nodes was computed based on the combination of beta distribution and tolerance factor for detection of nodes attacked with intrusions. | The study outcomes showed that detection rate is enhanced with reduced PR even when different kinds of intrusions are present. | Blackhole, Sinkhole, Wormhole, DoS attack | N/A. |
| **A. Basan (2017) [51]** | They established a reliability assessment technique to estimate the values of the node workload and the remaining | In the detection scenario of harmful node based on their properties, threshold based analysis mechanism | It was observed that if the number of defected nodes exceeding 70%, the accuracy also decreases. However, in the case of thousand | Active attacks, Sybil and DoS Attacks | N/A |

| | | | | | |
|---|---|---|---|---|---|
| | energy. | allowed to calculate the probability of compliance with the interval of reliability. | nodes, the attacker could not even attack 50% of the nodes and allows the malicious content to be detected and blocked. | | |
| **Ozcelik et al. (2017) [10]** | Proposed a hybrid Intrusion Detection system for clustered WSNs. | Base Station (BS) detects malicious nodes by combining functional Functional Reputation values with Rules for Detection of Misuse. | The simulation result shows that carrying control packets is not important in the realization of the implementation scheme. | N/A | The proposed design lacked a comprehensive simulation platform that could reflect its reliability. |
| **Sajal Sarkar and Raja Datta (2017) [52]** | Proposed a routing parameter known as the Mobility factor that is calculated based on pause moment, direction and velocity of the mobile node. | MARP, MLR, AODV, DSR techniques | The simulation trials show that DSR and AODV protocols have achieved better results gains relative to their main variants and MLP, MARP protocols. | N/A | N/A |
| **Boddu et al.** | Using a new | The energy | The result shows | N/A | Current work needs |

| | | | | | |
|---|---|---|---|---|---|
| **(2017) [13]** | route discovery and exploitation method, It proposed a multi-way routing protocol to reduce packet loss due to route interruption. | efficient algorithm is used for increasing network lifetime. | that proposed protocol achieves better throughput and packet delivery ratio with reduced delay, packet drop and energy. | | to be improved in terms of reduction of overhearing in order to efficiently manage energy requirements during route discovery process. |
| **Keerthana and Padmavathi (2016) [53]** | They had presented an IDS to detect sink hole attack in WSN. | The enhanced swarm-based approach was -used that combines Ant Colony Optimization (ACO), and Particle Swarm Optimization (PSO) approaches. | The effectiveness of the proposed work is demonstrated via comparison between individual ACO, PSO and hybrid EPSO. | Sinkhole Attack | N/A |
| **Abdul et al. (2016) [54**] | Demonstrated a protocols Low Energy Adaptive Clustering Hierarchy (LEACH) and Power-Efficient Gathering in Sensor Information Systems (PEGASIS) for | LEACH | P-LEACH provides better results in terms of energy and lifetime of network rather than LEACH and PEGASIS protocol. | N/A | N/A |

| | | | | | |
|---|---|---|---|---|---|
| | reducing energy consumption in the network. | | | | |
| **Aldaej, & Ahamad et al.(2016) [55]** | Aggrandized Ad hoc on-demand distance vector routing (AODV) is introduced here to identify the amount of synergistic and non-synergistic attacks and to avoid them. | Ad-hoc on demand (AODV) | To meet the increasing demand for MANET security, different algorithms and protocols have been created and developed, but there is still space for improvement to create a more secure and stress-free communication. | N/A | The drawback is that in this work doesn't improve the AAODV protocol to overcome the problems. |
| **Brar et al. (2016) [56]** | Described MANET 's layered architecture, its applications and a brief summary of the work done to protect the network from Gray Hole attacks in this particular area. | Ad hoc on demand Distance Vector (AODV) routing becomes one of the several protocols often becomes an easy victim to this type of attacks. | The result shows that the greyhole attack reduce the performance in the terms of Packet efficiency and throughput. | Greyhole Attack | The main disadvantage is that the gray hole is very difficult to judge, because sometimes they acted as a normal node, but sometimes they threw selective packets. |

| | | | | | |
|---|---|---|---|---|---|
| **Siddharth Dhama et al. (2016) [57]** | Suggested a system to prevent and detect Black Hole attacks. AODV (Ad hoc on-demand vector range routing) protocol was used by them. | IDSAODV Routing Protocol | AODV simulation has less packet loss, but packet loss increases to 88% in the case of black hole and when the IDSAODV in the similar network is used, the packet loss is reduced up to 66%. | Blackhole Attack | N/A |

