Abstract

Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Sequence Number and received count

A Wireless Sensor Network (WSN) contains a huge number of nodes. These nodes are often deployed in adverse environments and have limited resources in terms of power, capacity, processing, memory, and security. This makes the network susceptible to security attacks, such as Sybil, black hole, selective forwarding, etc. Hence, security plays an important role in WSNs. This thesis focuses on one of these attacks specifically; that is the selective forwarding attack, which involves dropped or forwarding a packet in the node to reduce its efficiency. Our technique is propose for detection of malicious nodes. It is assume that all nodes contribute to this process through the gathering of some statistical data related to their transmission. This data is periodically sent to a Base Station, where all functions are executed. We propose a model that effectively detects one type of malicious behavior: Selective forwarding attack. The model is based on the transmissions data of all nodes in the network that the node should monitor sender behavior and gather some pertinent information then if this information doesn't correct it will pass it to the base station and evaluated using some trust measures. [1]

KEYWORDS

Wireless Sensor Network (WSN), Selective Forwarding Attack (SFA), Denial of Service (DoS), attacks in WSN, malicious nodes, false alarm, detection rate, secure routing, ad hoc network, security information and event management, sequence Number

الكشف عن هجمات إعادة توجيه انتقائية في شبكات الاستشعار اللاسلكية باستخدام تقنية العدّاد

تحتوي شبكة الاستشعار اللاسلكية) WSN(على عدد كبير من العقد. غالبًا ما يتم نشر هذه العقد في بيئات غير محمية، ولديها موارد محدودة من حيث القوة والسعة والمعالجة والذاكرة والأمان. هذا يجعل الشبكة عرضة للهجمات الأمنية، مثل السيبل والثقب الأسود وإعادة التوجيه الانتقائي وما إلى ذلك، وبالتالي، يلعب الأمان دورًا مهمًا في شبكات WSN. تركز هذه الرسالة على إحدى هذه الهجمات على وجه التحديد؛ وهي هجوم إعادة التوجيه الانتقائي، والذي يتضمن إسقاط أو إعادة توجيه حزمة في العقدة لتقليل كفاءتها. في التقنية المقترحة، سيتم الكشف عن العقد الخبيثة. ومن المفترض أن جميع العقد تساهم في هذه العملية من خلال جمع بعض البيانات الإحصائية المتعلقة بنقلها. و يتم إرسال هذه البيانات إذا احتوت على أيّ ة خطأ او شكوك اثناء استلام البيانات الى المحطة الرئيسية والتي بدورها تقرر إذ ا حدث اي هجوم او لا.

Acknowledgements

In the name of Allah, Most Gracious, Most Merciful

This page is used to thank individuals, groups, or organizations for their support. If you are required to acknowledge the support of a sponsor, this is generally an appropriate place to do so.

An acknowledgments page must be included in your final dissertation or thesis. The acknowledgments page should be listed in the table of contents. Place it after the final list used in the document, and before any dedication, abstract, or epigraph that is included.

It is appropriate to acknowledge sources of academic and financial support; some fellowships and grants require acknowledgment.

We offer special thanks to the CCIS at KSU for allowing us to use their dissertation and thesis template as a starting point for the development of this document.

First name, Last name
June 2020

Dedicated to my parents.

Note: If you include a special dedication as shown here be sure to keep it brief and center it on the page both horizontally and vertically. Alternatively, you may remove this page altogether, and a special dedication can be placed as the final paragraph of your acknowledgments page. **Do not include the dedication page in your table of contents.**

Table of Contents

Examination Committee Page ii

Declaration iii

Abstract iv

الخلاص ة v

Acknowledgements vii

Table of Contents ix

List of Figures xii

List of Tables xiii

List of Abbreviations xiv

Chapter 1: Introduction 1

1.1 Overview and Background 1

1.2 Elements of WSN 2

1.2.1 Sensor Node 2

1.2.2 Network Architecture 3

1.3 Transmission Data 4

1.4 The routing protocol 4

1.5 Types of Routing Protocol 5

1.5.1 Low energy adaptive clustering hierarchy (LEACH): 5

1.5.2 Sensor protocols for information via negotiation (SPIN): 6

1.5.3 Ad-hoc on-demand distance vector routing system (AODV): 7

1.5.4 Dynamic source routing (DSR): 8

1.5.5 The Real-time Transport Protocol (RTP): 12

1.6 Attacks on WSN 12

1.7 Selective Forward Attack in WSN 13

1.8 Detection techniques of Selective Forwarding Attack 13

1.9 Motivation 15

1.9.1 Primary security goals: 15

- Confidentiality: 15
- Data Integrity: 16
- Availability: 16

1.9.2 Secondary Security Goals: 16

1.10 Problem Statement 17

1.11 Research Objectives 18

1.12 Thesis Contribution to the Field/ Significance and /or Impact of the Research 18

1.13 Thesis Outline 18

Chapter 2: Literature Review 19

2.1 Introduction 19

2.2 Conclusion to This Chapter 21

Chapter 3: Methodology 1 22

3.1 Introduction 22

3.2 Methodology and the Proposed Work 22

3.2.1 Transmission between Nodes 23

3.2.2 Transmission between Nodes 29

3.2.3 Send Alarm Packet to the Base station: 33

3.2.4 Base station Make Decision: 34

3.3 Conclusion to This Chapter 36

Chapter 4: Simulation and Result 37

4.1 Introduction 37

4.2 Result 42

4.2.1 Test One (50 Nodes) 42

4.2.2 Test Two (100 Nodes) 43

4.2.3 Test Three (150 Nodes) 44

4.2.4 Test Four (400 Nodes) 45

4.3 Conclusion to This Chapter 46

Chapter 5: Another Chapter (Discussion?) 47

5.1 Introduction 47

5.2 Section 47

5.2.1 Sub-section 47

5.3 Conclusion to This Chapter 47

Chapter 6: Conclusion and Future Work 48

6.1 Introduction 48

6.2 Section 48

6.2.1 Sub-section 48

References 49

Appendix A: Our Scenario in Different Cases 53

Appendix B: Screen shots from Our Simulation 61

Appendix C: Title here.. 62

Author's Biographical Sketch 63

List of Figures

Figure 1-1 WSN network architecture 1
Figure 0-2 Sensor Node in a WSN……………………………………………………………………………3
Figure 1-3 Base Station (BS) using wireless…………………………………………………………………3
Figure 1-2 LEACH 6
Figure 1-3 SPIN Protocol 7
Figure 1-4 AODV 8
Figure 1-5 Dynamic source routing 9
Figure 1-6 Dynamic source routing (route discovery stage) 10
Figure 1-7 Dynamic source routing (route maintenance stage) 12

Figure 1-8 Major Security goal 15
Figure 3-1 Methodology Flowchart 23
Figure 3-2 Sender Side .... 30 Figure 3-3 Transmission Nodes .... 30 Figure 3-4 Receiver side flowchart .... **Error! Bookmark not defined.** Figure 3-5 Alarm Packet .... 33 Figure 3-6 Base Station flowchart .... **Error! Bookmark not defined.**
Figure 4-1 50 Node Chart 43

List of Tables

Table 1-1 Attack’s in WSN 13
Table 1-2 Advantages and Disadvantages of techniques 14
Table 3-1 Header flag 31
Table 3-2 node 3D array 32
Table 3-3 Node 2 Header Packet.. 32
Table 3-4 Alarm Packet Flags 33
Table 3-5 Nodes energy 34
Table 3-6 steps of transmission data 35
Table 4-1 Simulation Parameters 42
Table 4-2 Test 50 node 42
Table 4-3 test 100 Node 43

List of Abbreviations

WSN	Wireless Sensor Network
SFA	Selective forwarding attack
DoS	Denial of Service
ACK	Acknowledgment
DSR	Dynamic source routing

Chapter 1: Introduction

1.1 Overview and Background

Wireless Sensor Networks (WSN) [2] is a set of sensors that are used to monitor a specific phenomenon (such as heat, humidity, vibration, light, etc.), then send these data to base station. Many researchers work to develop the security of WSN such as construction, contract operating systems, data collection and integration, etc. [3] . There are many issues to be resolved for WSN include security, power consuming, and so on.

With recent advances in internet and network technology, wireless sensors networks (WSNs) have been subject to rapid growth, and have become a primary solution for many different types of applications, including the monitoring of infrastructure [4].

WSN technology is present in all aspects of human daily activities. The sensor nodes within the network possess certain characteristics such as being small size, lightweight, low in manufacturing cost, wireless and capable of monitoring communication. In addition, WSNs contain a set of sensor nodes, routing nodes and a base station. Figure 1 illustrates the WSN network architecture.

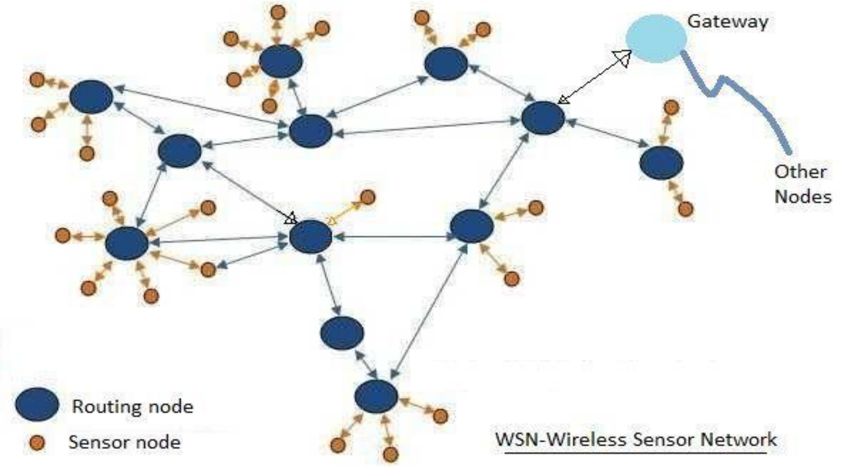


Figure 1-1 WSN network architecture

Many research efforts have aimed to address the issues of security, based on different types of attacks on WSNs. For example, in health care applications, the sensor node may be movable with the patients in order to send the patients information to the base station. In such health applications, the safety and accuracy of WSN information is very important and must be sent securely without loss or interception.

The wireless network attacks can originate from one of two forms, insider or outsider. Insider attackers damage the network when the attackers are those who have legitimate access, having all the authentication keys, e.g. encryption and decryption keys. It is not easy to detect these attacks. Inside attackers can perform modifications or drop packets. An outside attack is an attack originating externally, by an unauthorized or illegitimate user of the system. Outsider attacks can be prevented by using authentication cryptography and key management. [5]

In our thesis, we will concentrate on the selective forwarding attacks on WSNs, since this type of attack is considered as one of the most dangerous attacks [6]. Furthermore, this research will present a new novel detection technique for WSNs based on that all nodes contribute to this process through the gathering of some statistical data related to their transmission (sequence number and received count). This data is periodically checked if its matched with its saved data, if the receiver node detects any mismatch threshold it will send an alarm packet to the Base station. A novel detection technique for wireless sensor networks will be designed, implemented and evaluated.

1.2 Elements of WSN

A typical wireless sensor network can be divided into two elements:

- Sensor Node
- Network Architecture

1.2.1 Sensor Node

A Sensor Node in a WSN consists of four basic components:

- Power unit
- Sensor
- Processing Unit
- Communication System

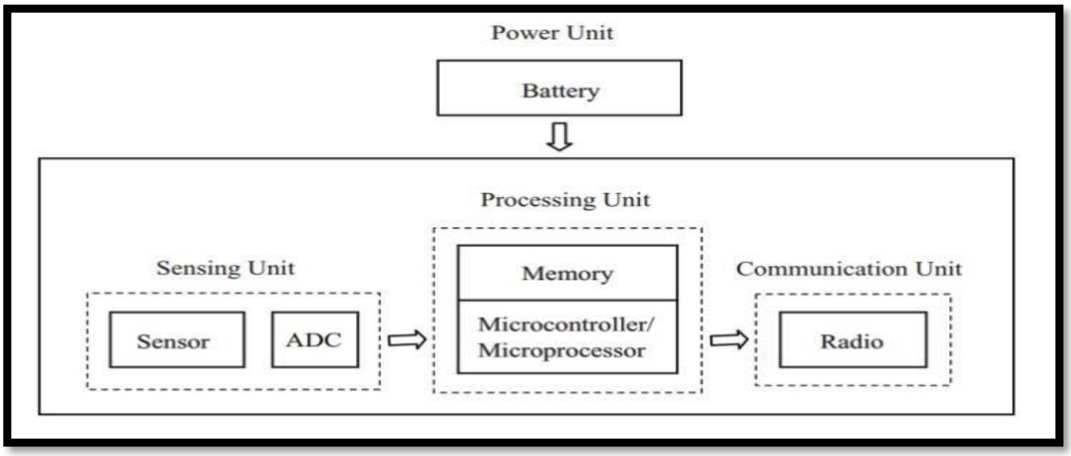


Figure 1-2 Sensor Node components in a WSN

The sensor collects the analog data from the physical world and an ADC converts this data to digital data. The main processing unit, which is usually a microprocessor or a microcontroller, performs data processing and manipulation.

Communication system consists of radio system, usually a short-range radio, for data transmission and reception. As all the components are low-power devices, a small battery, used to power the entire system.

Despite the name, a Sensor Node consists of not only the sensing component but also other important features like processing, communication and storage units.

1.2.2 Network Architecture

When a large number of sensor nodes are deploy in a large area to, cooperatively monitor a physical environment, the networking of these sensor nodes is equally important. A sensor node in a WSN not only communicates with other sensor nodes but also with a Base Station (BS) using wireless communication.

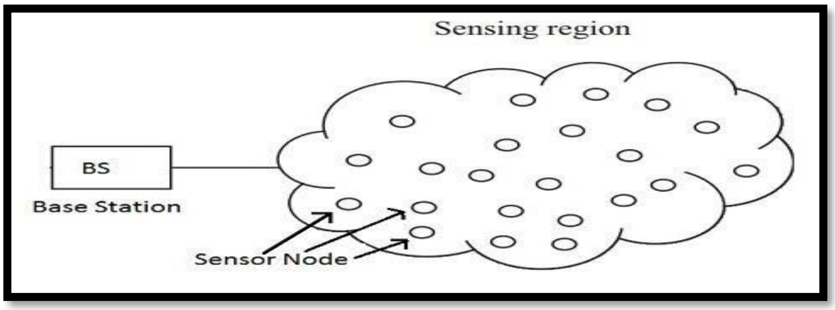


Figure 1-3 Base Station (BS) using wireless

The base station sends commands to the sensor nodes and the sensor node perform the task by collaborating with each other. After collecting the necessary data, the sensor nodes send the data back to the base station.

A base station also acts as a gateway to other networks through the internet. After receiving the data from the sensor nodes, a base station performs simple data processing.

1.3 Transmission Data

Data transmission between nodes occurs randomly in all areas of the network by using the shortest path protocol and multi-hop protocol [7]. Then the last station of the data is a base station, it collects all transmit information, then analysis this information to make decision. The shortest path can be found to connect all the nodes. A sensor network can be regarded as a weighted undirected graph, a node can be regarded as a vertex in the weighted undirected graph, and a connection between any two nodes can be regarded as an edge connecting two vertices, and its weight value is the length of the power line. [8]

1.4 The routing protocol

The routing protocol is a process to select a suitable path for the data to travel from source to destination. The process encounters several difficulties while selecting the route, which depends upon, type of network, channel characteristics, and performance metrics. [9] . The data sensed by the sensor nodes in a wireless sensor network (WSN) is typically forwarded to the base station that connects the sensor network with the other networks (may be internet) where the data is collected, analyzed and some action is taken accordingly.

In very small sensor networks, where the base station and sensor nodes so close, that they can communicate directly with each other than this is single-hop communication but, in most WSN application the coverage area is so large that requires thousands of nodes to be placed and this scenario requires multi-hop communication because most of the sensor nodes are so far from the base station so that they cannot communicate directly with the base station. The single-hop communication is also, called direct communication and multi-hop communication is called indirect communication.

In multi-hop communication, the sensor nodes not only produce and deliver their material but also serve as a path for other sensor nodes towards the base station. The process of finding suitable path from source node to destination node is called routing and this is the primary responsibility of the network layer. The routing protocols define how nodes will communicate with each other and how the information will disseminated through the network.

1.5 Types of Routing Protocol

There are many ways to classify the routing protocols of WSN:

1.5.1 Low energy adaptive clustering hierarchy (LEACH):

LEACH is a routing protocol that organizes the cluster such that the energy is equally divided in all the sensor nodes in the network. In LEACH, protocol several clusters are produced of sensor nodes and one node defined as cluster head and act as routing node for all the other nodes in the cluster.

As in routing protocols the cluster head is selected before the whole communication starts and the communication fails if there is any problem occurs in the cluster head and there is much chances that the battery dies earlier as compare to the other nodes in cluster as the fix cluster head is working his duties of routing for the whole cluster. [10]

LEACH protocol apply randomization and cluster head is selected from the group of nodes so this selection of cluster head from several nodes on temporary basis make this protocol more long lasting as battery of a single node is not burdened for long.

