People's democratic republic of Algeria

Ministry of higher education and scientific research

Mohamed kheider university of Biskra

Faculty of Exacts sciences and Sciences of nature and life

Computer science Department

Order $N°$: RTIC../M2/2020

Master thesis

presented for the academic masters degree in

Computer science

Option : Networking, Telecommunications and Information Technology

---

Intrusion Detection System For Wireless Body Area Networks WBAN

By:

Razika MEZGHICHE

Submitted on ../../2020, before the Jury :

.....	**XXX**	**President**
Boukhlouf Djemaa	**MCA**	**Supervisor**
.....	**XXX**	**Examinor**

Academic Year 2019/2020

Acknowlegments

First and foremost praise and thanks to Allah the Almighty , for his guiding and blessing throughout this work So I complete my thesis successfully .

I would like to express my gratitude to my thesis supervisor Mrs.Boukhlouf Djemaa for the continuous support during the work on this thesis, for her patience, motivation,enthusiasm, and immense knowledge. She consistently allowed this paper to be my ownwork, but guided me in the right direction whenever she thought I needed it.

I would also like to thank the committee members who were more than generous with their expertise and precious time. And also like to acknowledge all of the teachers of Mohamed Khider University for the guidance and effort over the years.

Finally, my thanks go to all the people who have supported me to complete the research work directly or indirectly.

Dedication

To the one and only , who never left me alone, who always guide me when I get lost , who gave me the strength to complete this work Allah the almighty , all praises to him .

To my parents ***Fatima*** *and* ***Abu-Bakr*** *they were the reason why I am doing all this .To my sisters :* ***Karima*** *,* ***Hamida*** *,* ***Sara*** *and* ***Sana*** *. To my brothers :* ***Abdullah****,* ***Miloud*** *and* ***Ayoub****. To my elder sister and my second mother who never forget me in her prayers* ***Louisa*** *and her husband* ***Omar*** *and their children : the elder twins* ***Abdelmouhaimen and Hadil*** *, the unique* ***Firas*** *and the little twins* ***Anes and Adem*** *.*

To the source of innocence ***my students*** *at* ***Allaoua Ahmed primary School*** *.*

To everyone helped me in order to accomplish this work especially ***Abir****. To all the friends I met in Biskra University.*

Razika

Abstract

Wireless Body Area Network WBAN consists of mini wearable or implantable biosensors capable of collecting as well as analyzing human physiological information, this makes it one of the most common technologies used in monitoring human body activities , An EEG is a part of WBAN which is responsible of recording the brain waves. The security is a great issue in such critical networks, in this work we propose an Intrusion Detection System based on Adhoc On demand Distance Vector AODV routing protocol, this IDS is designed against Black hole in EEG network .The proposed work gave very good results in term of Packet Delivery Ratio and Throughput , to evaluate the solution we used network simulator version 2 NS-2.35 .

Key words : WBAN ,EEG ,IDS, AODV, Black hole , PDR, Throughput .

الملخص

تتكون شبكة الجسم اللاسلكية WBAN من أجهزة استشعار حيوية صغيرة قابلة للارتداء أو قابلة للزرع قادرة على جمع وتحليل المعلومات الفسيولوجية البشرية ، وهذا يجعلها واحدة من أكثر التقنيات شيوعًا في مراقبة أنشطة جسم الإنسان ، تخطيط كهرباء الدماغ أو ما يسمى EEG هو جزء من شبكة الجسم اللاسلكية المسؤول عن تسجيل موجات المخ . يمثل الأمان مشكلة كبيرة في مثل هذه الشبكات الحساسة، في هذا العمل نقترح نظام اكتشاف التسلل IDS استنادًا إلى بروتوكول توجيه AODV ، تم تصميم IDS هذا ضد هجوم الثقب الأسود في شبكة EEG .أعطى الحل المقترح نتائج جيدة جدًا فيما يخص نسبة تسليم الحزم والإنتاجية ، لتقييم الحل استخدمنا محاكي الشبكات الإصدار 2 NS-2.35 .

الكلمات المفتاحية : WBAN ,EEG ,IDS, AODV, Black hole , PDR, Throughput

Contents

List of Figures

List of Tables

List of Abreviations

WBAN	Wireless Body Area Network
WSN	Wireless Sensor Network
IDS	Intrusion Detection System
EEG	Electroencephalogram
AODV	Adhoc On demand Distance Vector
RREQ	Route Request Message
RREP	Route Reply Message
RERR	Route Error Message
NS-2	Network Simulator version 2
PDR	Packet Delivery Ratio
OS	Operating System
DoS	Denial of Service attack
MAC	Media Access Control
BS	Base Station
RF	Radio Frequency
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
IEEE	Institute of Electrical and Electronics Engineers

General Introduction

The rapid evolution of microelectronics and wireless technologies have led to the creation of small devices, Electronic systems with a very low cost (limited resources), capable of collecting and to process information in an autonomous and flexible manner. These devices can be inter-connected and deployed on a large scale, giving rise to to a new type of network called Wireless Sensor Network (WSN). The development of WSN was originally motivated by military applications. Nevertheless, their remarkable performance in terms of reliability and low cost have allowed their use to proliferate in the field of civil applications. (environmental monitoring, industry, home automation, and health ...), among other,wireless sensor networks are designed to operate in groups and cooperating in order to transmit the data collected to a central point called base station or sink.In this work , we are interested in WSNs for medical applications. .