## 3. Justification for Research

This research work aims to provide an improved solution to the problems triggered by malicious activities in the N2N communication. In recent technological developments, the networking is one of the rapidly growing fields. It can be expanded in terms of number of nodes and network scale. The network composed of different elements, such as network management, network security, network applications, and many more. By observing and monitoring the node's activities, the behaviour of nodes (normal and abnormal) can be identified. In order to provide complete security against various attacks, it is necessary to provide authentication in each level of data transmission layer. This research aims to design a wireless network with minimum threat to security using swarm intelligence approach with machine learning approach.

### 3.1Motivation

The research work has its own impact in practical as well a scientific relevance. In this research, a model for Node to Node (N2N) communication in the wireless network will be presented because it has gained lot of attention from all over the world. Survey of existing works in relevant field shows that it is hard-to-find the intrusion in the network due to their

different behavior and development of secure strategy for communication. Moreover, scientific literature on the detection of the intrusion and network prevention from them is scarce, so this research will try to fill that gap by utilizing the concept of Machine Learning aiming to solve the existing issues raised in N2N communication in wireless as well as Ad-hoc network. In addition to this, the concept of Meta-heuristic approaches like Swarm Intelligence techniques will be integrated with network to establish an optimal routing.

## 3.2Research Gap

Based on the study made in the literature survey, it is observed that, a M-WSN network is made up of mobile and static nodes. The mobile nodes are there to assist the stationary nodes if they are overloaded or might be under threat. There are two issues which were addressed in terms of the security concerns. First and foremost issue is that, it cannot be directly justified that whether a mobile node is true node or it is under the influence of any other node which might be causing harm to the network. Second, whether the help seeking node genuinely requires support or it is a kind of false alarm which is raise by the intruder. Some amazing work has been carried out but obviously there are co-relations and issues in the works which have been carried out. The identified gaps are as follows.

a) In the integration of WSN and MANET, both clustering and routing can be enhanced rather than taking the traditional clustering approaches [54, 55, and 57].
b) Usage of Swarm Intelligence is observed in order to enhance the performance of detection in WSN but it could have been also used to enhance clustering [53].
c) The concept of multiway routing is also observed which enhances the route mechanism by introducing the mobility factor to it but again misses out on the enhancement part of machine learning [13, 52].

# 4. Problem Statement

Node to Node (N2N) communication is one of the recent fields of research that has gained attention from all over the world, whether it is the research industry or the commercial industry. N2N communication may involve two or more nodes interacting with each other in order to transfer the data from one end to another. Automation in any field significantly reduces human effort and leads to the production of efficient result. There are several issues

existing with the automation technique in the field of N2N communication. The N2N communication can be viewed in a network "Net" with "n" number of nodes following a communication protocol "P". As mobility is an integrated part of the N2N communication, security concerns like threat prevention and handling of data volume above a given threshold becomes a common practice in such networks. A network becomes more prone to security threats when mobility becomes an essential part of the network. The network administrator will have to put a lot of manual effort in order to understand what exactly is right or wrong. Some of the previous research architectures have tried their hands in solving the security measures by applying the rule set architecture which have proved to be successful for small set of networks. As the scalability comes into play, it becomes hard to manage thousands of rule-set at one time. In addition, it takes a lot of time to scan thousands of rules at once, which increases the delay in network. Delay could be defined as the unnecessary time which is spent in order to transfer the data. It can be also termed as the difference of the actual time consumed in the network and the expected time consumed in the network in order to transfer the data packets. Distributed Denial of Service (DDoS) attack is a commonly observed security threat in N2N communication network in which the server faces a lot of service requests which often goes out of the boundary limit of the serving capacity and that leads to either deadlock or packet dumps which eventually reduces the Packet Delivery Ratio (PDR). The PDR can be represented as follows:

$$PDR = \frac{Receive\ d_{Packet}}{Sent_{Packets}} \qquad (...1)$$

Gray hole attack is another similar intrusion that follows a similar architecture as that of the DDoS attack. As for example, in gray hole attack agrees to sends the same packet to keep the server busy in order to manage the packet identities. Black hole attack in a similar fashion sends false packets to the receiving node. The world is leading towards Machine Learning and aiming to solve the issues raised in daily life automation. Modern framework algorithms like Swarm Intelligence are making their mark in the real-world applications. Utilization of Machine learning will not only reduce the effort of creating thousands of rules but also will prevent from time lag and packet dumps. The challenge of this research work is to develop a Machine learning based security architecture to prevent security threat in N2N communication.