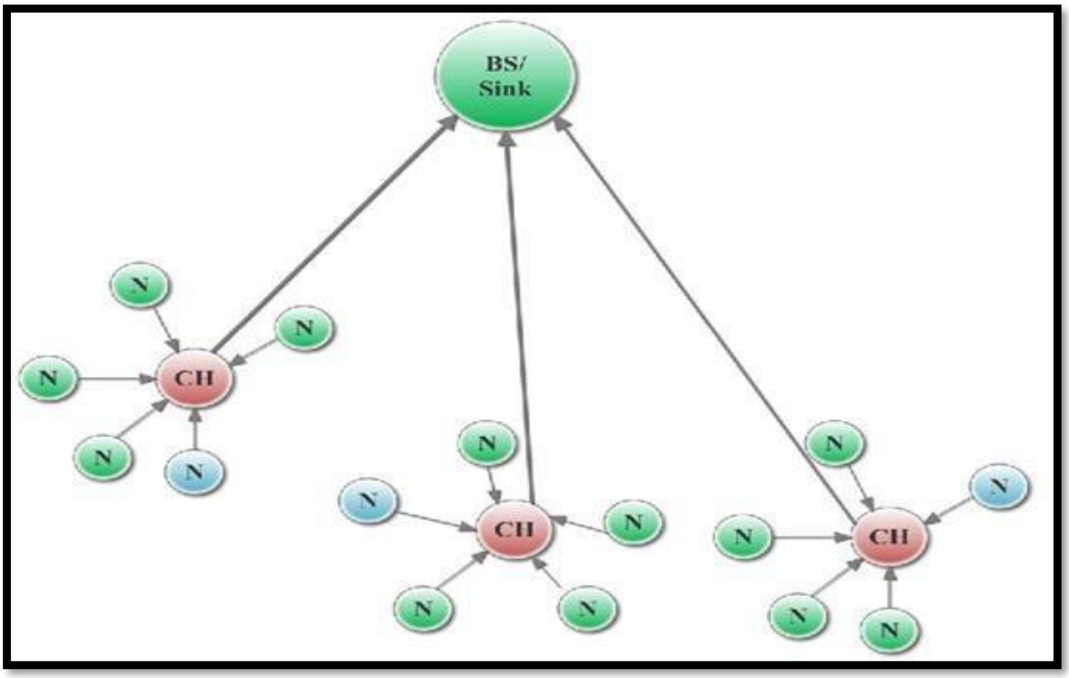


Figure 1-4 LEACH

1.5.2 Sensor protocols for information via negotiation (SPIN):

SPIN is abbreviation of sensor protocol for information via negotiation. This protocol is defined to use to remove the deficiency like flooding and gossiping that occurs in other protocols. The main idea is that the sharing of data, which is sensed by the node, might take more resources as compare to the meta-data, which is just a descriptor about the data sensed, by the node. The resource manager in each node monitors its resources and adapts their functionality accordingly. [11]

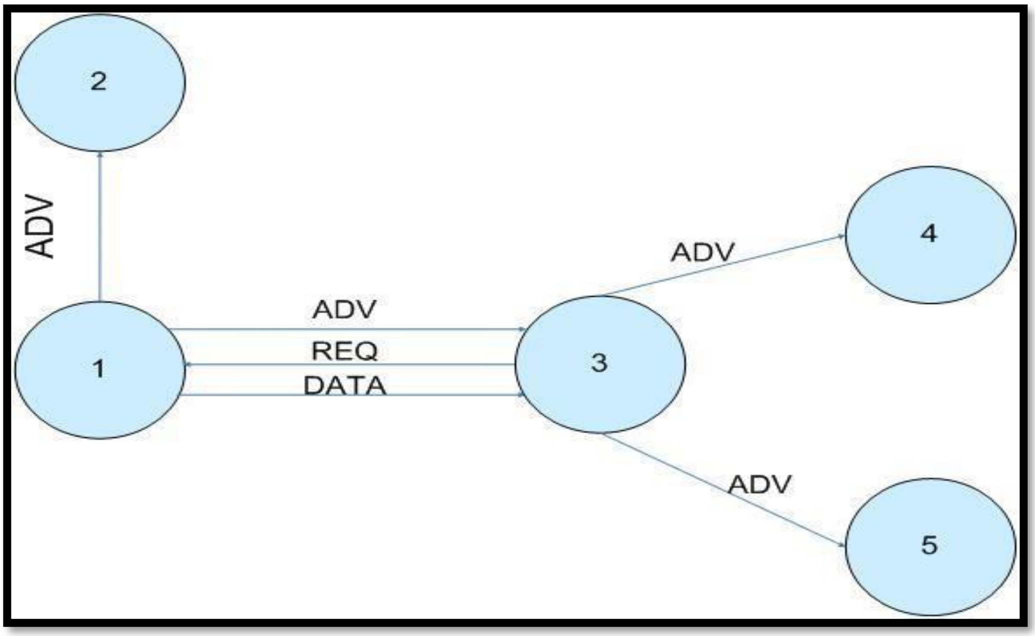


Figure 1-5 SPIN Protocol

As shown in the above figure [12].Node 1 sends broadcast packets to all its neighbors, nodes 2 and 3.Node 3 replay for the data using REQ packet , for which node 1 send data using packet DATA to node 3. After receiving the data Node 3 repeat the previous step by sending broadcast packet to its neighbors (4 and 5) to continue process.

1.5.3 Ad-hoc on-demand distance vector routing system (AODV):

Ad-hoc on-demand distance vector (AODV) is reactive on request protocol. AODV is engineered for Mobile infrastructure-less networks. It employs the on-demand routing methodology for formations of route among network nodes. Path is establish solitary when source node want to direct packs of data and pre-set route is maintained as long as the source node needs. That is why we call it as On-Demand. AODV satisfies unicast, multicast and broadcast routing. AODV routing protocol directs packets among mobile nodes of wireless ad-hoc network. AODV permits mobile nodes to pass data packets to necessary destination node via nodes of neighbor that are unable to connect link openly. The material of routing tables is switched intermittently among neighbor nodes and prepared for sudden updates [13] .

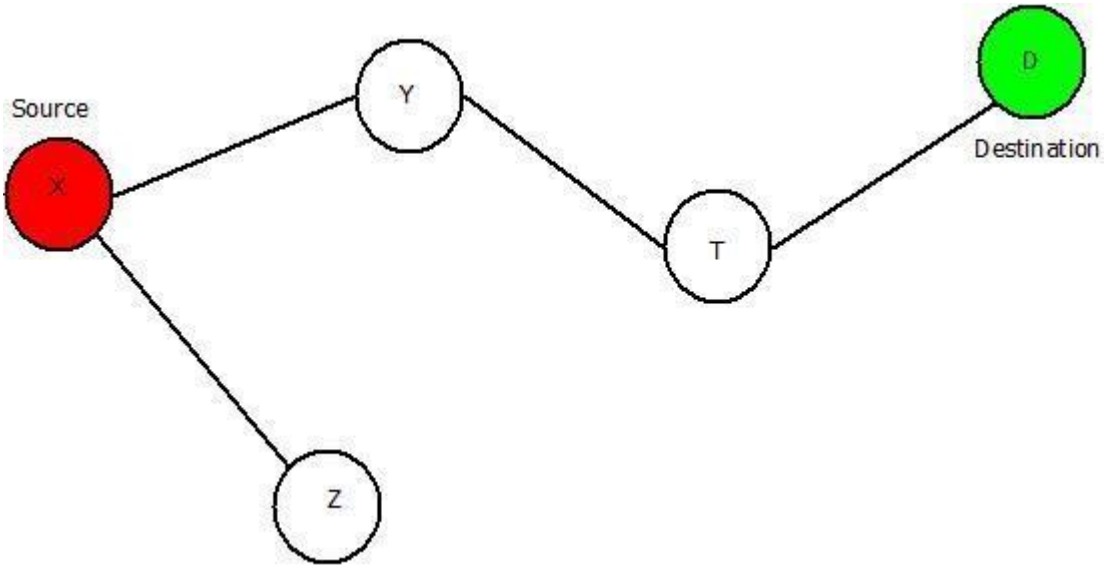


Figure 1-6 AODV

1.5.4 Dynamic source routing (DSR):

Dynamic source routing (DSR) is a routing protocol used in wireless sensor networks developed at CMU in 1996. Dynamic source routing can be reactive or on demand. As its name shows that, it uses source routing instead of routing tables. Routing in DSR is divided into two parts, route discovery and route maintenance.

This protocol routes from the source node including a header in the packets. This header indicates which nodes may need to be crossed to arrive at a destination since the originating node is responsible for calculating the complete route to the destination node. This process is called Source Routing. DSR does not require any periodic message. In this way, it reduces message overload. For this, when the origin node moves or the topology of the network changes, the algorithm perceives the modifications and adapts accordingly. In addition, DSR handles unidirectional links and asymmetric routes. Each node in the network has a cache memory that stores all the routes obtained through the discovery processes from the node itself. If there is no current route to a specific destination, the node starts a reactive route discovery just like AODV. The route table or route cache is constantly monitored to detect invalid routes and repairs them as the network topology changes. This process is called Route Maintenance. DSR features some advantages such as that nodes can obtain multiple routes to a specific destination but requesting only one route. DSR allows the network to be completely selfconfigurable, without a specific architecture or topology. In addition, it is a good choice in scenarios where the number of mobility nodes is reduced. This protocol adapts quickly to routing changes when a node is frequently moving and decreases network overload [14].

In this protocol, Source node will initiate a route discovery phase and this phase consist of route request (RREQ) and route reply (RREP) messages. In DSR, only destination node will reply with route reply RREP message to the source node unlike in AODV where every intermediate node would reply with route reply message RREP. Moreover, the purpose of next phase route maintenance is to avoid flooding of RREP messages and used for shortening of nodes between source and destination [15].

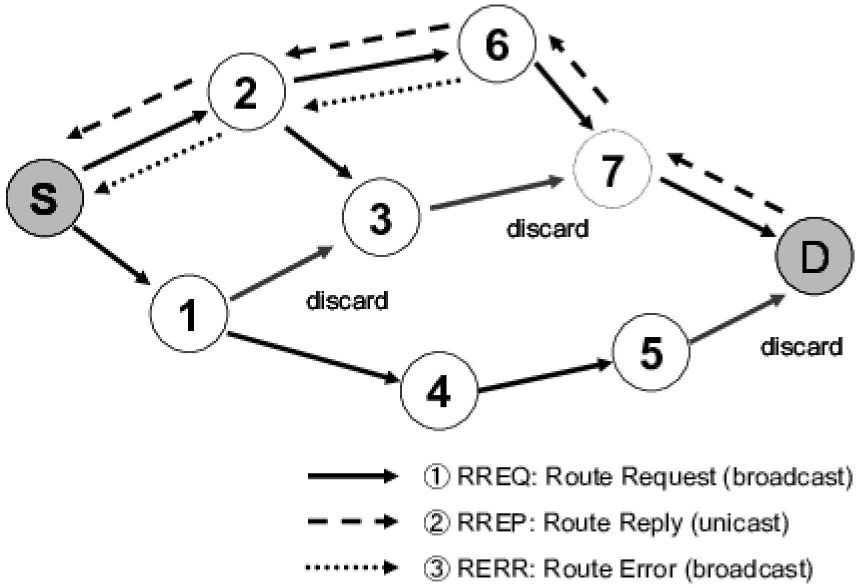

6
2
S
3
7
discard
D
1
discard
5
discard
4
① RREQ: Route Request (broadcast)
② RREP: Route Reply (unicast)
③ RERR: Route Error (broadcast)

Figure 1-7 Dynamic source routing

When the Source Node **S** wants to start the data communication with destination **D** in the network, it checks its routing cache. When around is no route obtainable to the destination in the route cache or if the way has expired, it initiates the route discovery mechanism by broadcasting the route request message RREQ to the neighbor nodes. As shown in the following figure that illustrates the path discovery mechanism of the DSR routing protocol. When the RREQ reaches the destination or any intermediate node that has a new route to the destination node then the route reply message RREP is generated. When the source node **S** receives the RREP, it updates its cache, and the data is routed through the discovered path. [16]

It differs from other protocols as DSR is based on the source routing principle, indicating that the node that owns the data to send must identify and know a multi-hop route to the receiver node. When any node has data packets to transmit, it immediately starts to search in the cache through the routing table to determine whether a route to the required destination exists or not. If the source finds multiple routes, the route with the minimum hop count will selected and added as a header of the transmitted data packet. Otherwise, two essential phases based on route discovery and maintenance will be established .

In the route discovery stage, a route request RREQ packet mainly consists of a unique ID, source address, and the destination address will be employed in this stage. The RREQ will be flooded by the source to all the nodes in the network. Each one of the intermediate participating nodes will receive the RREQ and then check to see whether it knows the destination or not. If not, the node will add its address and rebroadcast until the RREQ arrives at the target node. Then, this target node will send a route reply RREP packet back to the source. This packet carries route details obtained from the RREQ, which stored in the source's cache for the communication requirement.

The following figure describes the route discovery phase, where N1 represents the source and N7 is the destination. To identify the route, two RREQs with unique different ids (id = 3 and id = 1) will be sent, and two routes will be discovered, which are route 1 [N1, N2, N3, N7] and route 2 [N1, N4, N5, N6, N7]. In this case, route 1 will be selected as it has the minimum hop.

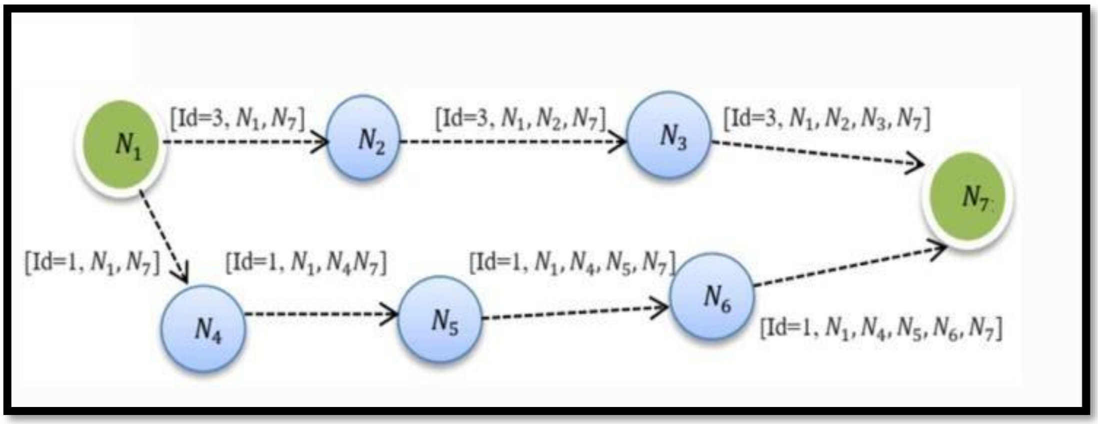


Figure 1-8 Dynamic source routing (route discovery stage)

1.5.5 The Route Discovery process briefly explained in the following steps:

Step 1: The source node S broadcast the RREQ message to its neighboring nodes.

If the node is within the transmission range, it forwards the RREQ packet to neighbors and adds ID, Previous hop node ID, pervious Node State and Node State.

Step 2: Ni upon receiving RREP updates its routing table with the information that includes source ID, destination ID, previous hop node ID and its state. It appends its state to the node state field to RREQ message and analyzes the destination ID.

```
If Ni ==! D
    Then
        Ni rebroadcasts RREQ to neighboring nodes
    Else
        Ni Sends RREP to Source Node.
End if
```

Ni IS THE CURRENT NODE, D IS THE Destination NODE.

The other mechanism used in DSR is route maintenance, which is applied to find alternative routes to continue the transmission of data packets when the current path experiences failure. In this stage, the source receives a route error (RERR) packet and then deletes the expired route from its cache to start a new search for a new route.

The following figure depicts the route maintenance mechanism. It shows that when the link between node N3 and destination node N7 is disconnected, the intermediate node N3 sends a RERR message to the source node N1.

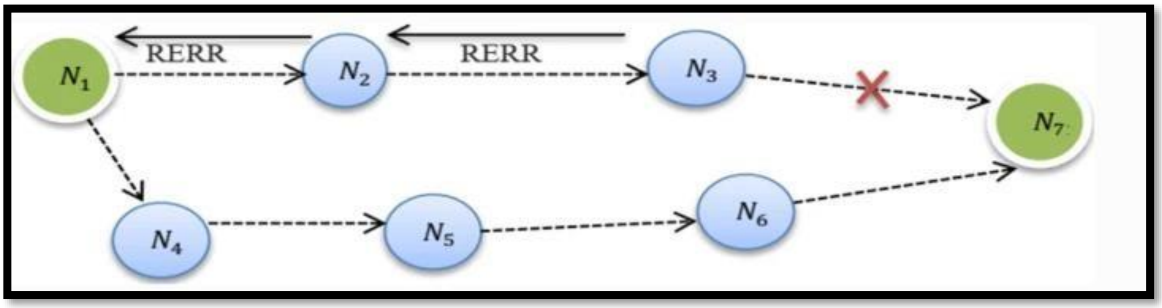


Figure 1-9 Dynamic source routing (route maintenance stage*)*

1.5.6 The Real-time Transport Protocol (RTP):

The Real-time Transport Protocol (RTP): is a network protocol for delivering audio and video over IP networks. RTP is used in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications including WebRTC,   television services and web-based push-to-talk features with no ACK.

1.6 Attacks on WSN

Some of the attacks, classified based on OSI reference model layers, are listed in table 1.1 given below with their defense strategies. [17]

Table 1-1 Attack's in WSN

Layer	Attacks	Defense strategy
Physical layer	1- Jamming 2- Tampering	1- Spread spectrum strategy 2- MAC layer admission control
Data link layer	1- Collusion 2- Jamming 3- Disruption MAC	1- Spread spectrum 2- Error correction techniques
Network layer	1- Selective forwarding 2- Hello flood 3- Black hole 4- Worm hole	1- Authentication
Transport layer	1- Adding false messages 2- Sync flood 3- De-synchronization	1- Authentication 2- Verification
Application layer	1- Attacks on reliability 2- Data aggregation distortion	1- Cryptography 2- Encoding 3- Watermarking

1.7 Selective Forward Attack in WSN

Selective forwarding attack (SFA) is an attack of network layer as shown in the above table. Usually in WSNs, sensor nodes forward data packets to neighboring sensor node keeping a trust factor that packet will reach their destinations at the end. In this attack, malicious nodes are setup by intruders, which act as sensor node of the network. These malicious nodes drop out data packets passing through them and forward only selective packets to the next sensor node. When all the packets are dropped out, in that instance, this attack can be called as black hole attack. [18]

1.8 Detection techniques of Selective Forwarding Attack

There are different techniques to detect selective forwarding attack:

1- **Detection using acknowledgement:** In this technique, if any node detects any malicious nodes, it sends the Error ACK message to the source node.

- **Detection process:** In this technique the system generates three values ACK_COUNT, ACK_SPAN, and ACK_TTL the ACK_COUNT set as ACK_SPAN, when the next node receives packet, it decreases ACK_COUNT by one and updates information then forwarding it to the next node, if ACK_COUNT value is zero then

ACK_TTL is set to ACK_SPAN and send packet to previous node and decrease ACK_SPAN by 1 until arrive to 0, in the all intermediate nodes matches their value ACK_COUNT, with ACK_TTL. If they do not match then an alarm packet is send to source node and, the selective forwarding attack can be detected. [19]

2- **Detection with the help of a neighboring nodes information**: In this technique, the neighbor's nodes detect the dropping packets and resend those packets making attack failed.