Nodes deployed on the patient's body or in the patient's environment, is a medical sensor node. Together they form a network of wireless medical sensors capable of monitoring the patient's health status by collecting physiological information and then communicating this information to a remote medical team.

One of the concerns of recent decades has been the continuing increase in the population of elderly or dependent people. Hence the need to provide quality care to such a rapidly growing population while reducing health care costs. So the implementation of systems allows to reduce patient hospitalization costs and to minimize the time of presence of the medical staff is a real challenge.

In this context, a number of researches are being conducted on the use of medical wireless sensor networks or WBAN (Wireless Body Area Network), to facilitate and improve the quality of medical care and monitoring at distance. These networks are

characterized by the mobility of their sensor nodes, their ease of deployment and self-organization.

WBANs are used to monitor certain vital signs such as the temperature, blood pressure or heart rate, brain waves etc. to better track patients in real time and respond to emergencies as soon as possible. Based on wireless technologies. The communication mode between the sensors and the treatment unit (sink) raise new challenges in terms of security, data protection against anomalies and attacks.

WBANs are vulnerable to different types of attacks and anomalies. Among these attacks and anomalies are those aimed at availability and the integrity of the system and therefore may indirectly influence the integrity dangerously such as the quality of care and the lives of patients, and other which are aimed at the confidentiality of the system and therefore may have an influence on the confidentiality of medical data. Vulnerability affects two parties of the system architecture. The first one represents the possible anomalies in the sensor nodes and possible attacks on the sensor network and on the wireless communication medium between these sensors and the medical the collection node, while the second, are the possible attacks on the high speed communications between the WBAN system and the medical server.

In this thesis we are going to focus on securing one of the most critical parts in WBAN which is Electroencephalogram EEG that is responsible for recordings the human brain activity against the Black hole attack , the implementation of the proposed solution is done by Network Simulator version -2- NS2.

Thesis Organisation

This thesis will structured as following:

- **First Chapter:** In this chapter we will explain in details the Wireless Body Area Networks including their topologies,technologies,Sensors and Operating Systems.
- **Second Chapter :** This chapter will cover the WBAN security requirements and the threat Models and the Intrusion detection System and its components and classification.

- **Third Chapter :** this chapter will contains the conception of our solution ,we will introduce in details the proposed solution using a flow chart for better understanding.

- **Fourth Chapter :** this chapter will be the experimental study of our proposed solution it will contain the all the simulation we made and their evaluation.

Chapter 1

Wireless Body Area Networks

1.1 Introduction

Since their inception, wireless communication networks have success within the scientific and industrial communities. Due to its various advantages, this technology has been able to establish itself as a key player in today's network architectures. The wireless medium offers indeed unique properties, which can be summed up in three points: ease of deployment, the ubiquity of information and the reduced cost of installation. As the wireless paradigm has evolved, the wireless paradigm has seen the emergence of various derivative architectures, such as: cellular networks, wireless local area networks and others. Over the last decade, a new architecture has emerged: wireless sensor networks (WSN).

1.2 Wireless Sensor Networks

Wireless sensor networks consist of individual sensor nodes, also called motes, deployed in a given area that cooperatively collect and carry data to a main entity in order to monitor physical or environmental conditions. The main entity, also denoted as base station or sink, can be connected to an infrastructure or to the Internet through a gateway, which allows remote users to access the collected data . [1]

WSN have a wide range of applications such as the environment, trade or

medicine, and that's what we're interested in, a WSN in the medical field is known as WBAN.

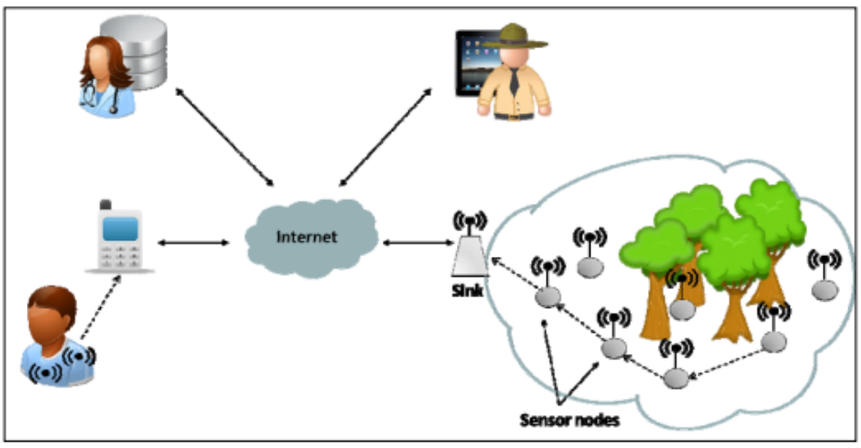

Figure 1.1: Wireless sensor networks [1]