## 4.1 Objectives

M-WSN has advantage of both WSN and adhoc network as it has both mobile and static nodes. The mobile nodes are there to support static nodes in order to prevent static nodes from any overload. At the same time the mobility brings a prone behaviour of intrusion and issues regarding the trust factors in the network. Based on the identified gaps he following objectives have been identified in order to make the network more reliable and secure.

a) To study and analyse the existing intrusion detection and prevention approaches during network communication in WSN, MANET and M-WSN.
b) Propose an intrusion detection framework for enhancing the secure communication in M-WSN using Cuckoo Swarm Intelligence Technique.
c) Design a framework for secure end to end communication using machine learning approaches.
d) To evaluate and compare the proposed framework with limitations of previous prevention frameworks based on Quality of Service (QoS), (Throughput, PDR, Delay, TDR and FDR).

## 4.2 Methodology

Proposed research work aims to reduce the security threat using Swarm Intelligence which is adaptive in nature. Obviously, a new behaviour is to be developed for the Swarm mechanism, across validator is required and hence Machine learning will be applied to complete this job. The proposed algorithm architecture is presented by flow diagram (see Figure 7).

STEP 1: Initially, a network with defined N number of nodes is deployed. Then the nodes are labelled for their identification and then initialize with their node's properties such as delay, packet drop, and energy consumption. After labelling each node, the source and the - Destination node is also defined to initiate the data communication process.

STEP 2: Before the source node broadcast message, a route is created between the source node and the destination node using routing protocol. Here, we will plane to use AODV as routing protocol, which creates route using Route Request (RREQ) and Route Reply (RREP) packet. RREQ is the message broadcasted by the source node to its nearby nodes.