3- **Multi-path data flow scheme:** In this technique, the system generates multiple acknowledgment message for each received packet to confirm packet transmission. In a multiple ACK message, one ACK is returned to destination on the transmission path, the other ACK return on other path. At the same time the source node send multiple data, one is primary, the other is backup sent through the different path and then wait the ACK message from the destination when a primary packet delivered, if a source doesn't receive ACK, the backup packet will be send to the destination. [20]

Table 1-2 Advantages and Disadvantages of techniques

Technique	Advantages	Disadvantages
Detection using acknowledgement	1- Easy to implement 2- No hardware need	If packet lost , Packet overhead will increase
Detection with the help of neighboring node's information	Traffic overheads will be reduced	Responsibilities will increase for watch nodes in the neighbors and GPS will require to determine the location of nodes
Multi-path data flow scheme	No packet loss	Network cost will be high

1.9 Motivation

Security is typically the main issue in wireless networks, as most WSNs are composed of a large number of nodes that are distribute in an untrusted area. The majority of WSN nodes are vulnerable to both external and internal malicious attacks [21]. The security goal of WSNs is to solve network availability issues, confidentiality issues, integrity issues, node authentication issues, and freshness issues.

Due to the characteristics of the wireless sensor network, there are some requirements that must be fulfilled when sending data through the WSN, in order to protect the data from attackers. [22] Therefore, the WSN security goals are categorized as follows in the next subsection.

1.9.1 Primary security goals:

There are three types of major security goals, confidentiality, integrity, and data availability

Confidentiality
SECURITY GOALS
Integrity
Availability

Figure 1-10 Major Security goal

- **Confidentiality:**

Data confidentiality is paramount in WSN security. It increases the secrecy of the data transmission, and this data is more trusted than leaked data. Hence, it is important to establish the secure paths between nodes and hide information from unauthorized users. [23]

In sensor networks, the data confidentiality relates to the following:

1- A sensor network should not leak sensor data to its neighbors. It is critical especially in an application like a military field in which the data stored in the sensor node may be highly sensitive.

2- In many applications, since nodes communicate highly sensitive data, it is extremely important to build a secure channel in a wireless sensor network.

3- Public sensor information, such as sensor identities and public keys, should be encrypted to some degree to protect against traffic analysis attacks.

- **Data Integrity:**

While implementing confidentiality, an enemy may be unable to attack the information. However, this does not mean the data is secure. The enemy can still potentially modify the data. For example, a malicious node may add some flags within a packet. This means that a new packet is sent to the receiver. [24]

- **Availability:**

Denial of Service (DoS) is a type of attack where a node becomes unavailable in the network. Availability is a main constraint that guarantees the stability of network performance against Denial of Service attacks. [23]

1.9.2 Secondary Security Goals:

All data in the WSN should get optimum freshness, data freshness means that keeping data fresh, and no old data is duplicated. To solve this problem, the time stamp is added to the packet and once the packet is received, we can find if the data is fresh or not.

1.10 Problem Statement

A sensor node is a limited sensing device. It contains a small processing unit, limited battery and a small amount of memory for saving its operation. In addition, a wireless sensor node contains a small transceiver. These sensor nodes communicate with a huge number of small nodes through the radio waves.

The sensors collect data to include in different environments. These environments include homes, transportation systems, military installations, healthcare systems, and buildings.

The network layer is an important layer in the networks and prone many types of security attacks. The most attacks in sensor network routing are spoofing, selective forwarding, sinkhole, Sybil attack, wormhole attack, node replication attack, flooding and attack against privacy. While the communication between sensor nodes in WSNs is accomplished wirelessly by radio, adversaries can use many types of those attacks.

In a sensor network domain, data are sent to the base station through routers. An attacker agrees on the nodes by attacking the network resources.

A selective forwarding attack is one of the major attacks in WSNs. It is an attack where a node sends some of the messages to other nodes or base station whilst drop the sensitive information. The adversary installs a malicious node in the network area, which drops packets. Once the malicious node is present in the network, it organizes routing loops that attract or refuse network traffic. In addition, a malicious node can do some activities that impact to the network. These activities are such as extend or shorten source routers, generate false messages, and attempt to drop significant messages. Packets that are dropped selectively sometimes come from one node or a group of nodes. Therefore, a malicious node refuses to forward the packets. Moreover, the base station does not receive the entire message.

The problem is selective forwarding attacks in network. The constraints such as reliability, energy efficient, and scalability in WSNs are challenging factors to solve. The state-of-art research in this area focuses on selective forwarding detection, reliability, energy efficient, and scalability. We propose a novel technique to increase the accuracy. In addition, the work will be test if we achieved our target of getting a higher accuracy level to detect selective forwarding attack.

1.11 Research Objectives

The main idea of our thesis is to save energy, use little time and getting a high accuracy level to detect SFA.

The detection technique will depended on Sequence number of packet and received Counter to detect SFA .The following objectives must be met to achieve the main aim of this study [25]

- Detecting selective forwarding attack using specific flags in the packet header.
- Providing clear results while avoiding the problems of overhead that found in other methods.
- Providing clear results with clear simulation with testing code.

1.12 Thesis Contribution to the Field/ Significance and /or Impact of the Research

We proposed a new technique for detecting selective forwarding attack using sequence number and received count. We generate sequence flag in the header of packet and compare with received count in the receiver side which is increased by one after receiving a packet, if any mismatch between them, system will send alarm message to base station to make a decision if attack is detected or not. Furthermore, for achieving more accurate results and increase life time, we determined threshold to mismatch. The results of our proposal can detected the selective forwarding attack in a more accuracy rate than other techniques.

1.13 Thesis Outline

Chapter one presents the introduction of information security. Chapter two presents the literature review studies and the existing techniques related to the field of research in this thesis. Chapter three presents the methodology and the proposed work. Chapter four discusses the result and Chapter five Contribution to Science / Significance in this thesis.

Chapter 2: Literature Review

2.1 Introduction

Digital data are the most common use way to share information between nodes in WSN, in most times, contain private information. Many researchers in security field exerting much more efforts to innovate new non-traditional techniques to achieve strong protection for these Networks from any attacks. Many studies and research were presented in the field of attack detections techniques. In addition, different systems of attack detections techniques were proposed. There are various techniques, which are proposed from time to time to detect and protect WSN from selective forwarding attack for more secure.

A DoS attack is one of the security attacks that occur to WSN. It occurs in each weak layer. Different types of DoS can effect on nodes; A DoS attack includes power consumption attack in WSNs. So, its main goal is to increase network resources consumption. [26]

[27] Describe some kinds of DoS attacks, selective forwarding, the sinkhole, the wormholes attack and Sybil attack. Therefore, DoS attacks are critical effects on sensor networks layers. Because a DoS attack include a dangerous threat to a WSN, the researchers have explored different techniques to detect these attacks, the important part of a DoS attack is the identification of the nodes that are harmed by the adversary.

[28] Proposed the hybrid technique from the geographic routing and watermark-based schemes to achieve high efficiency against selective forwarding attacks in WSNs. In this technique, the geographic routing allows to choose a best secure path, while the watermark is capable of finding and discarding the malicious nodes one at a time. However, the malicious node detection techniques consumes more energy and there are delays in transport due to extracting the watermark. In addition, it may be possible that an attack done to the node after selecting a secured path. This could lead to undetected selective forwarding attacks in the later stages of the system.

[29] Proposed the security to paths of WSNs. This algorithm use MD5 encryption method for confirming identities and securing multi-path. In addition, the use of encryption methods consumes more power and overhead before data transmission.

[30] Proposed an algorithm to detect the selective forwarding attack by using two factors. Number of packets sent and delivery ratio. This algorithm based on Fuzzy Logic. Fuzzy Logic provides a specific result based on input information and the minimum critical node was chosen as the shared node. Further node that have more energy can be chose to transmit the same size of data by using less energy consuming. The performance is evaluated in terms of throughput, packet delivery ratio and average of delay. This method consumes more power to calculate complicated values and execute equations.

[31] Is proposed for each packet transmission to detect selective forwarding attacks. In this algorithm, each node along forwarding path between source and destination generates ACK message for each received packet, this ACK packet returned to the source in the different path, this technique could increase the flexibility against attacks because it denies an attacker from compromising nodes in the return path. This proposed work consumes more traffic on the network because each ACK packet will transmit to all nodes in the transmission path.

[20] Proposed an algorithm called MDMA to detect the selective forwarding attack by generating multiple acknowledgment message for each received packet to confirm packet transmission. In a multiple ACK message one ACK is returned to destination on the transmission path, the other ACK return on other path. At the same time the source node sends multiple data, one is primary, the other is backup will be send through the different path and then wait the ACK message from the destination when a primary packet delivered, if a source doesn't receive ACK, the backup packet send to the destination. The accuracy of this method may be high in sometimes but it may cause high traffic in the network, also consumes more power to send the backup packet in the far path.

[32] Contains many different components sensors, nodes, clusters of nodes, cluster head. The sensor node collects information then encrypt it and send this information to cluster head; the cluster head aggregates and sends encrypted information to the access point then forwards it to the base station. Using encryption algorithm consumes more power.

The [33] proposed technique dependent on One Way Hash Chain (OHC) by generate sequence number using public function in the network and compare this sequence with special key in the upstream or downstream nodes during the neighbor discovery phase.

2.2 Conclusion to This Chapter

In this chapter, we discussed literature review and talked about some techniques related to our method. In the next chapter we will discuss about our methodology deeply.

Chapter 3: Methodology 1

3.1 Introduction

Security in wireless sensor networks is a very important issue, to prevent a selective forwarding attack, In WSN malicious nodes may selectively drop or forward some message to the wrong path, another variance of this type of attack is to delay packets forwarding through nodes. As a result, all packets are not transferred to the base station. The selective forwarding attack is a smart attack. [26] However, it can be detecting by using our proposal.

In our proposed work, we focus on adapting sequence number and received count of packets to detect a Selective Forwarding Attack that may be launch on a WSN. we use above techniques over other methods, because this technique able to provide very good results while avoiding the problems of overheads found in other methods and less time compared to other methods. We will use Python simulations to evaluate the performance of detect selective forwarding attack in WSN.

3.2 Methodology and the Proposed Work

The idea of our technique is to detect and protect from selective forwarding attack in the WSN by using a sequence number and received count technique. The proposed technique divided into many cases.

The first step of our technique, it is building a network structure, the network structure will build using the standard of IEEE 802.11. The network includes a selection of protocols used in our technique such as transmission protocols, detection path protocols, etc. shown in the following figure. After the structure is built, the nodes are ready to add to the network with their own parameters. We used some parameters of each node as ID, Position in the network, initial energy, and others. Then all nodes are ready to transmission.

3.2.1 Transmission between Nodes

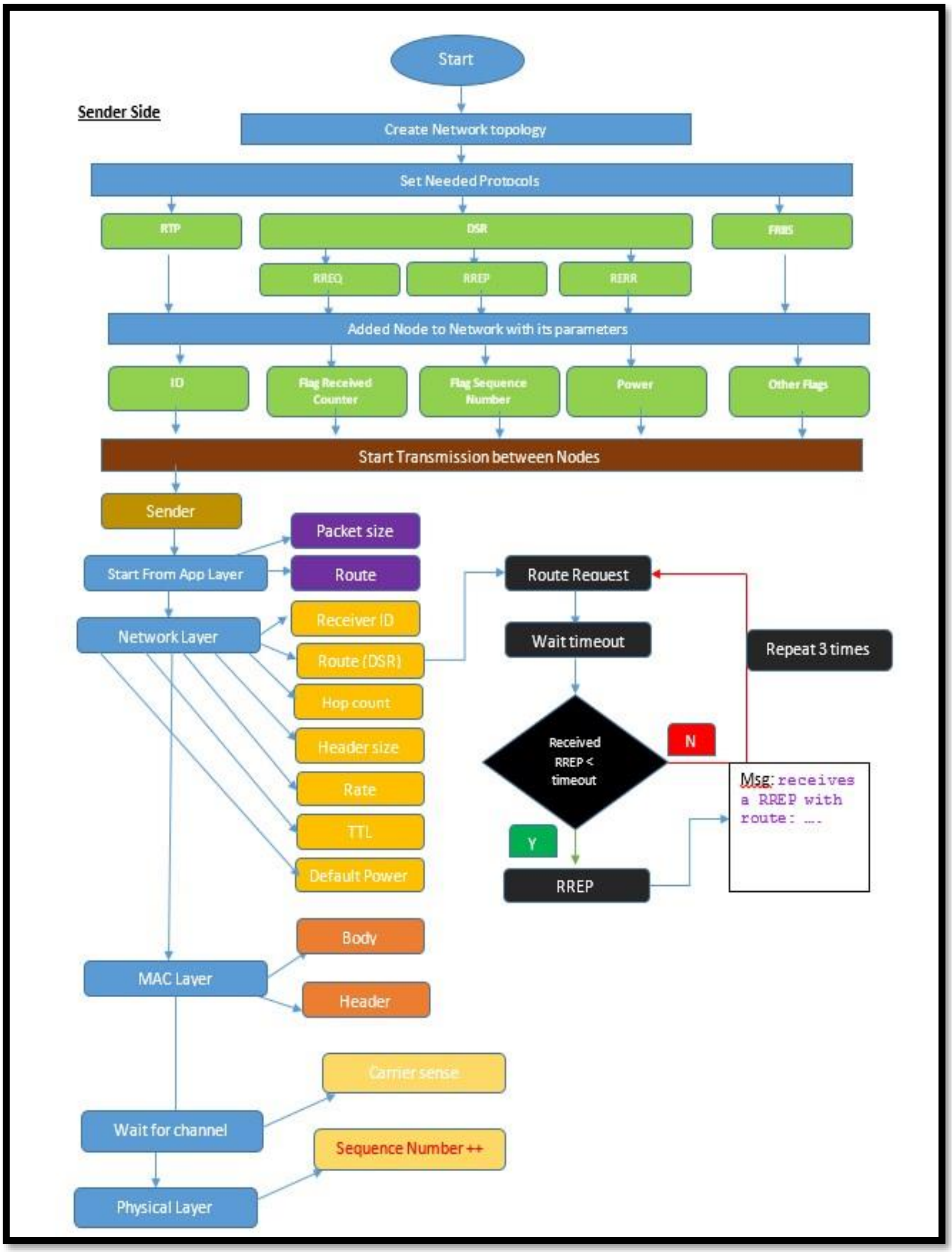
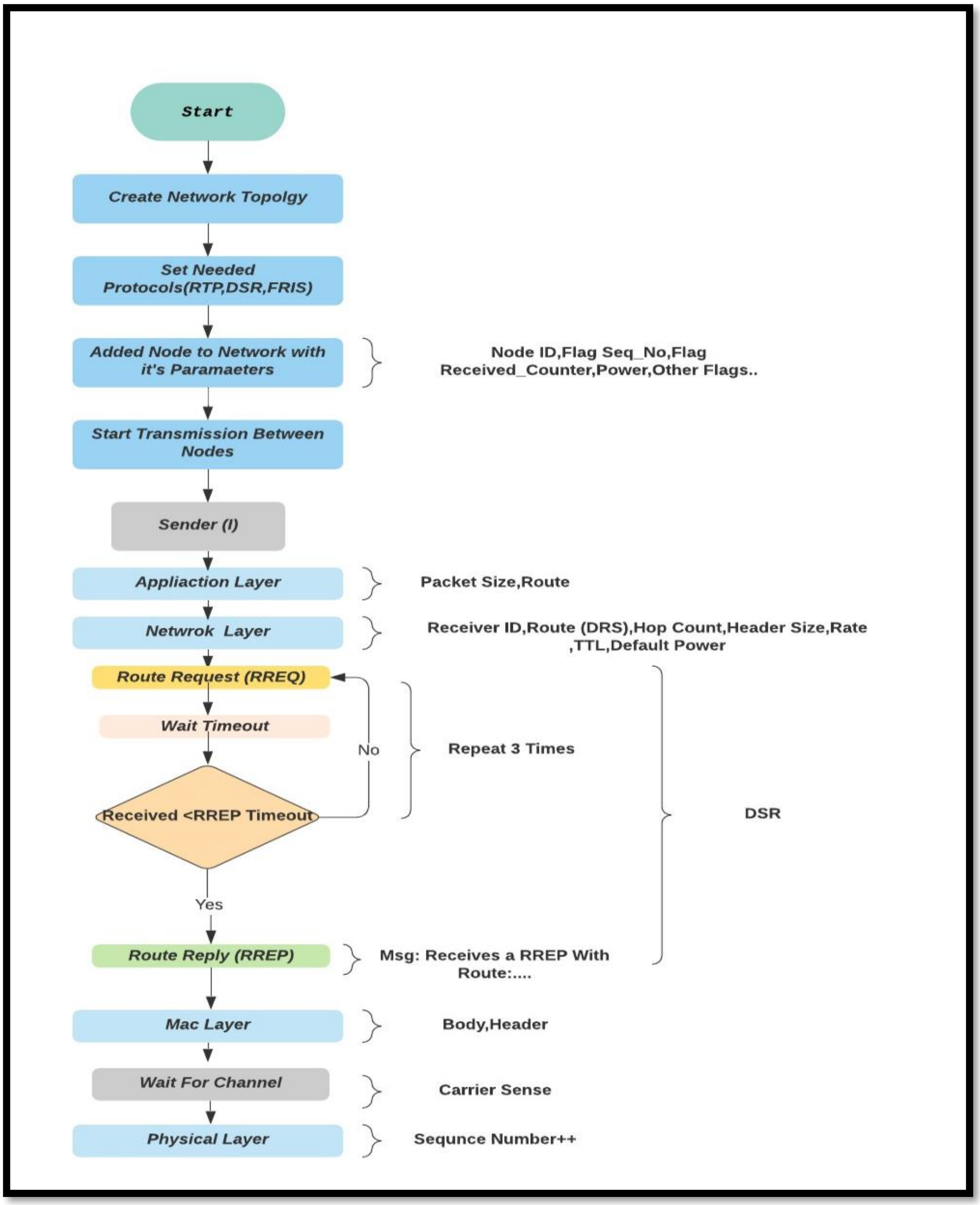
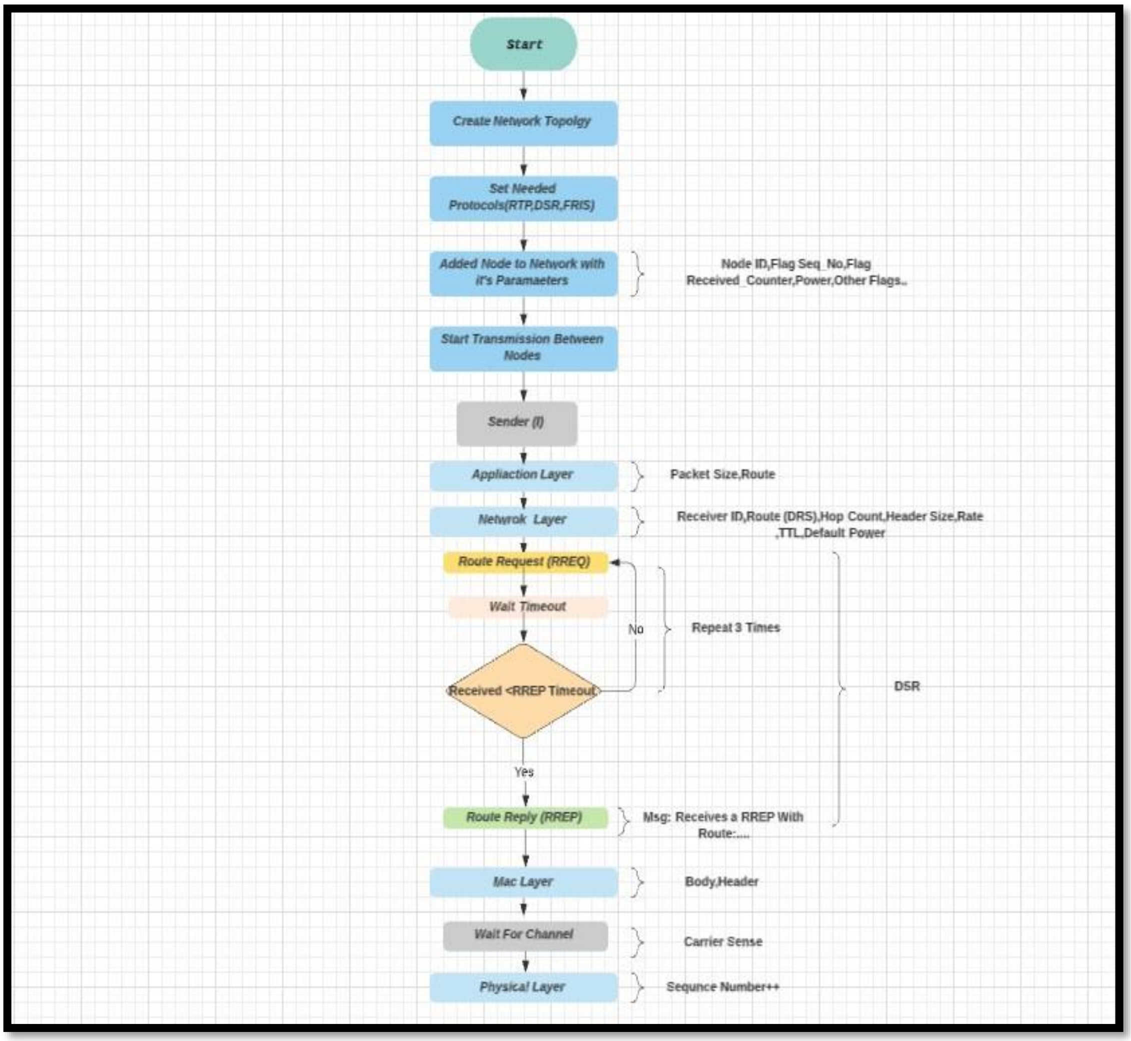
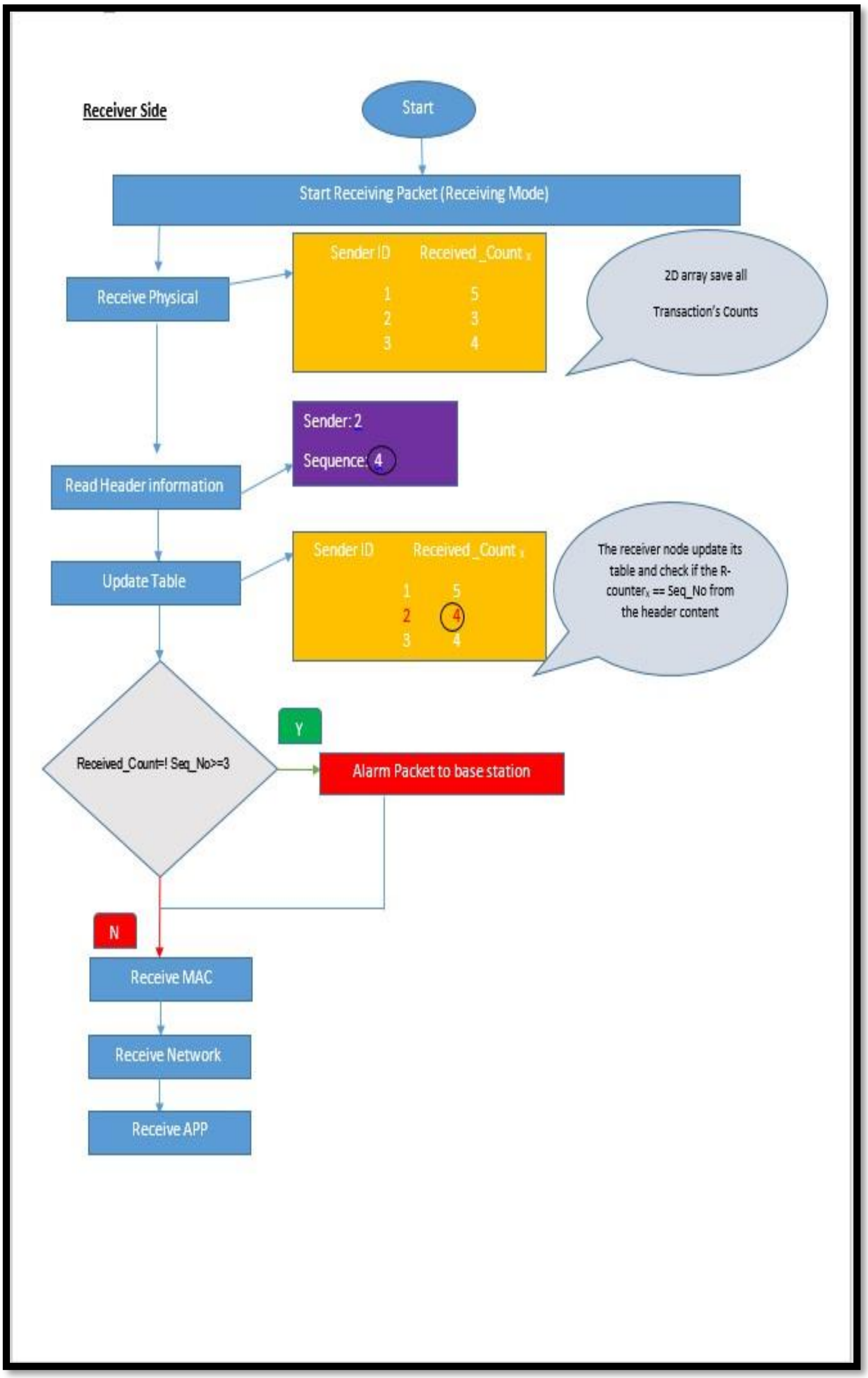