1.3 Wireless body Area Networks (WBAN)

Wireless Body Area Network (WBAN) is a network consists of several small devices either wearable or implanted into the human body. The devices communicate wirelessly through using a certain wireless communication technology such as Bluetooth, ZigBee, UWB, etc. Some of these devices have sensing capability, and they are commonly referred to as WBAN sensor nodes[2] [3], So they can sense and monitor a different biologic characteristics, such as temperature, heart rate, blood pressure,electrocardiogram (ECG) , electroencephalogram (EEG) , also Storing the processed data, and transmit through the wireless network to a central processing device known as Personal Server (also called "body gateway" or "sink node"). Finally, personal servers forward relevant data to the cloud for further feature mining and long-term healthcare monitoring. [4][5]

As we can see on the figure below the WBAN sensors are connecting to the WBAN Coordinator or the Sink node which will connect to cell phone (Local server) that sends the data through GSM or any other public network to Healthcare Provider generally it's a Hospital .

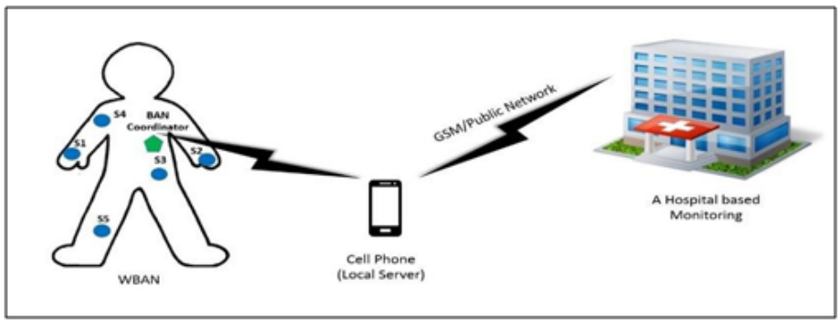

Figure 1.2: Wireless Body Area networks [6]

1.4 Communication Architecture in Wireless Body Area Network

Communication in WBAN can differ depending on the tier we are communicating in. Figure 1.3 illustrates a general architecture of a WBAN (Wireless Body Area Network) for medical monitoring, where several types of sensors send their measured data to a server through a wireless connection. Then, this data is transmitted (via the internet for example). to the medical team to obtain a real-time diagnosis or at a medical data to record them, or to corresponding equipment which issues an emergency alert.

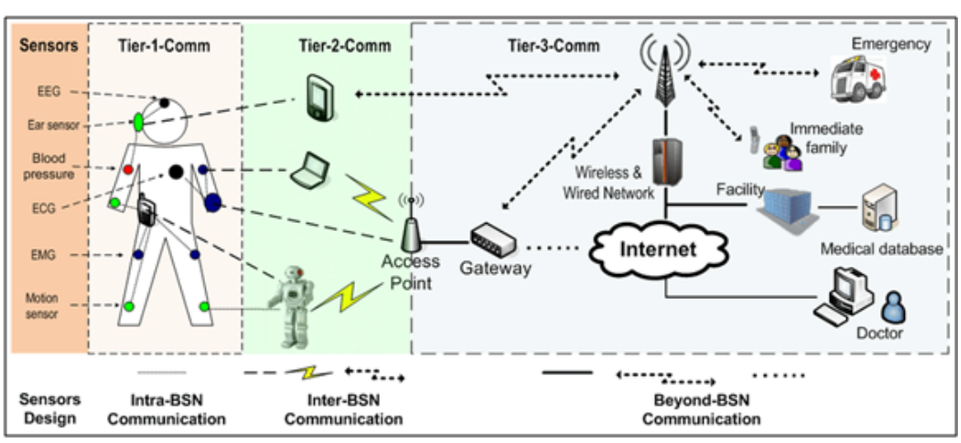

Figure 1.3: WBAN communications Architecture [7]

There are three types of communications in WBAN : «Intra-BAN» Communications, «Inter-BAN» Communications and «Beyond-BAN» Communications . [7]

1.4.1 «Intra-BAN» Communications

Intra-BAN concerns communications that take place around the human body. This type of communications consists of communications between the different body sensors as well as communications between the body sensors and the sink node .

1.4.2 «Inter-BAN» Communications

Inter-BAN are the Communications between the sink node and different Access points, The AP can be deployed as a part of the infrastructure, or strategically placed in dynamic environment for handling emergency situation . As with the terminology of "inter-BSN", the functionality of this type of communication (as shown in Figure 1.3) is used to interconnect BSNs with various networks that are easy to access in daily life, such as internet and cellular networks.

1.4.3 «Beyond-BAN» Communications

This type consists of communications between the access point and the team in medical center, for example in a hospital, via the Internet or a cellular network. «Beyond-BAN» Communications which helps to enhance the application and coverage range of E-healthcare system a step further by enabling authorized healthcare personnel (e.g., doctor or patient's immediate family) to remotely access a patient's medical information by means of cellular network or the Internet.