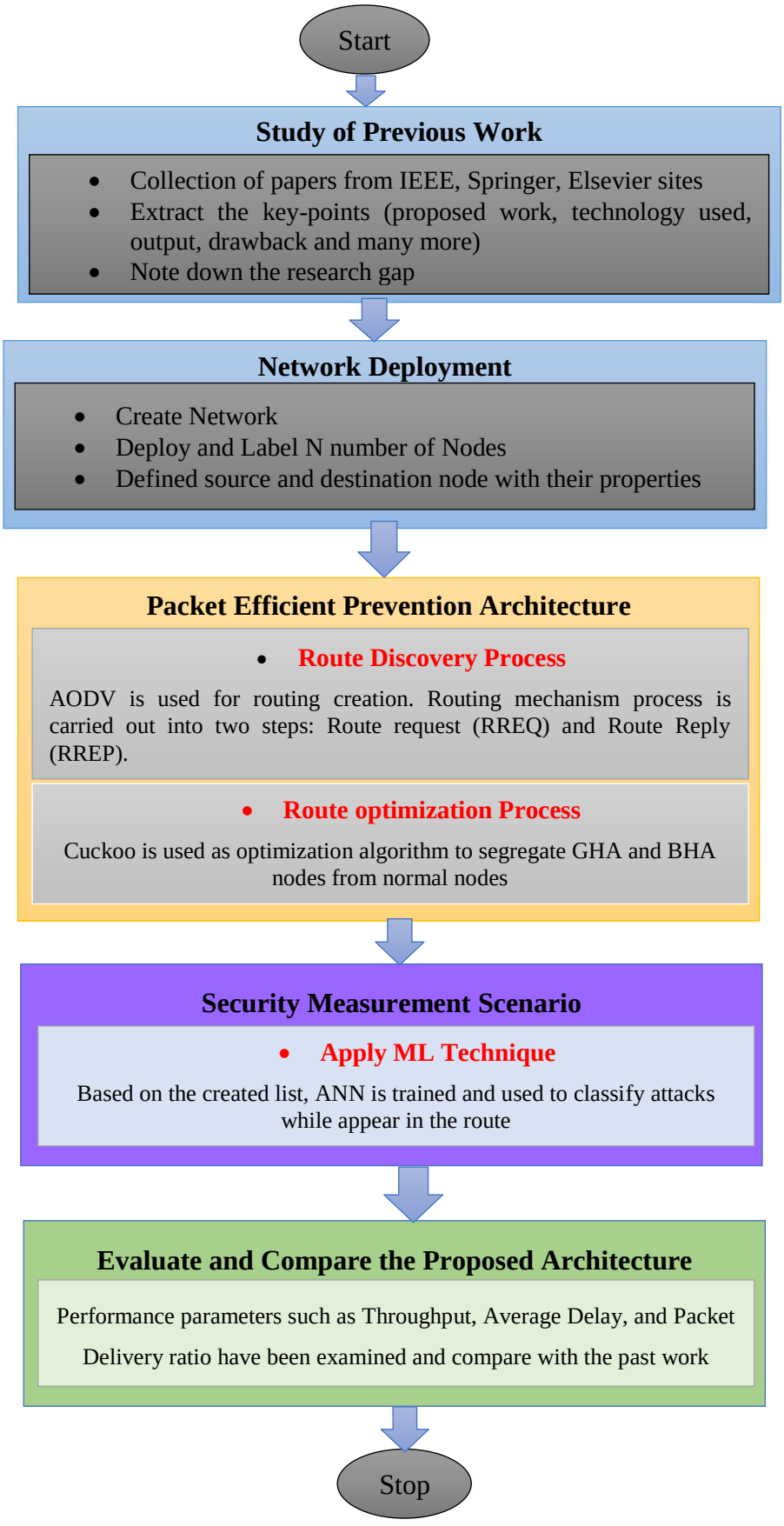


**Figure 6 Proposed Work**

STEP 3: AODV can creates a number of possible routes between the source and the destination node. CS is used as an optimization approach to select the best possible routes based on the fitness function

STEP 4: Swarm Intelligence based new behaviour will decide that whether the node is to be kept as suspect or not. Using this technique, a list of segregated nodes is created.

STEP 5: The cross validation through machine learning will identify the exact intruder out of the suspected node.

STEP 6: At last, performance analysis will be performed to determine the performance of designed IDS for N2N communication. To show the improvement of the proposed work, comparison between proposed and existing work or techniques will also be shown.

## 5. Expected Outcomes

It is hard to mention the exact parameters at this early stage of development but still some traditional parameters are discussed here that will be used for the comparative study and evaluation purpose.

**Throughput:** It is described as the ratio of the total packets delivered per time frame to the destination. Mathematically, can be given by equation (2)

$$\text{Throughput} = \frac{Total_{Receieved}\ Packets}{Unit\ Time} \quad (...2)$$

**Packet Delivery Ratio (PDR):** It is defined as the ratio of total packets received at the destination end to the total number of packets transmitted from the source end.

$$\text{PDR} = \frac{Total_{Receieved}\ Packets}{Total_{Sent}\ Packets} \quad (...3)$$

**True Detection Rate (TDR):** This parameter is used to measure the accuracy of the designed secure network that how accurately the network distinguished among normal and malicious node. Mathematically,

$$\text{TDR} = \frac{Total\ True\ Threat\ Detection}{Total\ Number\ of\ Detections} \quad (...4)$$

**False Detection Rate (FDR):** This parameter is used to represents the rate of falsely detected nodes (normal or malicious). Mathematically,

$$FDR = \frac{Total\ False\ Threat\ Detection}{Total\ Number\ of\ Detections} \quad (...5)$$

## 6. Work Plan

| | (August 2018-September 2019) | | | | (October 2019-December 2020) | | | | (January 2020-July 2020) | | | | (July 2020- June 2021) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Q1 | Q 2 | Q3 | Q4 | Q1 | Q 2 | Q3 | Q4 | Q1 | Q 2 | Q3 | Q4 | Q1 | Q 2 | Q3 | Q4 |
| Course Work | | | | | | | | | | | | | | | | |
| DCS | | | | | | | | | | | | | | | | |
| Submission of Synopsis | | | | | | | | | | | | | | | | |
| Objective 1 | | | | | | | | | | | | | | | | |
| Objective 2 | | | | | | | | | | | | | | | | |
| Objective 3 | | | | | | | | | | | | | | | | |
| Objective 4 | | | | | | | | | | | | | | | | |
| Thesis Preparation and Manuscript Writing | | | | | | | | | | | | | | | | |