Figure 3-1 (Sender Side)


Start
Create Network Topolgy
Set Needed Protocols(RTP,DSR,FRIS)
Added Node to Network with it's Paramaeters
Node ID,Flag Seq_No,Flag Received_Counter,Power,Other Flags..
Start Transmission Between Nodes
Sender (I)
Appliaction Layer
Packet Size,Route
Netwrok Layer
Receiver ID,Route (DRS),Hop Count,Header Size,Rate ,TTL,Default Power
Route Request (RREQ)
Wait Timeout
No
Repeat 3 Times
Received <RREP Timeout
DSR
Yes
Route Reply (RREP)
Msg: Receives a RREP With Route:....
Mac Layer
Body,Header
Wait For Channel
Carrier Sense
Physical Layer
Sequnce Number++


Start
Create Network Topolgy
Set Needed Protocols(RTP,DSR,FRIS)
Added Node to Network with it's Paramaeters
Node ID,Flag Seq_No,Flag Received_Counter,Power,Other Flags..
Start Transmission Between Nodes
Sender (I)
Appliaction Layer
Packet Size,Route
Netwrok Layer
Receiver ID,Route (DRS),Hop Count,Header Size,Rate ,TTL,Default Power
Route Request (RREQ)
Wait Timeout
No
Repeat 3 Times
Received <RREP Timeout
DSR
Yes
Route Reply (RREP)
Msg: Receives a RREP With Route:....
Mac Layer
Body,Header
Wait For Channel
Carrier Sense
Physical Layer
Sequnce Number++



Sender ID	Received _Count $_x$
1	5
2	3
3	4

2D array save all

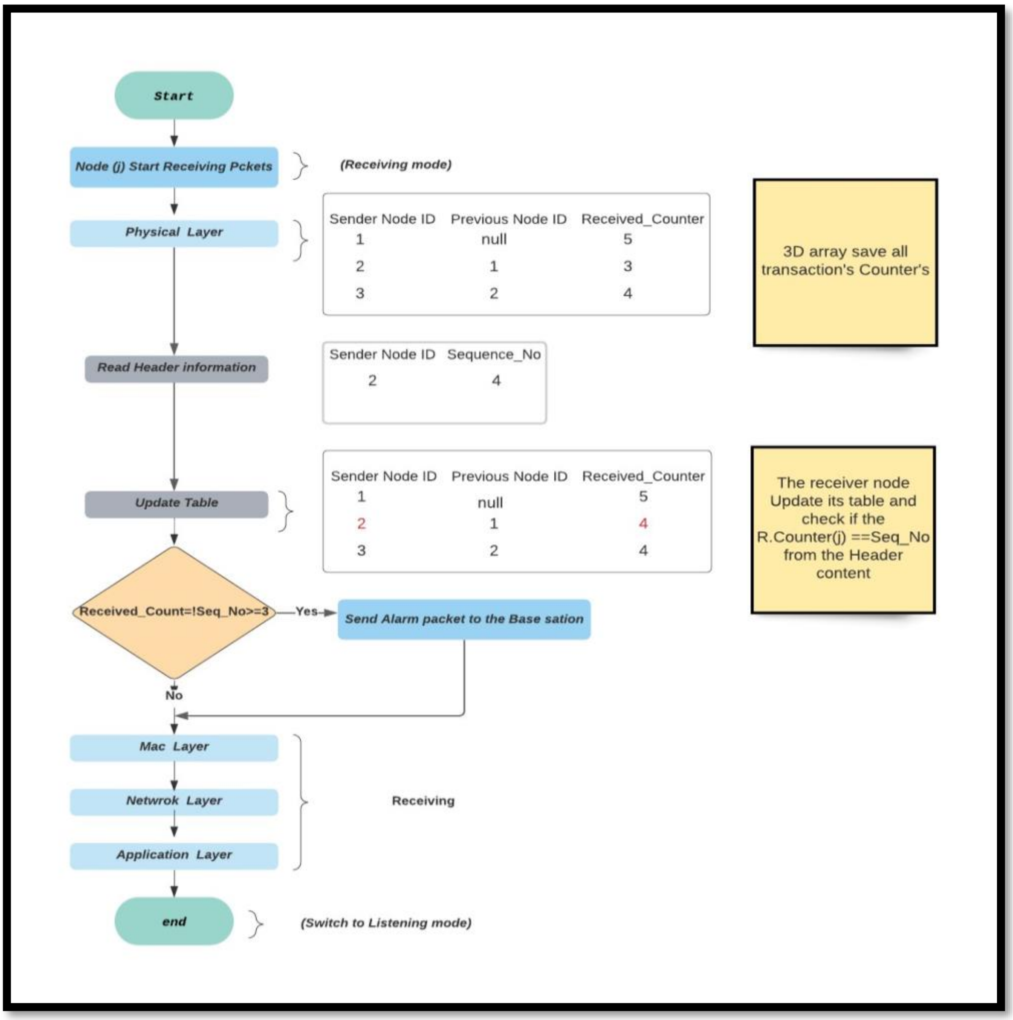
Transaction's Counts

Sender: 2

Sequence: 4

Sender ID	Received _Count $_x$
1	5
2	4
3	4

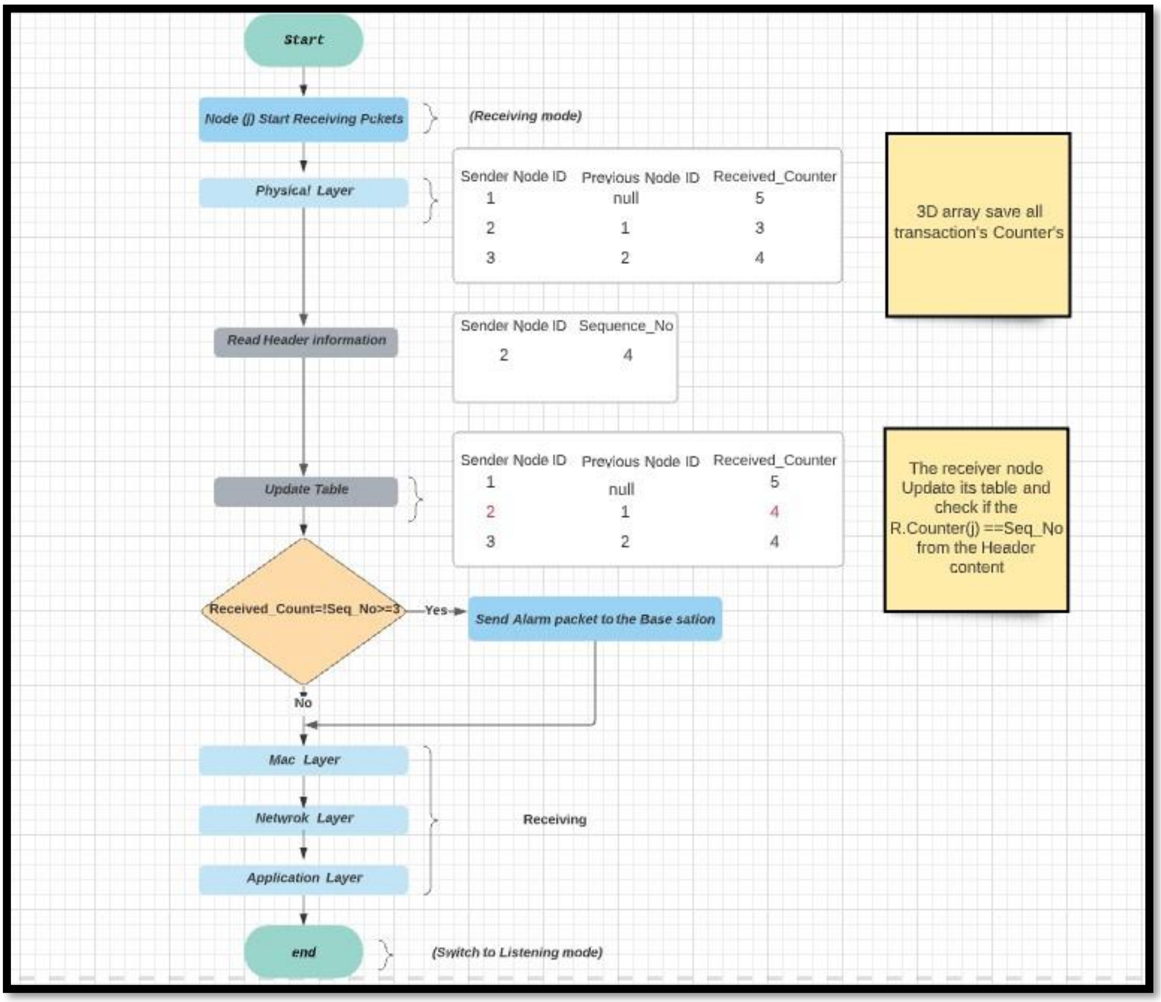
The receiver node update its table and check if the R-counter$_x$ == Seq_No from the header content


Start
Node (j) Start Receiving Pckets
(Receiving mode)
Physical Layer
Read Header information
Update Table
Received_Count=!Seq_No>=3
Yes
Send Alarm packet to the Base sation
No
Mac Layer
Netwrok Layer
Application Layer
Receiving
end
(Switch to Listening mode)
3D array save all transaction's Counter's
The receiver node Update its table and check if the R.Counter(j) ==Seq_No from the Header content

Sender Node ID	Previous Node ID	Received_Counter
1	null	5
2	1	3
3	2	4

Sender Node ID	Sequence_No
2	4

Sender Node ID	Previous Node ID	Received_Counter
1	null	5
2	1	4
3	2	4



Start
Node (j) Start Receiving Pckets
(Receiving mode)
Physical Layer
Read Header information
Update Table
Received_Count=!Seq_No>=3
Yes
Send Alarm packet to the Base sation
No
Mac Layer
Netwrok Layer
Application Layer
Receiving
end
(Switch to Listening mode)
3D array save all transaction's Counter's
The receiver node Update its table and check if the R.Counter(j) ==Seq_No from the Header content

Sender Node ID	Previous Node ID	Received_Counter
1	null	5
2	1	3
3	2	4

Sender Node ID	Sequence_No
2	4

Sender Node ID	Previous Node ID	Received_Counter
1	null	5
2	1	4
3	2	4

Figure 3-2 (Receiver Side)