1.5 WBAN technologies

The medium used by medical wireless sensor networks is the radio waves Some of the major radio standards that have been used for Medical applications are the following [8]

1.5.1 The Standard IEEE 802.15.1 /Bluetooth

Initially, the Bluetooth standard was proposed to transmit voice and data over Bluetooth data, it had the prior objective of enabling communications on short distances with limited communication speed have caught the attention of sensors developers.

1.5.2 Bluetooth Low Energy /BLE

A derived option of the Bluetooth standard is the Bluetooth Low Energy (BLE), which was introduced as a more suitable choice for WBAN applications where less power consumption is possible using low duty cycle operation. Bluetooth LE was designed to wirelessly connect small devices to mobile terminals.

1.5.3 The Standard IEEE 802.15.4 / ZIGBEE

It is designed to be used in very low power communications and for short distances. This technology is used in wireless sensor networks. Compared to Bluetooth, this technology provides low latency.

A physical layer " DSSS: Direct Sequence Spread Spectrum" allows nodes to switch to sleep mode without losing the synchronization. Through the sleep mode, ZigBee enabled devices are capable of being operational for several years before their batteries need to be replaced. [8]

1.5.4 The Standard IEEE 802.11x / WIFI

IEEE 802.11 is a set of standards for wireless local area network (WLAN). Based on the IEEE 802.11 standards, Wi-Fi allows users to surf the Internet at broadband speeds when connected to an access point (AP) or in ad hoc mode.

1.5.5 The Standard IEEE 802.15.6

This standard is a step forward in wearable wireless sensor networks as it is designed specifically for use with a wide range of data rates, less energy consumption, low range, ample number of nodes (256) per body area network and different node priorities according to the application requirements. The channel access is handled using CSMA/CA or slotted Aloha access procedure. It provides flexibility in security features, since it defines three security schemes. [8]

IEEE 802.15.6 is the first WBAN standard that serves various medical and non medical applications and supports communications inside and around the human body. IEEE 802.15.6 standard uses different frequency bands for data transmission including: The Narrowband (NB) which includes the 400, 800, 900 MHz and the 2.3 and 2.4 GHz bands; the Ultra Wideband (UWB) 4, which uses the 3.111.2 GHz; and the Human Body Communication (HBC) which uses the frequencies within the range of 1050 MHz.[8]

1.6 Wireless body Area Network Topologies

There are several topologies can be implemented according to the needs of the network As shown in Figure 1.4.

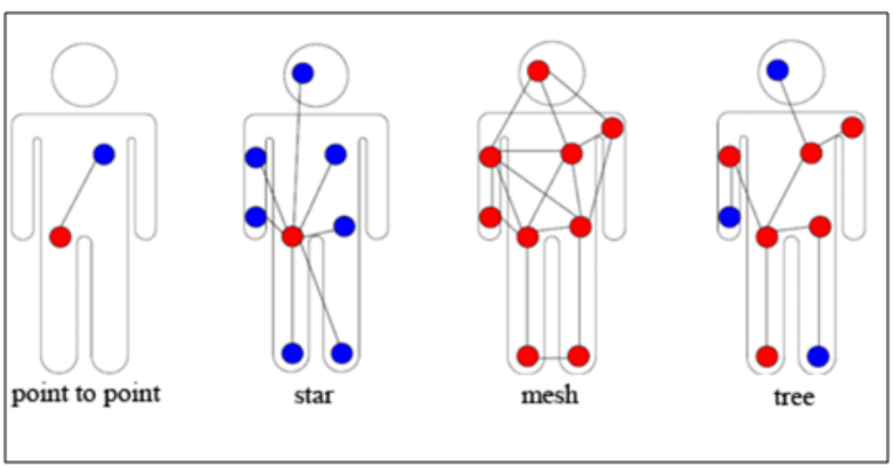

Figure 1.4: WBAN Network Topology

We will describe the deployment of point-to-point, star, mesh and tree WBAN networks

1.6.1 Point to Point Topology

This is the simplest topology in networks. This topology is designed to to a single link, for example between a data collector and a node sensor. The main advantage of this topology is the simplicity that allows often using a simple protocol, low latency and high throughput. Disadvantages include its limited functionality and its low coverage.

1.6.2 Star Topology

A topology in which all nodes are connected via a central node is a star topology. These nodes can only send or receive a message to or from a single central node. This topology has advantages that can be summarized by the simplicity, low power consumption of the nodes and lower latency of the communication between the nodes and the central node. On the other hand, its disadvantage is the vulnerability of the central node.

1.6.3 Mesh Topology

Mesh topology is a topology with complete connectivity between nodes also known as “multi-hop communication”, any node can exchange with any other node in the network if it is within transmission range. The advantage of using the mesh topology is that the network-wide scalability with redundancy and tolerance and a good coverage.

On the other hand, the disadvantages of this topology are the high energy consumption induced by the communication and the latency created by the passage of messages through the multi-skips several nodes before arriving at the destination node.