→ **Work Completed**

→ **Present Status of Work**

→ **Future Work**

**REFERENCES**


1. Mohamed, S.M., Hamza, H.S. and Saroit, I.A., 2017. Coverage in mobile wireless sensor networks (M-WSN): A survey. *Computer Communications*, *110*, pp.133-150.
2. Khan, A.W., Abdullah, A.H., Anisi, M.H. and Bangash, J.I., 2014. A comprehensive study of data collection schemes using mobile sinks in wireless sensor networks. *Sensors*, *14*(2), pp.2510-2548.
3. Zhao, Z., Huangfu, W., Liu, Y. and Sun, L., 2011, December. Design and Implementation of Network Management System for Large-Scale Wireless Sensor Networks. In *2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks* (pp. 130-137). IEEE.
4. Yick, J., Mukherjee, B. and Ghosal, D., 2008. Wireless sensor network survey. *Computer networks*, *52*(12), pp.2292-2330.
5. Sabor, N., Sasaki, S., Abo-Zahhad, M. and Ahmed, S.M., 2017. A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: Review, taxonomy, and future directions. *Wireless Communications and Mobile Computing*, *2017*.
6. Hinds, A., Ngulube, M., Zhu, S. and Al-Aqrabi, H., 2013. 'A review of routing protocols for mobile ad-hoc networks (manet)'. *International journal of information and education technology*, *3*(1), p.1.
7. Ahmad, M., Aydın, N., Boeloeni, L., Boukerche, A., Turgut, D. and Turgut, B., 2011. 'Routing protocols in ad hoc networks: A survey'.
8. Cheng, B.N. and Moore, S., 2012, October. 'A comparison of MANET routing protocols on airborne tactical networks'. In *MILCOM 2012-2012 IEEE Military Communications Conference* (pp. 1-6). IEEE.
9. Nadeem, A. and Howarth, M.P., 2013. 'A survey of MANET intrusion detection & prevention approaches for network layer attacks'. *IEEE communications surveys & tutorials*, *15*(4), pp.2027-2045.
10. Ozcelik, M.M., Irmak, E. and Ozdemir, S., 2017, May. 'A hybrid trust based intrusion detection system for wireless sensor networks'. In *2017 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.
11. Zhang, Z., Zhu, H., Luo, S., Xin, Y. and Liu, X., 2017. 'Intrusion detection based on state context and hierarchical trust in wireless sensor networks'. *IEEE Access*, *5*, pp.12088-12102.

12. Singh, R., Singh, J. and Singh, R., 2017. 'Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks'. *Wireless Communications and Mobile Computing*, *2017*.
13. Boddu, N., Vatambeti, R. and Bobba, V., 2017. 'Achieving Energy Efficiency and Increasing the Network Life Time in MANET through Fault Tolerant Multi-Path Routing'. *International Journal of Intelligent Engineering and Systems*, *10*(3), pp.166-172.
14. Prabha, V.R. and Latha, P., 2017. 'Enhanced multi-attribute trust protocol for malicious node detection in wireless sensor networks'. *Sādhanā*, *42*(2), pp.143-151.
15. Zamani, A.T. and Zubair, S., 2014. 'Key management scheme in mobile Ad Hoc networks'. *International Journal of Emerging Research in Management & Technology*, *3*(4), pp.157-165.
16. Abdel-Azim, M., Salah, H.E.D. and Eissa, M.E., 2018. 'IDS Against Black-Hole Attack for MANET'. *IJ Network Security*, *20*(3), pp.585-592.
17. Wazid, M. and Das, A.K., 2017. 'A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks'. *Wireless Personal Communications*, *94*(3), pp.1165-1191.
18. Schweitzer, N., Stulman, A., Shabtai, A. and Margalit, R.D., 2015. 'Mitigating denial of service attacks in OLSR protocol using fictitious nodes'. *IEEE Transactions on Mobile Computing*, *15*(1), pp.163-172.
19. Ahmed, H. and Glasgow, J., 2012. Swarm intelligence: concepts, models and applications. *School Of Computing, Queens University Technical Report*.
20. Kout, A., Labed, S. and Chikhi, S., 2018. AODVCS, a new bio-inspired routing protocol based on cuckoo search algorithm for mobile ad hoc networks. *Wireless Networks*, *24*(7), pp.2509-2519.
21. Stephen, K.V.K., Mathivanan, V. and Kumar, K., 2020, May. A Novel Cuckoo Search Structure Optimized Neural Network for Efficient Data Aggregation in Wireless Sensor Network. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 941-947). IEEE.
22. Akbas, A., Yildiz, H.U., Ozbayoglu, A.M. and Tavli, B., 2019. Neural network based instant parameter prediction for wireless sensor network optimization models. *Wireless Networks*, *25*(6), pp.3405-3418.