3.2.2 Methodology flowchart

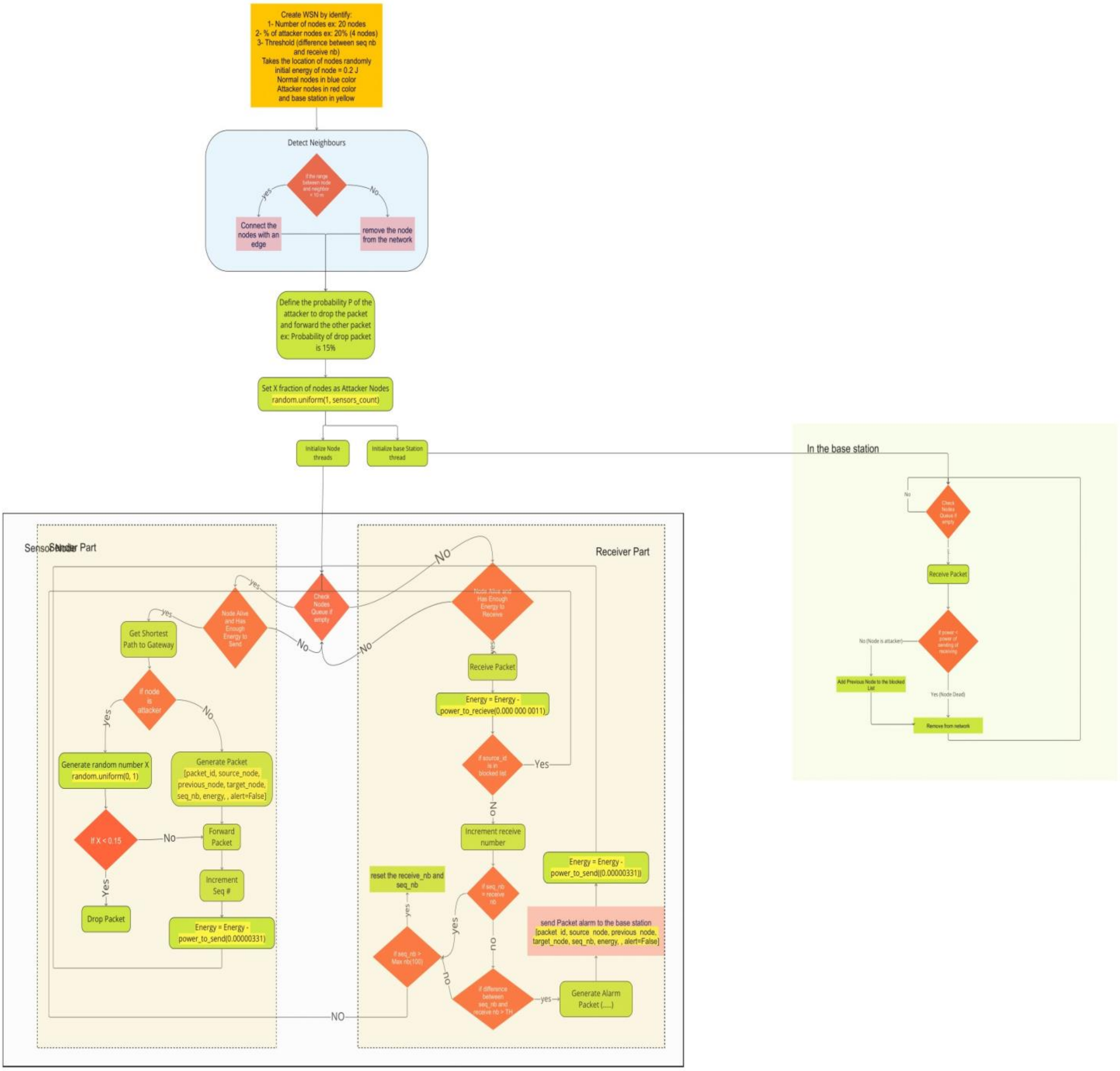

Create WSN by identify:
1- Number of nodes ex: 20 nodes
2- % of attacker nodes ex: 20% (4 nodes)
3- Threshold (difference between seq nb and receive nb)
Takes the location of nodes randomly
initial energy of node = 0.2 J
Normal nodes in blue color
Attacker nodes in red color
and base station in yellow
Detect Neighbours
if the range between node and neighbor < 10 m
yes
No
Connect the nodes with an edge
remove the node from the network
Define the probability P of the attacker to drop the packet and forward the other packet ex: Probability of drop packet is 15%
Set X fraction of nodes as Attacker Nodes random.uniform(1, sensors_count)
Initialize Node threads
Initialize base Station thread
Sensor Node
Sender Part
Check Nodes Queue if empty
yes
No
Node Alive and Has Enough Energy to Send
yes
No
Get Shortest Path to Gateway
If node is attacker
yes
No
Generate random number X random.uniform(0, 1)
Generate Packet [packet_id, source_node, previous_node, target_node, seq_nb, energy, , alert=False]
If X < 0.15
No
Yes
Forward Packet
Increment Seq #
Drop Packet
Energy = Energy - power_to_send(0.00000331)
NO
Receiver Part
NO
Node Alive and Has Enough Energy to Receive
No
yes
Receive Packet
Energy = Energy - power_to_recieve(0.000 000 0011)
if source_id is in blocked list
Yes
No
Increment receive number
if seq_nb = receive nb
yes
no
reset the receive_nb and seq_nb
yes
if seq_nb > Max nb(100)
no
if difference between seq_nb and receive nb > TH
yes
Generate Alarm Packet (.....)
send Packet alarm to the base station [packet_id, source_node, previous_node, target_node, seq_nb, energy, , alert=False]
Energy = Energy - power_to_send((0.00000331))
In the base station
No
Check Nodes Queue if empty
Receive Packet
if power < power of sending of receiving
No (Node is attacker)
Add Previous Node to the blocked List
Yes (Node Dead)
Remove from network

Figure 3-3 Methodology Flowchart **The sensor node may switch to many statuses:**

1- **Listening mode:** Waiting for transmission packet.

2- When event occur, the node switches to **transmission mode**, and then returns to the listening mode.

3- The node may be awakening by one of its preceding neighbors to forward their packets. It switches to **receiving mode**, receives the packets, sends them to its next-hop node, and returns to the listening mode. [1]

In addition, the total amount of the node energy is 0.2 Joule.

There are two types of transmission:

1- Generated Packets: in this type the node send alarm to Base station. [1]

2- Forwarding packet: which include all packets arriving from other nodes and using the considered node as a relay node. [1]

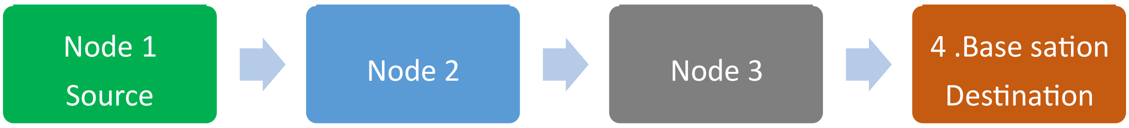


Figure 3-4 Trnsmission Nodes

As shown in the above figure, node 1 will send data to node 4 though nodes 2 and 3. The source node will send a Hello message to the neighbor nodes to build its initial routing table after it has the response from them.

When there is, a source node does not have a specific route for specific destination node to send on it, its initiate the DSR route discovery process as we explained in the previous steps. Once Source node got the RREP packet (with new route) from the Receiver node, it will update its routing table with the new route and generate header packet with specific flags contain sequence number and power flag then start the transmission process as follow:

Table 3-1 Header flag

Source ID	Seq_No	Destination ID	Previous Node ID	Current Node state	(power= PR)
1	1	4	null	Transmission	(1,0.19999669)

The above table the header contains the following flags:

1- Source ID: is the source Node which has the original data that will send to the destination.

2- Sequence number: is the packet sequence starts from 1 to the max sequence (when sequence number reach to max, it will auto reset its value to zero)

3- Destination ID: Is the destination Node which the final destination of the packet.

4- Previous Node ID: If transmission run through route, this flag will store the previous node ID.

5- Current Node State: is the status of the sender node.

6- Power: Is the current power of the sender node, this flag has 2D array the first one is the node ID and the second one is the current power.

The current power can calculate as the following equation:

$$Current\_power=initial\_power - consuming\_power \qquad \textbf{3-1}$$

Every node has 3D array in local memory, to store sender node ID, Previous node ID and received count as shown in the following table, after node 2 received the packet, it will increment received count value by one. Then the received node will compare the sequence number value of the sender node with its received count value, if they are matched or their different is less than the threshold value, it will be forwarding packet, otherwise the node will generate alarm packet to base station.

Table 3-2 node 3D array

Sender ID	Previous node ID	Receive Count
1	null	1

```
If (Sequencee_No  -  Received _Count) <th        3-2
                Forward packet
 Else
        Send_Alarm_Message to the BS
```

When node 2 transmit packet to node 3 it will update the header as shown in the following table:

Table 3-3 Node 2 Header Packet

Source ID	Seq_No	Destination ID	Previous Node ID	Current node status	(power= PR)
1	1	4	1	Transmission	(1,0.19999669), (2, 0.1999966889)

The above steps will repeat until the packet arrives at its destination. However, if there is any abnormal event such as differences between the sequence number and received count value is grater or equal to the threshold value, the node will send an alarm packet to the base station.

3.2.3 Send Alarm Packet to the Base station:

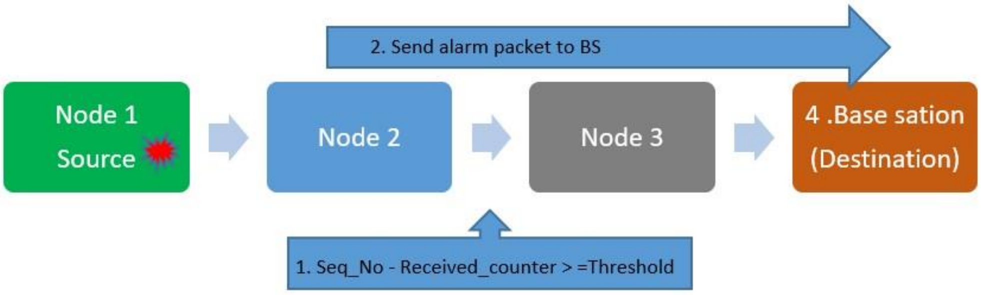

2. Send alarm packet to BS
Node 1
Source
Node 2
Node 3
4 .Base sation
(Destination)
1. Seq_No - Received_counter > =Threshold

Figure 3-2 Alarm Packet

Let Node 2 received packet from Node 1 and find (Seq_No and Received _count) >=TH

Then Send alarm packet to the BS as follow:

ALARM CODE=444_S.N=2_P.N=1_SEQ.No=5_R.Count=2_PWR=0.19999669

Which:

ALARM CODE =444: Error Alarm code

S.N: Sender Node: Node 2

P.N: Previous Node: Node 1 (Error Node)

Seq.NO: Sequence Number =5

R_COUNT: Received counter =2

PWR: Power of node 1 =0.19999669

For example:

Alarm packet fields: from the node 2 to the BS:

Table 3-4 Alarm Packet Flags

Sender node	Previous Node(P.N)	Sequence No	Received counter	Power of P.N
2	1	5	2	0.19999669

When the received node checks that, the Sequence_No! = Received_count and the difference between them is equal or higher than the threshold (3), 5! = 2 so an alarm packet will send to the BS, so the received node (2) will send the alarm packet to the BS to take the decision. In addition, the header of alarm packet contains the Previous Node ID.

3.2.4 Base station Make Decision:

when any packet arrives at to base station, the base station stores some information about this packet such as the current power of each node as shown in the following table, so when any node sends alarm packet to the base station it can be decide if the node dead or not by analyse its energy and if the node is attacked it will send a BC message to all others node and source node to block this malicious node from their routes.

Table 3-5 Nodes energy

Node ID	Current Energy
1	0.19999669
2	0.1999946
3	0.1999946

If Node (1) Current Power near to Zero, Then Node is dead. Else, it is an attack node (Discard to receive from this attacked node or Send Broadcast Packet to all nodes and to Source Node and resend packet with new path).

Then add this blocked node in the blocked node list by BS in the memory, to avoid overhead of the network with size five MB.

Therefore, in every receiving mode step if sender node was found as one of the blocked node the receiver node will stop receiving from this attacked node.

The following table shows all steps of the transmission data:

Table 3-6 steps of transmission data

Transmission SEQ_No	Node 1	Node 2	Node 3	Node 4
0	Default Energy A = 0.2	Default Energy A = 0.2	Default Energy A = 0.2	Default Energy A = 0.2
Packet Seq 1	Consume, (0.000 00331) Transmission mode =(0.19999669) current	Consume, (0.000 000 0011) Receiving mode - (0.000 00331) Transmission mode = (0.1999966889) current	Consume, (0.000 000 0011) Receiving mode - (0.000 00331) Transmission mode = (0.1999966889) current	Consume, (0.000 000 0011) Receiving mode = (0.1999999989) current
Packet Seq 2	Consume, (0.000 00331) Transmission mode = (0.19999338) current	Consume, (0.000 000 0011) Receiving mode - (0.000 00331) Transmission mode =(0.1999933778) current	Consume, Dead Node Receiving mode - (0.000 00331) Transmission mode = (0.1999933778) current	Consume, (0.000 000 0011) Receiving mode = (0.1999999978) current
Packet Seq 3	Consume, (0.000 00331) Transmission mode =(0.19999007) current	Consume, (0.000 000 0011) Receiving mode - (0.000 00331) Transmission mode = (0.1999900667) current	Consume, (0.000 000 0011) Receiving mode - (0.000 00331) Transmission mode = (0.1999900667) current	Consume, (0.000 000 0011) Receiving mode = (0.1999999967) current
Packet Seq 4	Not Send (Power Near Zero)	-	-	-

Packet Seq 5	Consume, (0.000 00331) Transmission mode = (0.19999007) current	Consume, (0.000 000 0011) Receiving mode - (0.000 00331) Transmission mode = (0.1999900667) current **Diff < TH** **DON’T Send Alarm to BS** **,then continue**	Consume, (0.000 000 0011) Receiving mode - (0.000 00331) Transmission mode = (0.1999900667) current	Consume, (0.000 000 0011) Receiving mode = (0.1999999956) current

As we showed in the above table, the nodes (1-4) have 0.2 Joule power.

In the first round of transmission, node 1 consumed 0.000 00331 NJ for transmission, node 2 consumed 0.000 000 0011 NJ for receiving mode, Transmission mode 0.000 00331 NJ, node 3 consumed 0.000 000 0011 NJ for receiving mode, Transmission mode 0.000 00331 NJ, node 4 consumed 0.000 000 0011 NJ for receiving mode.

In the second round nodes consuming energy as shown in row 3, also round three the nodes consume power as shown in next row, and so on.

However, in round four, node 1 did not send packet because the power is near-zero (has not enough power). But in case after it recharged by admin with a few power to send SEQ 5, in node 2 the sequence not matched with the Received count, the node 2 classified if the difference between them is grater or equal to the TH value, then send an alarm message to BS and reset counters, else continue transmission.

3.3 Conclusion to This Chapter

In this chapter, we discussed our methodology in deep. In the next chapter, we will discuss the simulation and its result .

Chapter 4: Simulation and Result

4.1 Introduction

In our simulation, we kickstart the process by utilizing the powerful capabilities of the NetworkX package. Leveraging the `fast_gnp_random_graph` function, we construct a dynamic wireless sensor network. This method allows us to fine-tune the network's characteristics by specifying the number of nodes and the edge probability, enabling us to precisely control the density of connections between the sensors and their neighboring nodes.

Next, we introduce a crucial element: the inclusion of attacker nodes. By defining a predetermined percentage of attacker nodes within the network, we establish a foundation for evaluating security protocols. This percentage is instrumental in calculating the precise number of attacker nodes present in the network. To ensure a balanced and realistic representation, we adopt a uniform random selection process cscsc from the pool of sensor nodes.

To facilitate concurrent operations within the network, we implement a custom thread class. This class enables nodes to operate in parallel, enhancing the efficiency and responsiveness of the simulation. This multithreaded approach is pivotal in simulating real-world scenarios where nodes must execute tasks simultaneously, allowing us to glean valuable insights into the network's overall performance under diverse conditions.

Sender part:

In the sender module, once the node is activated, we initiate a crucial series of checks. Firstly, we inspect whether the queue of this particular node is either empty or currently contains a packet awaiting transmission. If the queue is vacant, the node is poised to initiate transmission. Subsequently, a critical energy assessment is conducted to ascertain if the node possesses adequate energy reserves to transmit. This evaluation hinges on comparing the node's current energy level against the threshold required for packet transmission.

Upon confirming the node's eligibility to send, a brief two-second countdown ensues. Following this interval, the node executes the transmission process in adherence to the

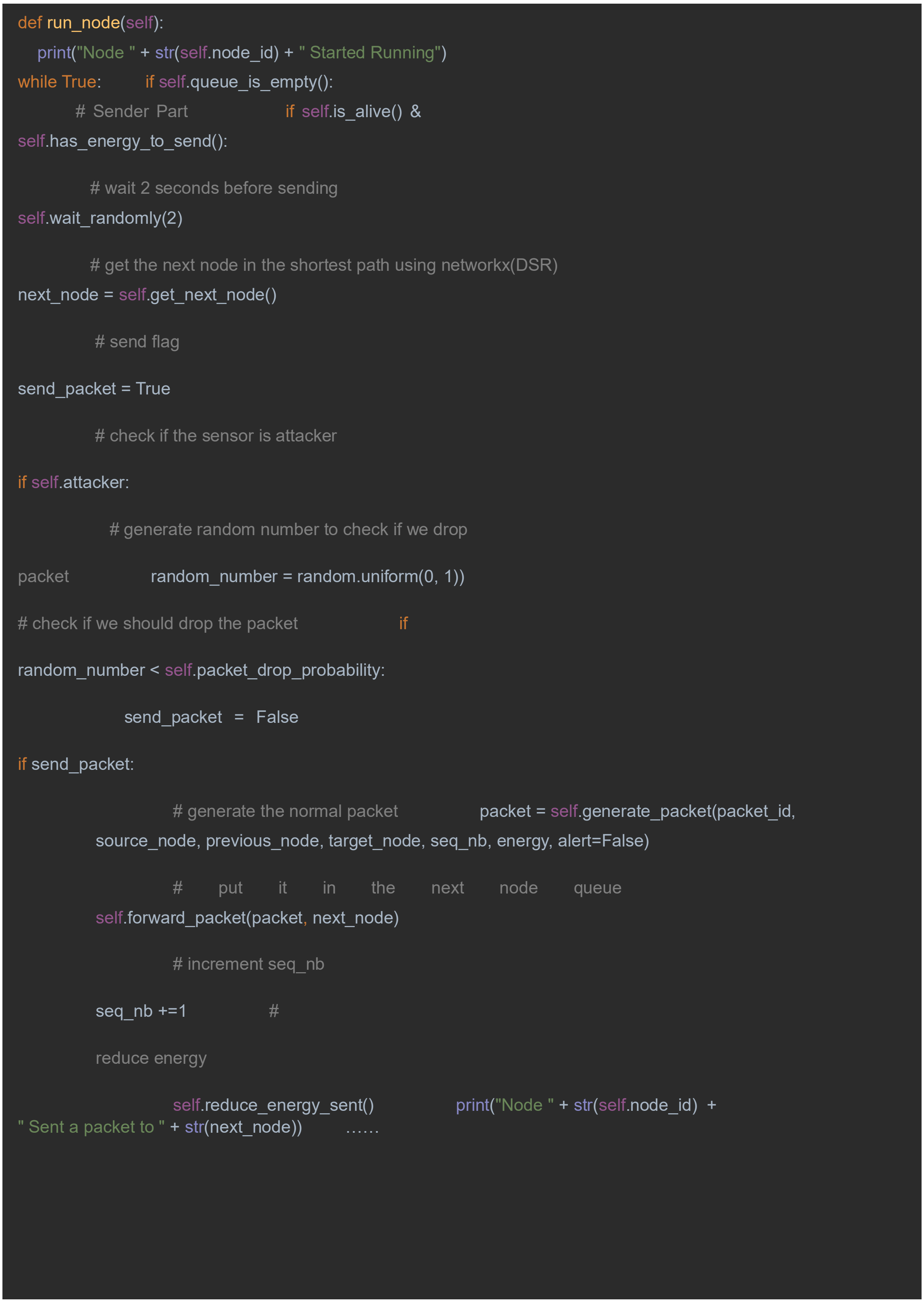
Dynamic Source Routing (DSR) protocol, and the sequence number is increment. At this juncture, an important determination is made: whether the packet being dispatched is of malicious origin. This determination is influenced by the predetermined probability of a node being an attacker.