1.6.4 Tree Topology

A tree topology contains a top with a branch structure below. The connections between the nodes are structured hierarchically, which means that each node can be a son to a node and a father at a lower level node. It has a good fault tolerance, good coverage, high bandwidth and low latency. But still, father nodes can consume a lot of energy.

1.7 WBAN sensor nodes

1.7.1 Medical sensor

In this section, we describe several types of medical sensors which are commercially available [9][10][12] Examples of these medical sensors with their flow requirements (showing the impact on their flow rate and energy consumption) are presented in Figure 1.5 and Figure 1.6

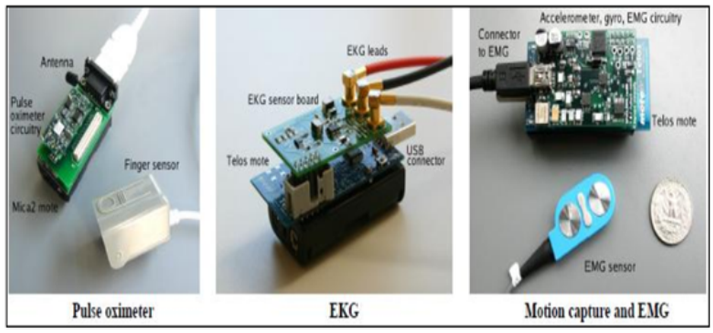

Figure 1.5: Some Medical Sensors[12]

1.7.1.1 Accelerometer and Gyroscope

The accelerometer is used to recognize and monitor the body posture (sitting, standing, walking and running, etc). This monitoring is essential for many applications, including health care. The posture monitoring system is based on 3 triaxial accelerometers that are placed at strategic points on the human body

1.7.1.2 Blood Glucose Sensor

It is used to measure the concentration of glucose in the blood. Traditionally Glucose measurements are performed by pricking a finger and extracting a drop of blood. A glucometer is used to analyze the blood sample and give a digital display of the glucose levels.

1.7.1.3 Blood pressure sensor

The blood pressure sensor is a sensor designed to measure systolic pressures and diastolic of human blood, using the oscillometric technique.

1.7.1.4 CO2 gas detector

It measures the level of carbon dioxide gas to monitor changes in the level of CO2, as well as to monitor oxygen concentration during human respiration .

1.7.1.5 EEG Sensor

Electroencephalography (EEG) is a method of brain exploration that measures the electrical activity of the brain through electrodes placed on the scalp. It is often represented in the form of a plot called an electroencephalogram. The EEG is an examination which provides information on the neurophysiological activity of the brain over time and in particular of the cerebral cortex, either for diagnostic purposes in neurology or for research in cognitive neuroscience. [13][14]

1.7.1.6 ECG Sensor

Electrocardiography is a method that measures the electrical signals produced by the heart. It is used to evaluate cardiac activity (heart rate, interval between two heartbeats, etc) by intercepting electrical activity from the heart muscle. Electrocardiography (ECG) is a graphical representation of the electrical potential that controls the muscular activity of the heart. This potential is collected by electrodes at the skin

surface. It can highlight various cardiac abnormalities and has an important place in cardiology diagnostic tests. [12]

1.7.1.7 EMG Sensor

The electromyogram is an examination that records the electrical activity of a muscle or a nerve. The EMG sensor measures the electrical signals produced by the muscles during contraction or during rest. It can detect nerve damage peripheral and muscle damage.

1.7.1.8 Pulse Oximetry (SpO2) sensor

Pulse oxymetry or oxygen saturation is a method of measuring the saturation in hemoglobin oxygen to the blood capillaries. We're talking about pulsed saturation in oxygen: SpO2. A small clip with a sensor is attached to the person's finger. The sensor sends a light signal that passes through the skin. Depending on the absorption of the light by oxygenated hemoglobin and total hemoglobin in arterial blood, the measurement is expressed as the ratio of oxygenated hemoglobin to total hemoglobin. [12]

1.7.1.9 Temperature and humidity sensors

The temperature sensor is used to measure the temperature of the human body and/or of the environment surrounding the patient. The humidity sensor is used to measure the humidity of the environment surrounding the patient. An alarm signal may be issued if a number of changes are measured. [12]

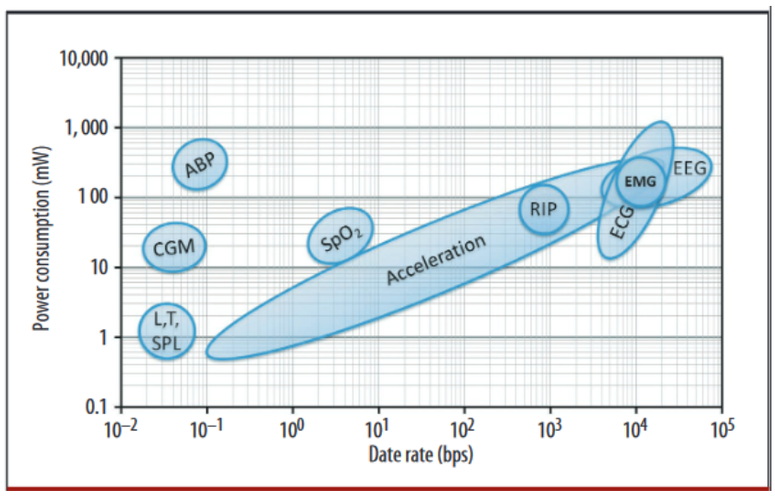

Figure 1.6: Energy consumption Vs data Rate for some Medical sensors[11]