23. Olakanmi, O.O., Odeyemi, K.O. and Abbas, A., 2020. Mobility and energy prediction models: Approach toward effective route management in mobile wireless sensor networks. *Engineering Reports*, *2*(3), p.e12095.
24. Kousar, A., Mittal, N. and Singh, P., 2020. An improved hierarchical clustering method for mobile wireless sensor network using type-2 fuzzy logic. In *Proceedings of ICETIT 2019* (pp. 128-140). Springer, Cham.
25. Rady, A.A., Sabor, N., Shokair, M. and El-Rabaie, E.S.M., 2020. Efficient Clustering based Genetic Algorithm in Mobile Wireless Sensor Networks. *Menoufia Journal of Electronic Engineering Research*.
26. Thandapani, P., Arunachalam, M. and Sundarraj, D., 2020. An energy- efficient clustering and multipath routing for mobile wireless sensor network using game theory. *International Journal of Communication Systems*, *33*(7), p.e4336.
27. Elsaid, S.A. and Albatati, N.S., 2020. An optimized collaborative intrusion detection system for wireless sensor networks. Soft Computing, pp.1-15.
28. Umarani, C. and Kannan, S., 2020. Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network. Peer-to-Peer Networking and Applications, 13(3), pp.752-761.
29. Zafar, S., Bashir, A. and Chaudhry, S.A., 2019. Mobility-aware hierarchical clustering in mobile wireless sensor networks. *IEEE Access*, *7*, pp.20394-20403.
30. Otoum, S., Kantarci, B. and Mouftah, H.T., 2019. 'On the feasibility of deep learning in sensor network intrusion detection'. *IEEE Networking Letters*, *1*(2), pp.68-71.
31. Fang, W., Song, X., Wu, X., Sun, J. and Hu, M., 2018. Novel efficient deployment schemes for sensor coverage in mobile wireless sensor networks. *Information Fusion*, *41*, pp.25-36.
32. Jamshidi, M., Ranjbari, M., Esnaashari, M., Qader, N.N. and Meybodi, M.R., 2018. Sybil node detection in mobile wireless sensor networks using observer nodes. *JOIV: International Journal on Informatics Visualization*, *2*(3), pp.159-165.
33. Shone, N., Ngoc, T.N., Phai, V.D. and Shi, Q., 2018. 'A deep learning approach to network intrusion detection'. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), pp.41-50.
34. Yang, X., Wang, L. and Xie, J., 2017. Energy efficient cross-layer transmission model for mobile wireless sensor networks. *Mobile Information Systems*, *2017*.