In scenarios where the protocol adhered to is normal, the node proceeds to generate a packet and subsequently dispatches it to the next designated node in the network. This seamless process ensures the robustness and reliability of our simulation, allowing for comprehensive analysis of network behavior under varying conditions and potential security breaches.

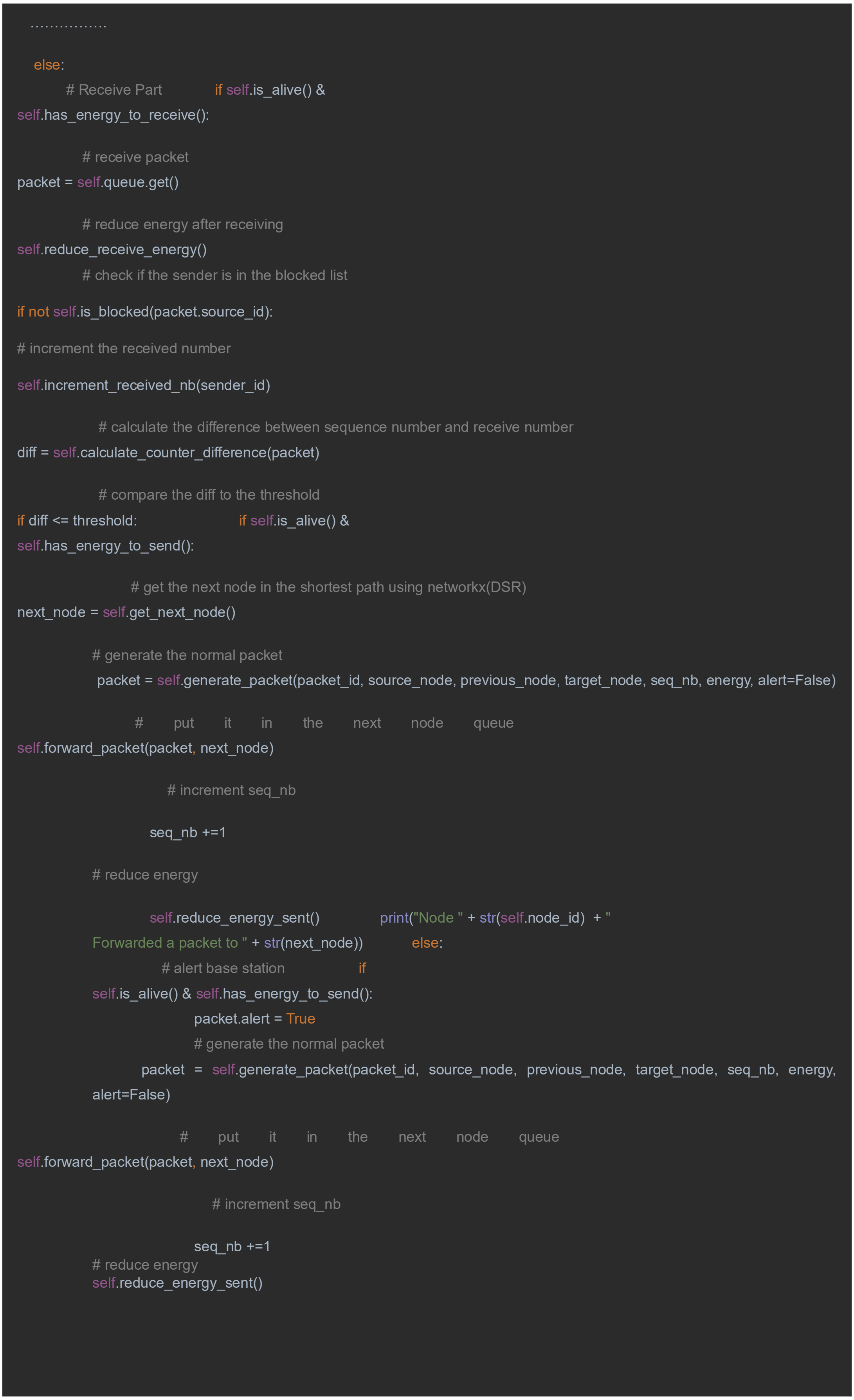
Receiver part:

In the receiver module, a meticulous set of conditions are evaluated to ensure seamless packet reception. Firstly, we scrutinize the node's packet queue to determine if it holds any awaiting transmissions. Simultaneously, we gauge the node's energy reserves to confirm that it's capable of receiving the incoming packet. If both conditions are met, the node proceeds to extract the packet from the queue, incurring an energy cost, and increments the count of successfully received packets.

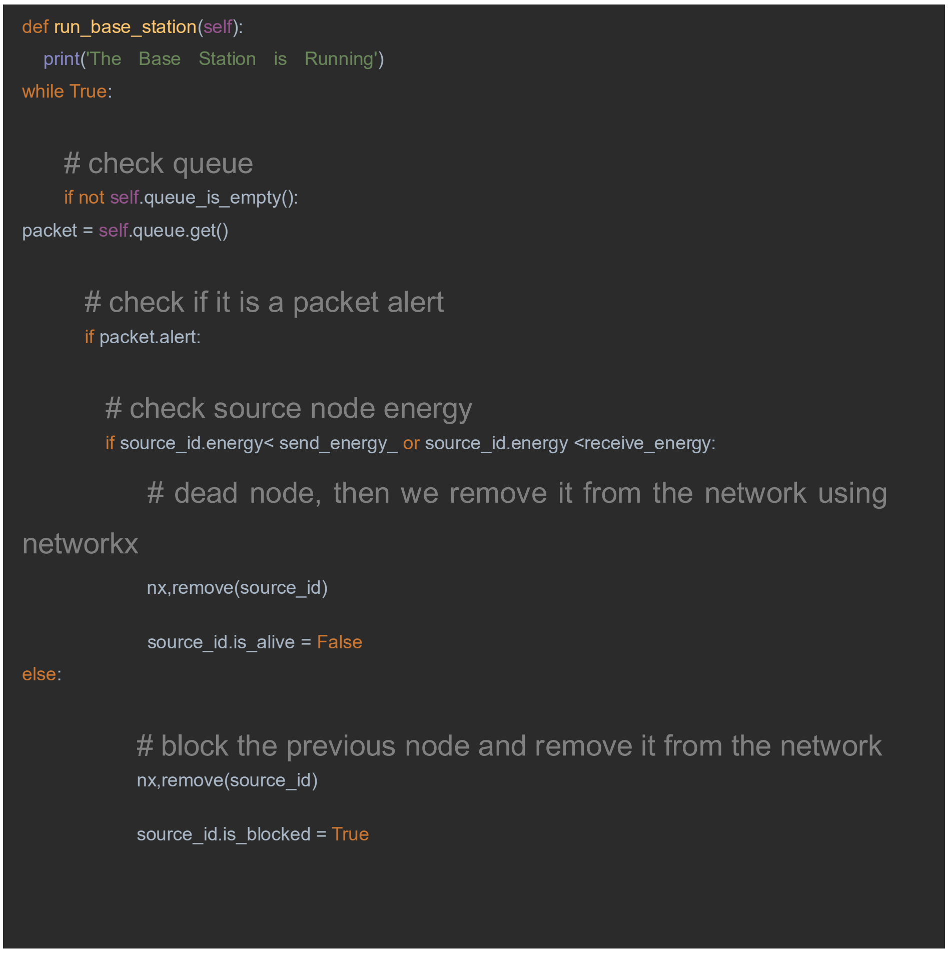
Next, a crucial metric is computed: the disparity between the sequence number and received number of packet. This differential is pivotal in evaluating the integrity of the communication. If this difference exceeds a predetermined threshold, an alarm packet is promptly dispatched to the base station, effectively signaling a potential security breach. This notification unequivocally designates the node as a compromised or attacker node, triggering immediate response measures. This sophisticated detection mechanism fortifies the network against potential threats and allows for swift identification and mitigation of security vulnerabilities. The base station specify the packet which is from attacker node, then the base station remove the previous node that send this packet.



```
def run_node(self):
    print("Node " + str(self.node_id) + " Started Running")
while True:         if self.queue_is_empty():
         # Sender Part                  if self.is_alive() &
self.has_energy_to_send():

            # wait 2 seconds before sending
self.wait_randomly(2)

            # get the next node in the shortest path using networkx(DSR)
next_node = self.get_next_node()

             # send flag

send_packet = True

             # check if the sensor is attacker

if self.attacker:

               # generate random number to check if we drop

packet                 random_number = random.uniform(0, 1))

# check if we should drop the packet                    if

random_number < self.packet_drop_probability:

                  send_packet  =  False

if send_packet:

                         # generate the normal packet                packet = self.generate_packet(packet_id,
             source_node, previous_node, target_node, seq_nb, energy, alert=False)

                         #      put      it      in      the      next      node      queue
             self.forward_packet(packet, next_node)

                         # increment seq_nb

             seq_nb +=1                #

             reduce energy

                         self.reduce_energy_sent()               print("Node " + str(self.node_id)  +
" Sent a packet to " + str(next_node))        ……
```



```
  ................

   else:
         # Receive Part             if self.is_alive() &
self.has_energy_to_receive():

            # receive packet
packet = self.queue.get()

            # reduce energy after receiving
self.reduce_receive_energy()
            # check if the sender is in the blocked list

if not self.is_blocked(packet.source_id):

# increment the received number

self.increment_received_nb(sender_id)

               # calculate the difference between sequence number and receive number
diff = self.calculate_counter_difference(packet)

               # compare the diff to the threshold
if diff <= threshold:                      if self.is_alive() &
self.has_energy_to_send():

                     # get the next node in the shortest path using networkx(DSR)
next_node = self.get_next_node()

              # generate the normal packet
               packet = self.generate_packet(packet_id, source_node, previous_node, target_node, seq_nb, energy, alert=False)

                     #     put     it     in     the     next     node     queue
self.forward_packet(packet, next_node)

                           # increment seq_nb

                        seq_nb +=1

              # reduce energy

                        self.reduce_energy_sent()              print("Node " + str(self.node_id)  + "
              Forwarded a packet to " + str(next_node))           else:
                          # alert base station                  if
              self.is_alive() & self.has_energy_to_send():
                                packet.alert = True
                                # generate the normal packet
                       packet  =  self.generate_packet(packet_id,  source_node,  previous_node,  target_node,  seq_nb,  energy,
              alert=False)

                             #     put     it     in     the     next     node     queue
self.forward_packet(packet, next_node)

                                   # increment seq_nb

                                seq_nb +=1
              # reduce energy
              self.reduce_energy_sent()
```



```
def run_base_station(self):
  print('The  Base  Station  is  Running')
while True:

    # check queue
    if not self.queue_is_empty():
packet = self.queue.get()

      # check if it is a packet alert
      if packet.alert:

        # check source node energy
        if source_id.energy< send_energy_ or source_id.energy <receive_energy:

            # dead node, then we remove it from the network using
networkx
            nx,remove(source_id)

            source_id.is_alive = False
else:

           # block the previous node and remove it from the network
           nx,remove(source_id)

           source_id.is_blocked = True
```

In our simulation scenario, we use 50, 100,150 and 400 nodes. We divided it into 70% nodes as trusted or legitimate and 30% nodes as malicious. The nodes are placed randomly in the area of 500 * 500 m^2 using python simulation. We run the simulation with the initial parameters shown in the following table.

Table 4-1 Simulation Parameters

Parameter	Value
Network size	500*500 m^2
Initial energy	0.2 J
Protocol	802.11
Radio Model	FRIIS
Trust Node	70%
malicious node	30%

We run the simulation over three tests (50, 100,150 and 400) nodes, each test runs three times and takes an average of the results of it.

4.2 Result

4.2.1 Test One (50 Nodes)

Table 4-2 Test 50 node

Tests	NO. Trust	NO. malicious	Number of Transmission	Detecting NO	Accuracy %
1	35	15	14200	13	87%
2	35	15	14200	12	80%
3	35	15	14200	12	80%
AVG					82%

In the above table, we show the test of our technique which run three times when use 50 nodes, and we determined 15 malicious nodes, the system detect about 82% average.

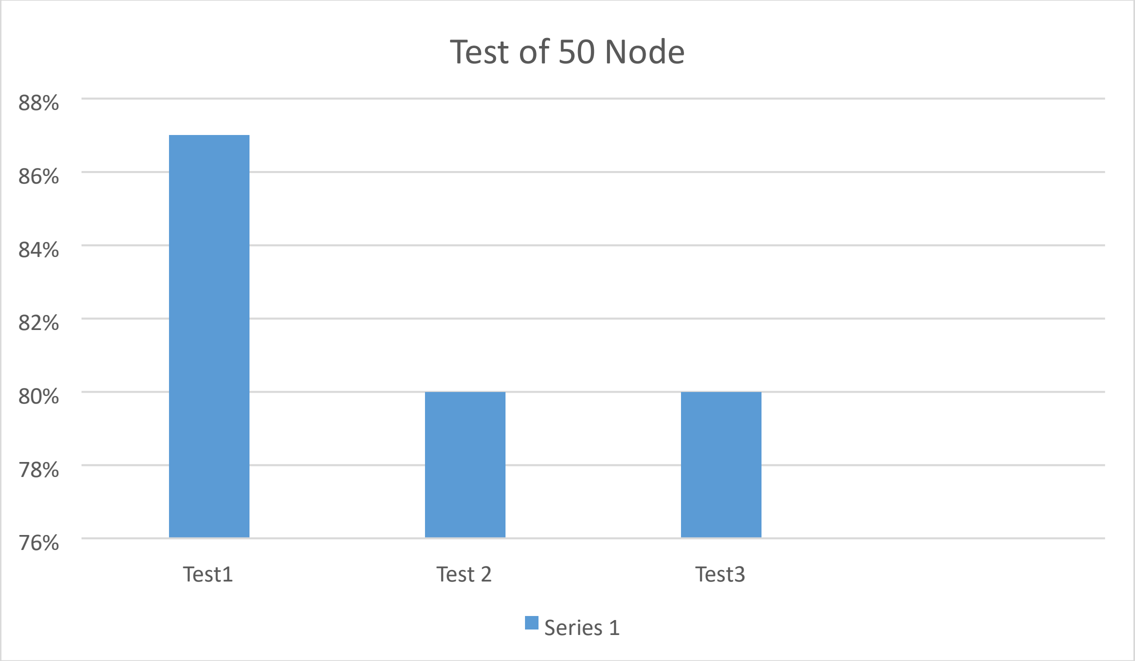


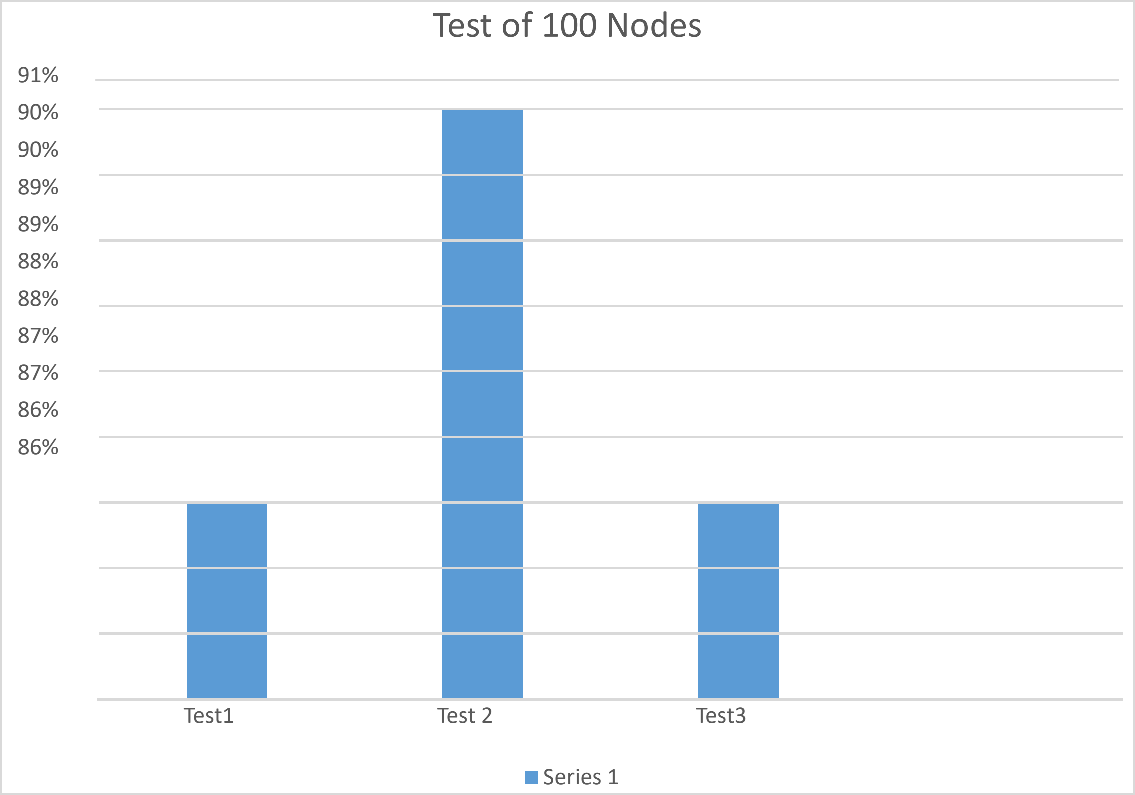
Figure 4-1 50 Node Chart

4.2.2 Test Two (100 Nodes)

Table 4-3 test 100 Node

Tests	NO. Trust	NO. malicious	Number of Transmission	Detecting NO	Accuracy %
1	70	30	25080	26	87%
2	70	30	25080	27	90%
3	70	30	25080	26	87%
AVG					88%

In the above table, we show the test of our technique which run three times when use 100 nodes, and we determined 30 malicious nodes, the system detect about 88% average.