1.7.2 Sensors Operating systems

Operating systems for wireless sensor networks are specific computer interfaces for the operation of sensors in networks. The role of the operating system for a networked sensor is to be the interface between the hardware resources and distributed applications. It must provide a variety of services basic systems such as resource allocation management on the peripherals of the various materials and the management and planning of tasks. The purpose of the operating system is to facilitate the programming of applications, but also to optimize the use of the resources. Over the years, we have seen various OSes emerging in the sensor network community . The most prestigious works include TinyOS , Contiki, MANTIS OS, LiteOS, RETOS, Nano-RK . In our work we present TinyOS , Contiki and LiteOS .

1.7.2.1 TinyOS

TinyOS is an open source operating system for wireless sensor networks that Developed in the computer lab at the University of California, Berkeley, and has been one of the first operating systems designed for miniature sensor networks. At Indeed, TinyOS is the most widespread OS for wireless sensor networks. It is capable of integration very quickly innovations in relation to the progress of applications and networks themselves while minimizing the size of the source code due to problems with

the inherent memory requirements in sensor networks.[16]

1.7.2.2 Contiki

The Contiki operating system is an open source operating system for networked embedded systems in general, and wireless sensor nodes in particular. It is developed by a team of developers from the industry and academia. The Contiki project is lead by Adam Dunkels. [16]

The hybrid architecture of the Contiki kernel allows two modes of operation, either multitasking or based on the events. Contiki is an operating system designed to take as little space as possible, with a small memory footprint. To achieve this, the code is written in C language.[16]

A system using Contiki contains processes, which can be applications or services, i.e. a process that offers functionality to one or more applications. The communication between process is done by sending events.[16]

The Contiki kernel remains, natively, a event-driven operating system. To get multitasking mode, a library must be installed. The functions associated with this library do not directly access all wireless sensor resources. They must, in some cases, call upon the part of the kernel dedicated to the management of events. This two-tiered structure results in a degradation system performance when multitasking is enabled.[16]

1.7.2.3 LiteOS

LiteOS developed in the University of Illinois at Urbana Champaign, is designed to provide a traditional Unix-like environment for programming WSN applications. It includes: a hierarchical file system and a wireless shell interface for user interaction using UNIX-like commands; kernel support for dynamic loading and native execution of multithreaded applications; and online debugging, dynamic memory, and file system assisted communication stacks. LiteOS also supports software updates through a separation between the kernel and user applications, which are bridged through a suite of system calls.[16]

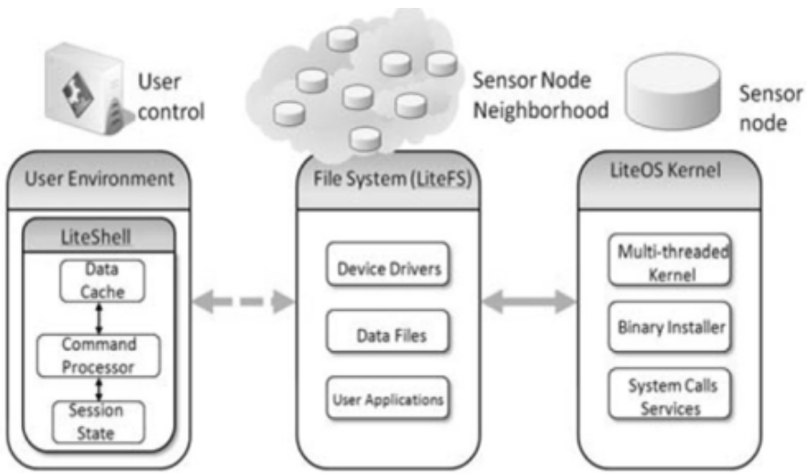

Figure 1.7: liteOS Architecture [16]

1.8 Conclusion

WBANs have greatly improved the medical sector by giving real-time monitoring of patients by the medical team, allowing for immediate intervention in case of need, this chapter covered most aspects related to WBAN including definitions and WBAN topologies and WBAN common medical sensors and their operating systems .

In the following chapter, we will discuss attacks and threats can compromise the WBAN network.

Chapter 2

Security and Intrusion Detection

2.1 Introduction

wireless body networks WBAN have many potential applications. In many scenarios, these networks are vulnerable to numerous attacks. due to the deployment in an open environment and their limited resources. These applications often require a high level of security. However, on the part of their characteristics (lack of infrastructure, energy constraints, topology, etc.). dynamic, large number of sensors, limited physical security, capacity reduced nodes,...), the securing of sensor networks is at the source, today, of many scientific and technical challenges. In order to face to these attacks protection systems exist. Intrusion detection can be considered as a complementary action to the implementation of the security mechanisms

In this chapter we will present WBAN network requirement and a different types of attacks that may compromise its security , also the Intrusion Detection Systems IDS.