35. Abuarqoub, A., Hammoudeh, M., Adebisi, B., Jabbar, S., Bounceur, A. and Al-Bashar, H., 2017. Dynamic clustering and management of mobile wireless sensor networks. *Computer Networks*, *117*, pp.62-75.
36. Jamshidi, M., Zangeneh, E., Esnaashari, M. and Meybodi, M.R., 2017. A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks. *Computers & Electrical Engineering*, *64*, pp.220-232.
37. Idris, M.Y.I., Wahab, A.W.A., Qabajeh, L.K. and Mahdi, O.A., 2017. Low communication cost (LCC) scheme for localizing mobile wireless sensor networks. *Wireless Networks*, *23*(3), pp.737-747.
38. To, M.A., 2016. 'A proactive approach for strip interoperability in wireless ad hoc routing protocols'. *IEEE Latin America Transactions*, *14*(6), pp.2543-2549.
39. Mohanapriya, M. and Krishnamurthi, I., 2014. Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers & Electrical Engineering, 40(2), pp.530-538.
40. Shah, S.K. and Vishwakarma, D.D., 2012, July. 'FPGA implementation of ANN for reactive routing protocols in MANET'. In *2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat)* (pp. 11-14). IEEE.
41. Le Fessant, F., Papadimitriou, A., Viana, A.C., Sengul, C. and Palomar, E., 2012. A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis. Computer communications, 35(2), pp.234-248.
42. Ali Zardari, Z., He, J., Zhu, N., Mohammadani, K.H., Pathan, M.S., Hussain, M.I. and Memon, M.Q., 2019. A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs. *Future Internet*, *11*(3), p.61.
43. Muhammad, H.A., Yahiya, T.A. and Al-Salihi, N., 2019, June. Comparative Study Between Reactive and Proactive Protocols of (MANET) in Terms of Power Consumption and Quality of Service. In *International Conference on Computer Networks* (pp. 99-111). Springer, Cham.
44. Gorine, D. and Saleh, R., 2019. Performance Analysis of Routing Protocols in MANET under Malicious Attacks. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *11*.
45. Gurung, S. and Chauhan, S., 2019. A novel approach for mitigating gray hole attack in MANET. *Wireless Networks*, *24*(2), pp.565-579.

46. Singh, V., Singh, D. and Hassan, M.M., 2019, March. Survey: Black Hole Attack Detection in MANET. In *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*.
47. Saudi, N.A.M., Arshad, M.A., Buja, A.G., Fadzil, A.F.A. and Saidi, R.M., 2019. Mobile ad-hoc network (MANET) routing protocols: A performance assessment. In *Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017)* (pp. 53-59). Springer, Singapore.
48. Ghugar, U., Pradhan, J., Bhoi, S.K., Sahoo, R.R. and Panda, S.K., 2018. 'PL-IDS: physical layer trust based intrusion detection system for wireless sensor networks'. *International Journal of Information Technology*, *10*(4), pp.489-494.
49. Otoum, S., Kantarci, B. and Mouftah, H.T., 2017. 'Detection of known and unknown intrusive sensor behavior in critical applications'. *IEEE Sensors Letters*, *1*(5), pp.1-4.
50. Jin, X., Liang, J., Tong, W., Lu, L. and Li, Z., 2017. 'Multi-agent trust-based intrusion detection scheme for wireless sensor networks'. *Computers & Electrical Engineering*, *59*, pp.262-273.
51. Basan, A., Basan, E. and Makarevich, O., 2017, October. 'A trust evaluation method for active attack counteraction in wireless sensor networks'. In *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (pp. 369-372). IEEE.
52. Sarkar, S. and Datta, R., 2017. An adaptive protocol for stable and energy-aware routing in MANETs. IETE Technical Review, 34(4), pp.353-365.
53. Keerthana, G. and Padmavathi, G., 2016. Detecting sinkhole attack in wireless sensor network using enhanced particle swarm optimization technique. *International Journal of Security and Its Applications*, *10*(3), pp.41-54.
54. Razaque, A., Abdulgader, M., Joshi, C., Amsaad, F. and Chauhan, M., 2016, April. 'P-LEACH: Energy efficient routing protocol for Wireless Sensor Networks'. In *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-5). IEEE.
55. Aldaej, A. and Ahamad, T., 2016. AAODV (aggrandized ad hoc on demand vector): a detection and prevention technique for manets. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *7*(10), p.2016.
56. Brar, S. and Angurala, M., 2016. Review on grey-hole attack detection and prevention. International Journal of Advance research, Ideas and Innovations in Technology, 2(5), pp.1-4.

57. Dhama, S., Sharma, S. and Saini, M., 2016, March. Black hole attack detection and prevention mechanism for mobile ad-hoc networks. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 2993-2996). IEEE.
58. Malik, K. I., & Yaqoob, M. M. An Analytical Survey on Routing Protocols for Wireless Sensor Network (WSN). *International Journal of Computer Applications*, *975*, 8887.
59. Subramaniyan, S., Johnson, W., & Subramaniyan, K. (2014). A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique. *EURASIP Journal on Wireless Communications and Networking*, *2014*(1), 205.