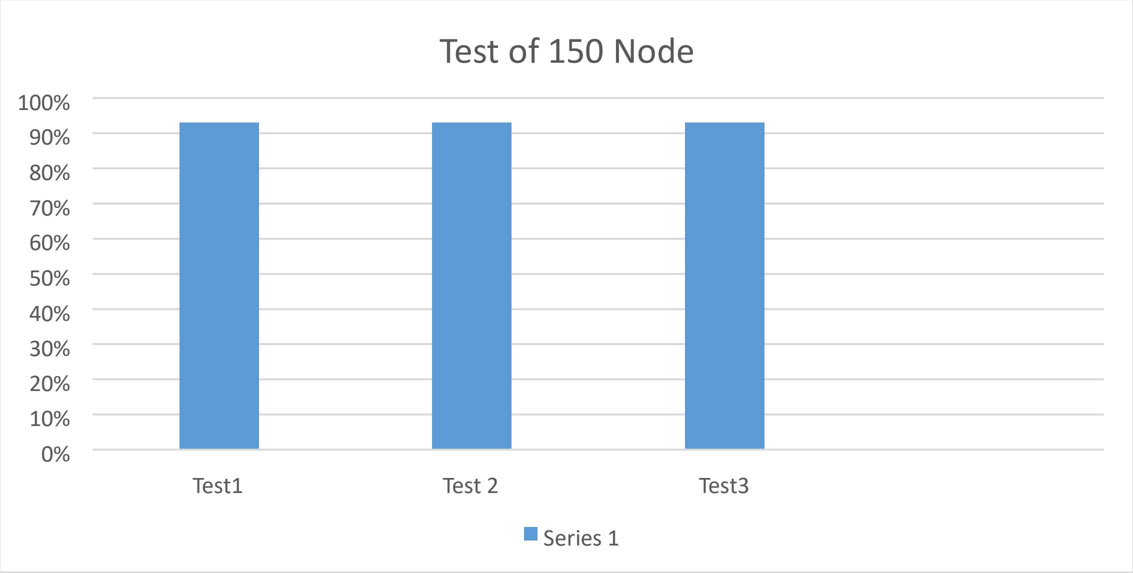
4.2.3 Test Three (150 Nodes)

Table 4-4 test 150 Node

Tests	NO. Trust	NO. malicious	Number of Transmission	Detecting NO	Accuracy %
1	105	45	69600	42	93%
2	105	45	69600	42	93%

3	105	45	69600	42	93%
AVG					93%

In the above table, we show the test of our technique which run three times when use 150 nodes, and we determined 45 malicious nodes, the system detect about 93% average.



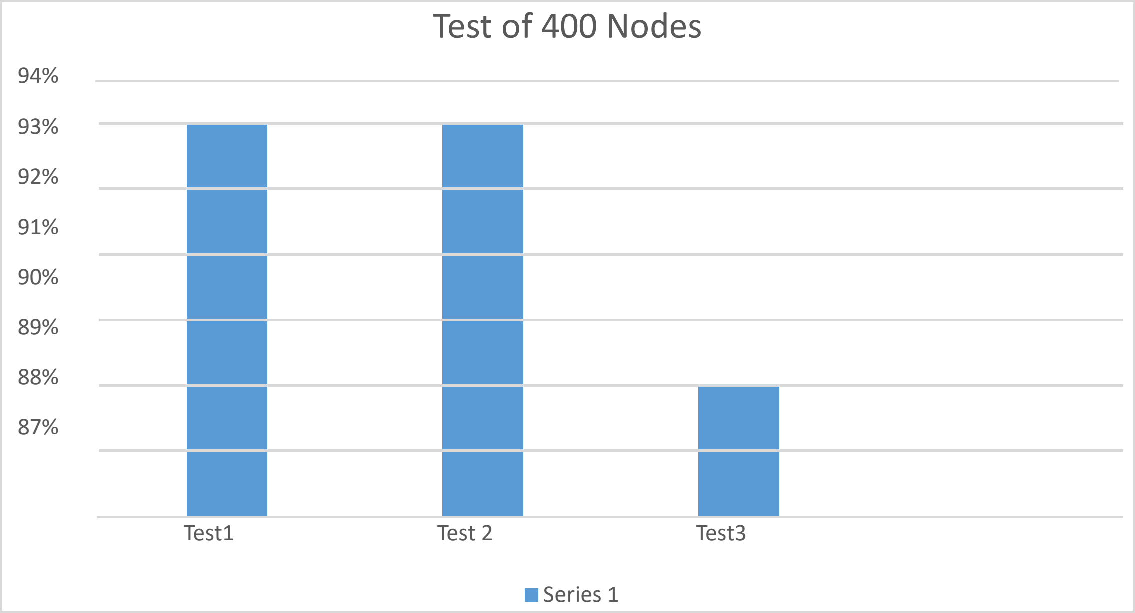
4.2.4 Test Four (400 Nodes)

Table 4-5 test 400 Node

Tests	NO. Trust	NO. malicious	Number of Transmission	Detecting NO	Accuracy %
1	280	120	356640	112	93%
2	280	120	356640	112	93%
3	280	120	356640	107	89%

AVG			92%

In the above table, we show the test of our technique which run three times when use 400 nodes, and we determined 120 malicious nodes, the system detect about 92% average.



4.3 Conclusion to This Chapter

Our technique is to detect and protect from selective forwarding attack in the WSN by using a sequence number and received count technique to check the node behaviour in the network and get an accuracy result to evaluate our simulation.

Chapter 5: Another Chapter (Discussion?)

5.1 Introduction 5.2 Section

5.2.1 Sub-section

5.3 Conclusion to This Chapter

Give the reader a reminder of the key points for this chapter. Then, tell them what follows in the next chapter.

Chapter 6: Conclusion and Future Work

6.1 Introduction 6.2 Section

Possible sections might include:

- Contributions to existing knowledge
- Future work

6.2.1 Sub-section

References

[1] N.-E. R. Aljawharah Alnasser, “New trust-based detection model for concealed malicious nodes in a wireless sensor network,” *ResearchGate,* 2015.

[2] B. G. G. T. Soltani, "Covert single-hop communication in a wireless network with distributed artificial noise generation". 2014 52nd Annual Allerton Conference on Communication, Control, and Computing," *Annual Allerton Conference on Communication, Control, and Computing (Allerton),* vol. 2, no. 1, p. 1078–1085, 2014.

[3] C. ,. S. K. Hongbing, "Weighted trust evaluation-based malicious node detection for wireless sensor networks.," *International Journal of Information and ComputerSecurity,* vol. 3, pp. 132-149, 2009.

[4] j. J. G. Han, "An Efficient Distributed Trust Model for Wireless Sensor Networks," *LATEX,* vol. 26, no. 5, pp. 1228 - 1237, 2015.

[5] N. F. F. K. KalsoomShabana, "Security issues and attacks in Wireless Sensor Networks," *International Journal of Advanced Research in Computer Science and Electronics Engineering,* vol. 5, no. 7, pp. 81-87, 2016.

[6] L. B. S. R. B. A. Fatma Gara, "An Efficient Intrusion Detection System for Selective Forwarding and Clone Attackers in IPv6-based Wireless Sensor Networks under Mobility," *International Journal on Semantic Web and Information Systems,* vol. 13, no. 3, pp. 22-24, 2017.

[7] M. F. Y. ,. K. A. A. Moustafa A. Youssef, “A Constrained Shortest-Path EnergyAware Routing Algorithm for Wireless Sensor Networks,” *IEEE,* 1997.

[8] P. R.-P. Juan Cota-Ruiz, “A Recursive Shortest Path Routing Algorithm With Application for Wireless Sensor Network Localization,” *IEEE SENSORS JOURNAL,* vol. 16, no. 11, p. 4631, 2016.

[9] N. S. a. S. R. Hassan, “Routing Protocols for Wireless Sensor Networks (WSNs),” *intechopen,* no. 10.5772, October 4th 2017.

[10] C. FU, “An Energy Balanced Algorithm of LEACH Protocol in WSN,” *International Journal of Computer Science ,* vol. 10, no. 1, p. 354 , January 2013 .

[11] N. S. a. S. R. Hassan, “Routing Protocols for Wireless Sensor Networks (WSNs),” *RESEARCH GATE,* October 2017.

[12] J. K. a. others, “Wireless Sensor Network (WSN) Configuration Method to Increase Node Energy Efficiency through Clustering and Location Information,” *Symmetry,* vol. 13, pp. 1-11, 2021.

[13] A. N. C. K. Ramachandram, “Ad-Hoc On Demand Distance Vector Routing Algorithm Using Neighbor Matrix Method in Static Ad-Hoc Networks,” *International Conference on Computer Science and Information Technology,* vol. 132, pp. 44-54, 2011.

[14] *. ,. C. M.-P. 2. R. V. 4. a. A. R.-S. Carolina Del-Valle-Soto 1, “Wireless Sensor Network Energy Model and Its Use in the Optimization of Routing Protocols,” *Energies,* vol. 13, no. 728, pp. 1-33, 2020.

[15] N. R. I. M. Z. J. Shabbir N, “Routing protocols for a small scale WLAN based wireless sensor networks,” *9th International Conference on Sensing Technologies. New Zealand: IEEE,* 2015.

[16] P. Muthusamy, “Sybil Attack Detection Based on Authentication Process Using Digital Security Certificate Procedure for Data Transmission in MANET,” *International Journal of Engineering & Technology,* pp. 270-276 , 2018.

[17] N. M. A. a. K. M. Elleithy, "Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks," *International Journal of Computer Applications,* vol. 111, no. 14, p. 0975 – 8887, 2015.

[18] a. o. KalsoomShabana, "Security issues and attacks in Wireless Sensor Networks," *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE),* 2016.

[19] H. S. Rajat Malik, "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 0976-5697, 2017.

[20] X. L. ,. H. L. ,. J. L. Anfeng, "A multi data and multi ACK verified selective forwarding attack detection schema in WSN," *IEICE Transactions on Information and Systems,* vol. E99, no. 8, 2016.

[21] A. A. Nasser-Eddine Rikli, "New trust-based detection model for concealed malicious nodes in a wireless sensor network," *Conference Paper Research gate,* vol. RG.2.1.5121.352, 2015.

[22] N. M. A. a. K. M. Elleithy, "Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks," *International Journal of Computer Applications (0975 – 8887),* vol. 111, no. 14, p. 0975 – 8887, 2015.

[23] K. A, "A Secure and Advanced Data Gathering Pattern for Wireless Sensor Networks.," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 4, no. 5, pp. 8409 - 8415, 2016.

[24] N. M. A. a. K. M. Elleithy, "Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks," *International Journal of Computer Applications ,* vol. 111, no. 4, p. 0975 – 8887, 2015.

[25] Aircc, "investigration computational intellegant techniques for IDS in WSN," *MCDERMOTT,* vol. 3826, no. 0795, pp. 45-56, 2017.

[26] K. E. Naser Alajmi, "A MULTI-LAYER APPROACH FOR DETECTION OF SELECTIVE FORWARDING ATTACKS IN WIRELESS SENSOR NETWORKS," *sensors,* vol. 15, no. ISSN 1424-8220, pp. 29332-29345, 2016.

[27] V. S. Kanchan Kaushal, "Early Detection of DDoS Attack in WSN," *International Journal of Computer Applications (0975 – 8887),* 2016.

[28] X. S. ,. B. W. Huijuan Deng, "Selective forwarding attack detection using watermark in wsns," *ISECS International Colloquium on Computing, Communication, Control, and Management,* no. 978-1-4244-4247-8, 2013.

[29] N. V. M. Gaurav Gulhane, "Securing multipath routing protocol using authentication approach for wireless sensor network.," *International Conference on Communication Systems and Network Technologies,* vol. 59, no. 1, pp. 222231, 2014.

[30] E. B. S. S. D. J. S. Er. Amandeep Singh, "A Fuzzy Approach to Avoid Selective Forwarding Attacks and Energy Efficient Path Selection in Wireless Mesh Networks," *International Journal of Engineering and Management Research,* vol. 4, no. 2, pp. 164-169, 2014.

[31] PHACK, "An Efficient Scheme for Selective Forwarding Attack Detection in WSNs," 2015.

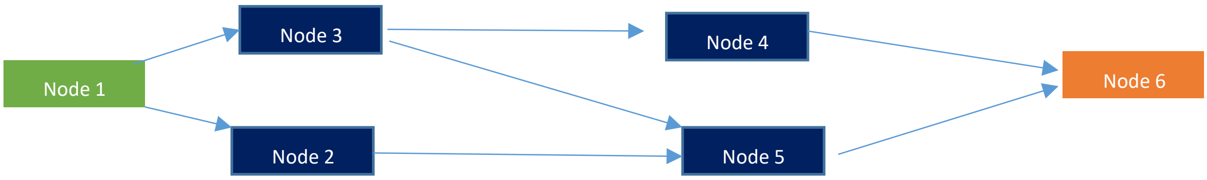
[32] T. N. a. M. R. Avijit Mathur, "Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs," *Sensors,* vol. 16, no. 1, 2016.

[33] B. X. Bo Yu, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," *IEEE,* pp. 1-8, 2016.

[34] N.-E. R. a. A. Alnasser, "Lightweight trust model for the detection of concealed malicious nodes in sparse wireless ad hoc networks," *International Journal of Distributed Sensor Networks,* vol. 12, pp. 1-16, 2016.

Appendix A: Our Scenario in Different Cases

Case 1:



- **Process 1 (Trust) one genral example with nodes + its equation**

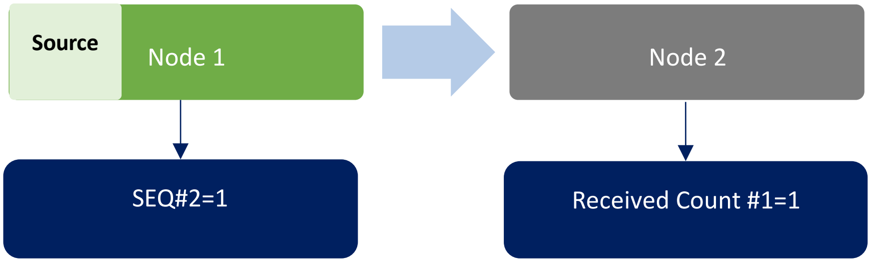
- **Node 1 :**

  1- **Run DSR**

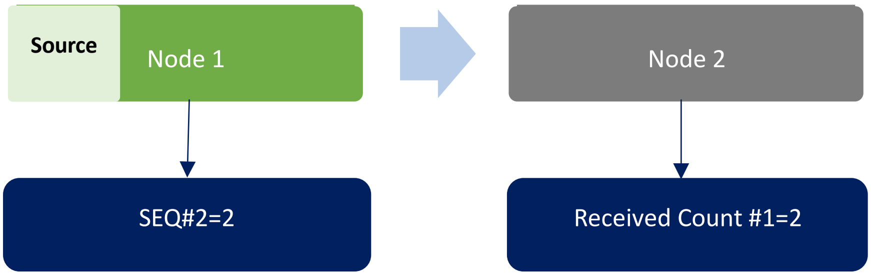
#	Route
1	1-3-4-6
2	1-2-5-6
3	1-3-5-6

2- **Start Transmission**

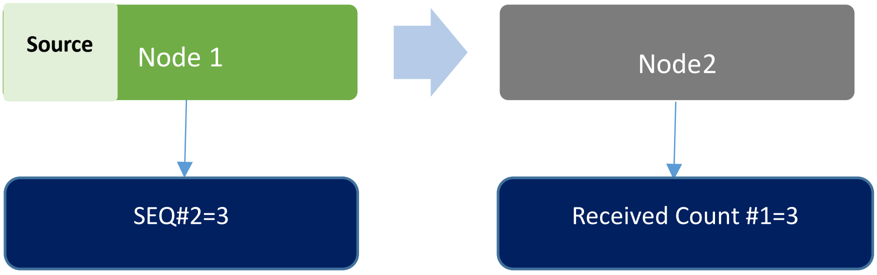
- **Send Packet 1 from node 1 to node 2**



- **Send Packet 2 from node 1 to node 2**



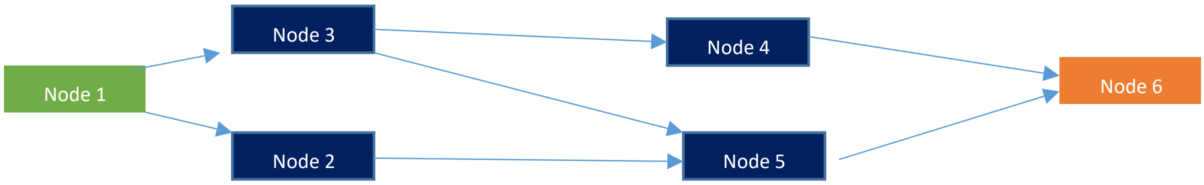
- **Send Packet 3 from node 1 to node 2**



Repeat Until Send 5 Packets....