2.2 Security requirements in WBANs

WBANs need to have all essential security methods which help to prevent, detect, and respond to different security attacks immediately. This section presents major

security requirements those are important in order to maintain network reliability and secure infrastructure-less environment. They are mainly :

2.2.1 Authentication

As we know in WBANs, an adversary can easily inject malicious information. So when data arrives at the receiver end, it is important for it to know exactly which node sent the data? Therefore, there should be some mechanism that authenticates the message and for this particular purpose, communication networks use Message Authentication Code (MAC).[17][18]

2.2.2 Integrity

Integrity is maintaining data consistency and it is equally important as authentication. It is vital to detect the adversary that has altered or changed the messages otherwise this adversary can cause catastrophes in these networks. Fortunately; data integrity can be achieved with authentication without any extra mechanisms required. [17][18]

2.2.3 Confidentiality

Data confidentiality is about protecting information from disclosure to unauthorized persons and can easily be Achieved through encryption. The confidentiality of data is usually compromised by attacks on privacy. [17][18]

2.2.4 Availability

There must be mechanisms to ensure that network services are always available. In particular, in ad-hoc, we need appropriate security methods to ensure the availability of the service at all times; otherwise their performance and service availability could be easily compromised. Suppose that a signal interference Attacking the physical layers and the MAC could dangerously impede communication or even

collapse.all physical channels. A malicious device can also interrupt routing services, which can cause the network partition.[17][18]

2.2.5 Freshness

Freshness ensures that the data is recent and not reproduced by an opponent. There are two types of freshness; weak freshness and strong freshness. Low freshness allows partial ordering of messages, but there is no information about the delay, while a strong freshness makes it possible to order all messages and estimate the delay. Strong Freshness is useful for time synchronization in a network. Since sensor networks are vulnerable to the response attacks, so at least a low level of freshness is required.[17][18]

2.2.6 Non-Repudiation

guarantees that senders and recipients can never refuse to send and receive the data, or the information they sent and received.[17][18]

2.2.7 Secure Localization

Many WBAN services require a correct estimation of the location of the network node. Lack of an intelligent tracking system Allows an attacker to transmit false data about the location of the node by reporting an erroneous signal.[17][18]

2.2.8 Anonymity

In this case, anonymity means that the attacker cannot know exactly what the conversation was about. i.e. two conversations from the same patient or two different patients. This means that anonymity hides the source of the data and may allow high level of confidentiality. [17][18]

2.3 Threat Models

The goal of an attacker, either he's insider or outsider, is to directly change user data, or try and gain access to its privacy. What makes it even easier for him is that the incontrovertible fact that most protocols for wireless sensor networks aren't designed up-to-date security threats in mind. As a consequence, deployments of sensor networks rarely include security protection mechanisms and small, or zero effort is sometimes required from the side of the attacker to perform the attack.

2.3.1 physical layer attacks

2.3.1.1 Jamming

Jamming It is a sort of attack which the attacker sends out signals (e.g., employing a specialized waveform generator) that interfere with the radio frequencies being employed by the WBAN A jamming source is additionally powerful enough to disrupt the full network. on action nodes unable to transmit data along the channel. jamming scenario where a jammer or the attacker interferes with communications associated with all nodes within a specific radius, r, of the jammer, as shown in the figure below. [23] [24] [26] [27]

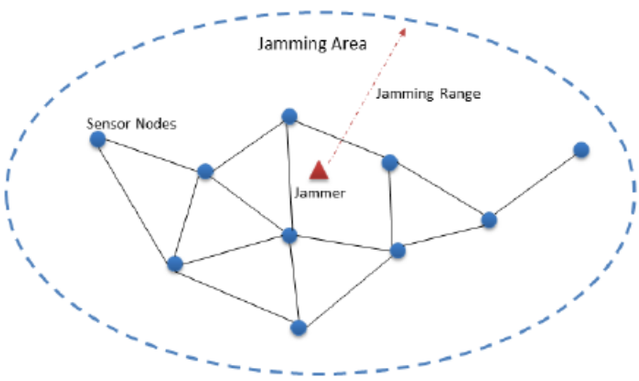

Figure 2.1: Jamming attak [29]

2.3.1.2 Tempering

Given physical access to a WBAN node, the attacker could temper with the node inseveral ways, which include compromising data stored on the nodes (e.g., encryption keys), tamper with its circuitry, modify the program codes or perhaps replace it with a malicious sensor. [23] [24] [26] [27]

2.3.1.3 Eavesdropping and traffic analysis

Since WBAN signals are broadcast within the air, an adversary within the range of the signals could hear the transactions occurring within the wireless channel with the help of antennas that cost as little as $20, From data captured during eavesdropping, the adversary could directly extract the message content, or do traffic analysis to make inferences like the placement of the bottom station, which could successively inform more targeted attacks. Often, for an adversary to effectively render the network useless, the attacker can simply disable the bottom Station (BS). A rate monitoring attack simply makes use of the concept that nodes closest to the bottom station tend to forward more packets than those farther faraway from the bottom station.