#	sender	Packet NO	Sequence	Receiver	Received Count	Current Sender Power	Current Receiver Power	Comments
1	1	1	1	2	1	0.19	0.195	
2	1	2	2	2	2	0.18	0.19	
3	1	3	3	2	3	0.17	0.185	
4	1	4	4	2	4	0.16	0.18	
5	1	5	5	2	5	0.15	0.175	
6	2	1	1	5	1	0.165	0.195	Now 2 is sender the power change
7	2	2	2	5	2	0.155	0.19	
8	2	3	3	5	3	0.145	0.185	
9	2	4	4	5	4	0.135	0.18	
10	2	5	5	5	5	0.125	0.175	
11	5	1	1	6	1	0.165	0.195	Now 5 is sender the power change
12	5	2	2	6	2	0.155	0.19	
13	5	3	3	6	3	0.145	0.185	
14	5	4	4	6	4	0.135	0.18	
15	5	5	5	6	5	0.125	0.175	

Case 2:



- **Process 2 (Attacked)**

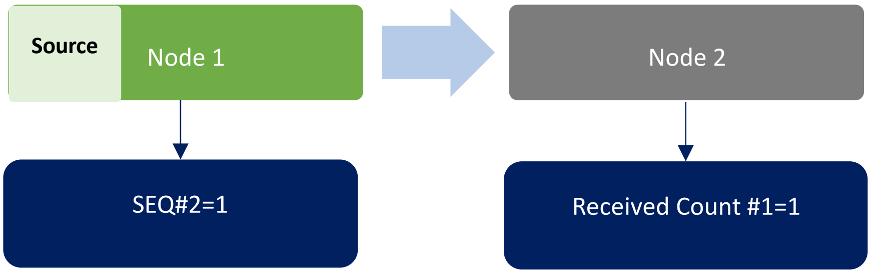
- **Node 1 :**

3- Run DSR

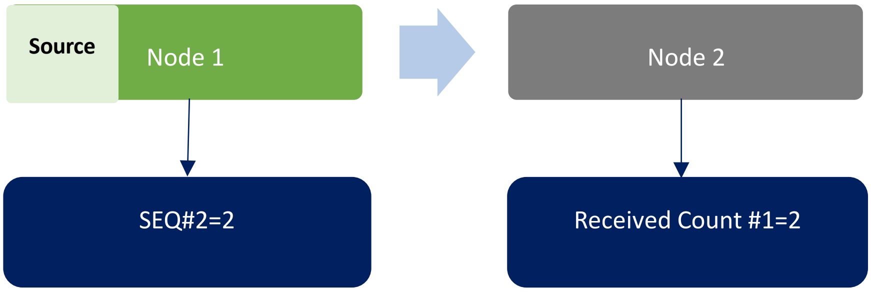
#	Route
1	1-3-4-6
2	1-2-5-6
3	1-3-5-6

4- Start Transmission

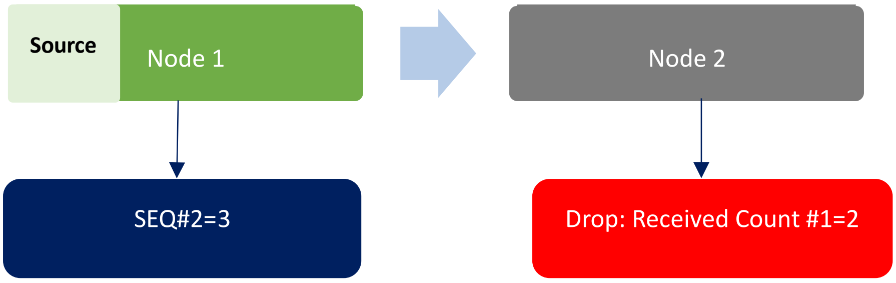
- **Run DSR And Send Packet 1 from node 1 to node 2**



- **Send Packet 2 from node 1 to node 2.**



- **Send Packet 3 from node 1 to node 2.**



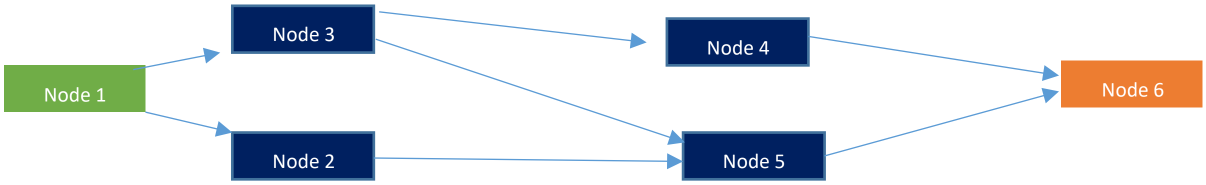
Repeat Until Send 5 Packet….

#	sender	Packet NO	Sequence	Receiver	Received Count	Current Sender Power	Power
1	1	1	1	2	1	0.19	
2	1	2	2	2	2	0.18	
3	1	3	3	2	DROP 2	0.17	
4	1	4	4	2	3	0.16	
5	1	5	5	2	DROP 3	0.15	0.175
6	2	1	1	5	1	0.165	
7	2	2	2	5	2	0.155	
8	2	3	3	5	3	0.145	
9	2	4	4	5	4	0.135	
10	2	5	5	5	5	0.125	

11	5	1	1	6	1	0.165	
12	5	2	2	6	2	0.155	
13	5	3	3	6	3	0.145	
14	5	4	4	6	4	0.135	
15	5	5	5	6	5	0.125	

Notes: In the previous Case, the system can't Detect the Attack cause the drop time <TH.

Case 3:



- **Process 2 (Attacked)**

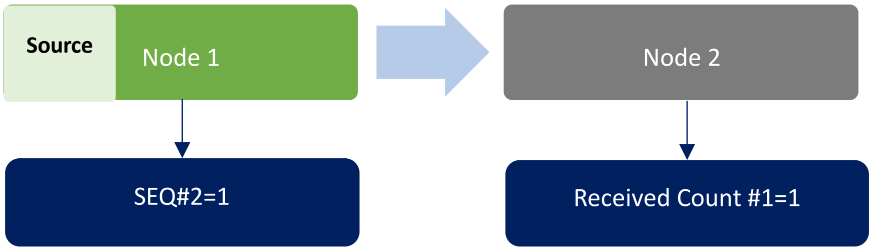
- **Node 1 :**

1- Run DSR

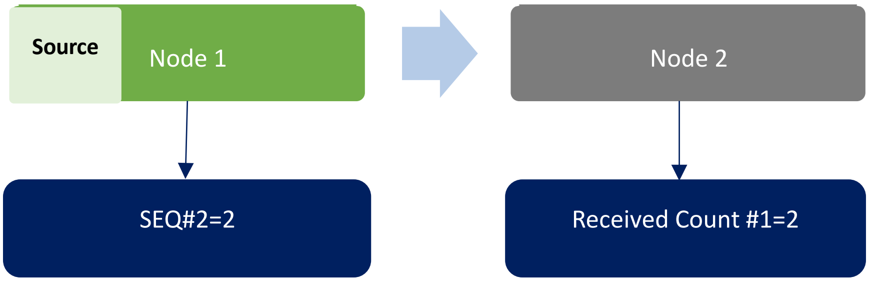
#	Route
1	1-3-4-6
2	1-2-5-6
3	1-3-5-6

2- Start Transmission

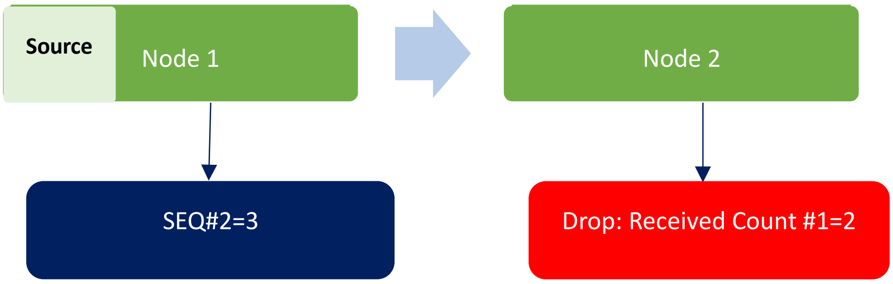
- **Send Packet 1 from node 1 to nod 2**



- **Send Packet 2 from node 1 to node 2**



- **Send Packet 3 from node 1 to node 2**


Source

Node 1

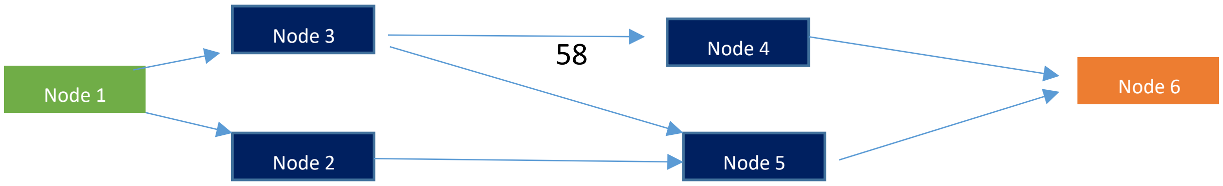
Node 2

SEQ#2=3

Drop: Received Count #1=2

Repeat Until Send 5 Packets...

#	der se	Packet Sequence No		Receiver	Received Count	Current Sender Power	Current Receiver Power	Comme
1	1	1	1	2	1	0.19	**0.195**	
2	1	2	2	2	DROP 1	0.18	**0.19**	
3	1	3	3	2	DROP 1	0.17	**0.185**	
4	1	4	4	2	2	0.16	**0.18**	
5	1	5	5	2	DROP 2	0.15	**0.175**	
6							**0.195**	
7		SEND ALARM MESSAGE						
8								
9								
10								Seq_no=!R.count>=3
11	2	1	1	5	1	0.14		Node 5 send the alarm packet to the BS (node 6)
12	5	1	1	6 Base Station	1	0.165		forward the packet to the BS



13								
14								
15								

Notes: In the previous Case, the system Detect the Attack.

Case 4:

- **Process 2 (Attacked)**

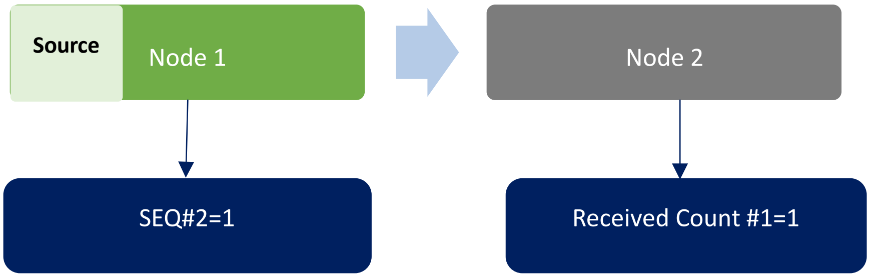
- **Node 1 :**

1- Run DSR

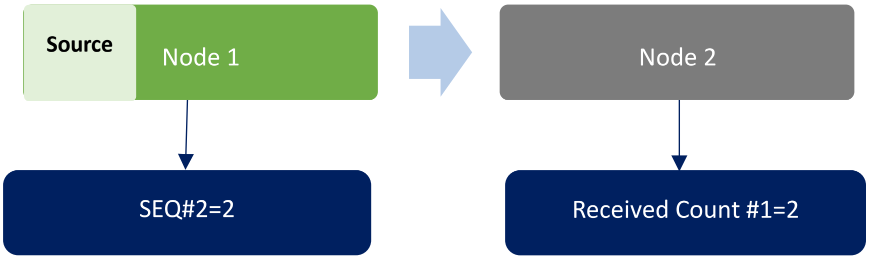
#	Route
1	1-3-4-6
2	1-2-5-6
3	1-3-5-6

2- Start Transmission

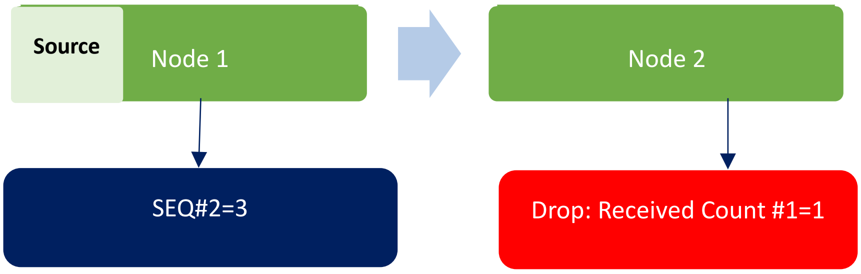
- **Send Packet 1 from node 1 to node 2.**



- **Send Packet 2 from node 1 to node 2.**



- **Send Packet 3 from node 1 to node 2**



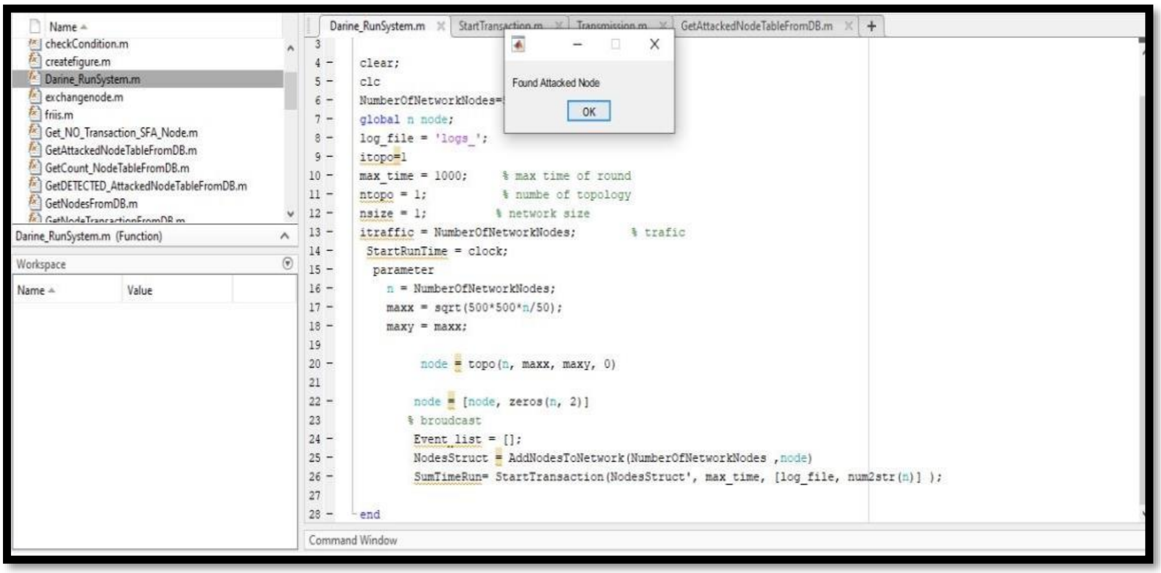
Repeat Until Send 5 Packets….

#	sender	Packet No	Sequence	Receiver	Received Count	Current Sender Power	Current Receiver Power	Comments
1	1	1	1	2	1	0.19	0.195	
2	1	2	2	2	DROP 1	0.18	0.19	
3	1	3	3	2	DROP 1	0.17	0.185	
4	1	4	4	2	2	0.16	0.18	
5	1	5	5	2	DROP 2	0.15	0.175	Seq_no=!R.count>=3
6							0.195	
7		SEND ALARM MESSAGE						
8								
9								
10								
11	2	1	1	4	1	0.14		Node 2 send the alarm packet to the bs (node 6) by node 4

12	Node 4 Drop alarm Packet ….. Doesn't Detect							Node 4 drop the packet
13								
14								
15								

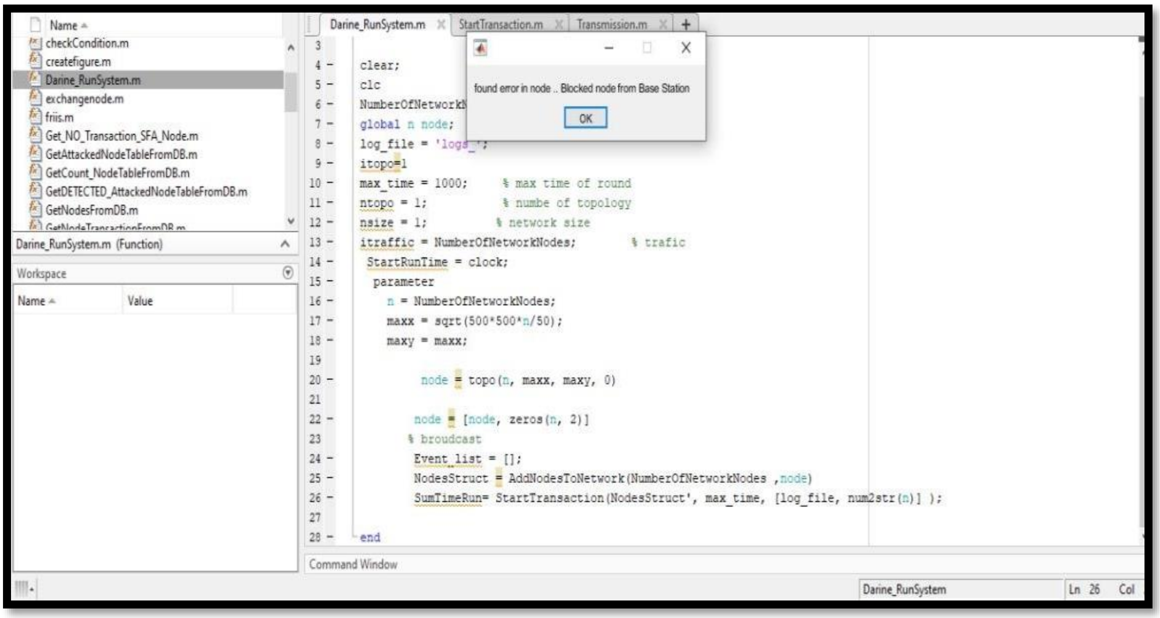
Notes: In the previous Case, the system doesn't detect the

Appendix B: Screen shots from Our Simulation


Name
checkCondition.m
createfigure.m
Darine_RunSystem.m
exchangenode.m
friis.m
Get_NO_Transaction_SFA_Node.m
GetAttackedNodeTableFromDB.m
GetCount_NodeTableFromDB.m
GetDETECTED_AttackedNodeTableFromDB.m
GetNodesFromDB.m
GetNodeTransactionFromDB.m
Darine_RunSystem.m (Function)
Workspace
Name
Value
Darine_RunSystem.m
StartTransaction.m
Transmission.m
GetAttackedNodeTableFromDB.m
Command Window
OK

Found Attacked Node

```

clear;
clc
NumberOfNetworkNodes=
global n node;
log_file = 'logs_';
itopo=1
max_time = 1000;      % max time of round
ntopo = 1;            % numbe of topology
nsize = 1;           % network size
itraffic = NumberOfNetworkNodes;        % trafic
 StartRunTime = clock;
  parameter
    n = NumberOfNetworkNodes;
    maxx = sqrt(500*500*n/50);
    maxy = maxx;

         node = topo(n, maxx, maxy, 0)

        node = [node, zeros(n, 2)]
       % broudcast
        Event_list = [];
        NodesStruct = AddNodesToNetwork(NumberOfNetworkNodes ,node)
        SumTimeRun= StartTransaction(NodesStruct', max_time, [log_file, num2str(n)] );

end
```



found error in node .. Blocked node from Base Station

```

    clear;
    clc
    NumberOfNetworkN
    global n node;
    log_file = 'logs_';
    itopo=1
    max_time = 1000;     % max time of round
    ntopo = 1;           % numbe of topology
    nsize = 1;          % network size
    itraffic = NumberOfNetworkNodes;        % trafic
     StartRunTime = clock;
      parameter
        n = NumberOfNetworkNodes;
        maxx = sqrt(500*500*n/50);
        maxy = maxx;

             node = topo(n, maxx, maxy, 0)

            node = [node, zeros(n, 2)]
           % broudcast
            Event_list = [];
            NodesStruct = AddNodesToNetwork(NumberOfNetworkNodes ,node)
            SumTimeRun= StartTransaction(NodesStruct', max_time, [log_file, num2str(n)] );

    end
```

Appendix C: Title here

Author’s Biographical Sketch

To insert Biographical Sketch text here, select this text and then either type the text you wish to use or paste text from another document, being sure to keep the text only and not the formatting from the previous document. To keep text only, choose Paste, and then from the drop-down box that will appear, choose the Keep Text Only option on the right, with the icon of a clipboard and the letter A.