An attacker need only monitor which nodes are sending packets and follow those nodes that are sending the foremost packets. during a time correlation attack, an adversary simply generates events and monitors to whom a node sends its packets. [25] [26] [27]

2.3.2 Link Layer attacks

2.3.2.1 collision

When two nodes attempts to send a packet on the identical frequency simultaneously the collision occurs , when these packets touch one another this can cause a checksum mismatch , then all the packets during this case are often discarded as invalid , an attacker can launch his attacks in this manner in order to degrade the

network performance. A defense against such sorts of collisions is that the use of error-correcting codes. [21]

2.3.2.2 Sybil attack

It is an attack where one node presents quite one identity in a very network. The Sybil attack is effective against routing algorithms, data aggregation, voting, fair resource allocation, and foiling misbehavior detection. irrespective of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. as an example, during a sensor network voting scheme, the Sybil attack might utilize multiple identities to get additional "votes". Similarly, to attack the routing protocol, the Sybil attack would depend on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through one malicious node. [23][24][26][27]

2.3.2.3 MAC protocol violations

MAC protocols generally help make sure that the sensors within the network efficiently use the shared communication. When a given node violates the MAC protocol mechanisms (e.g., by sending data during a interval when another node is meant to be sending), packet collisions occur. reckoning on the extent of the violation, the collisions could result into a good range of issues, including corruption of the information in the packets, unfair bandwidth usage, and within the worst case, total denial of service if the malicious sender continuously occupies the channel and (or) the attacked nodes continually try to retransmit corrupted packets. [26]

2.3.3 Network layer attacks

2.3.3.1 Hello Flood Attack

In Hello flood attack, the attacker broadcasts hello message with a really powerful radio transmission to dupe them into classifying the attacking node as their

neighbor, the attacker node falsely broadcasts a shorter route to the bottom station, and every one the nodes which received the HELLO packets, try to send data via this route. Potentially resulting into failed data transfers, retransmissions and channel congestion (since the offending node is truly not in radio range with many of the nodes. The affected nodes waste their energy by sending messages to the node which is out of their radio range. [19][23][24][26]

2.3.3.2 Selective Forwarding

In a multi-hop network sort of a WBAN, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such how that it selectively forwards some messages and drops others. The impact becomes worse when these malicious nodes are at closer to the bottom station. Then many sensor nodes route messages through these malicious nodes. As a consequence of this attack, a WBAN may give wrong observation about the environment. [23][24]

2.3.3.3 Sinkhole Attack

The sinkhole attack is severe attack, within which the adversary manipulates routing information to lure an outsized number of nodes into routing their traffic via a node controlled by the adversary. The attacker prevents the bottom station from obtaining the whole and therefore the correct sensing data from the nodes within the WBAN network .As shown in figure 2.2 . as an example, an attacker may claim that it's a high-quality or low-latency route to the bottom station for attracting the neighbor nodes to send data through it. When the routes bear the attacker, the info packets could also be tampered or the attacker can start attacks to influence the network ash shown in the figure 2.2 . [19]

2.3.3.4 Wormhole attack

The wormhole attack could be a severe threat against packet routing in sensor networks that's particularly challenging to detect and stop. This attack is centered

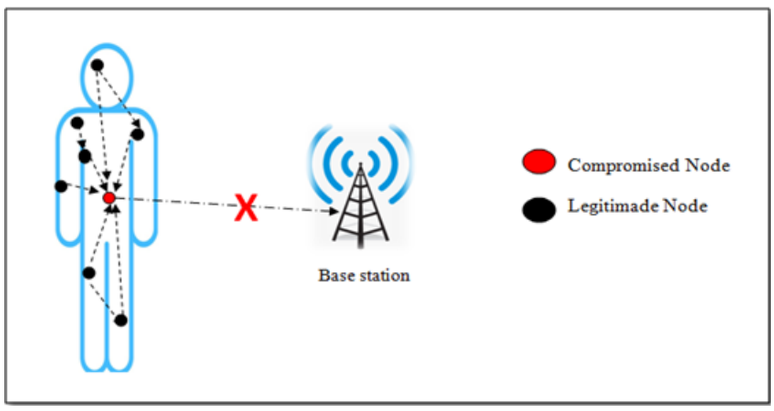

Figure 2.2: The model of sinkhole attack

on route manipulations designed to form two distant malicious nodes appear to the opposite nodes to be much closer to every apart from is truly the case by relaying packets along an out-of-bound channel available only to the attacker.[22][29][31]

2.3.4 Transport layer attacks

2.3.4.1 Desynchrosization attack

In desynchronization attack, an attacker repeatedly forges messages to 1 or both end points of a lively reference to fake sequence number or control flag. Thus attackers desynchronize the tip points in order that sensor nodes retransmit messages and waste their energy.[23][24][26]

2.3.5 Application Layer attacks

2.3.5.1 Attacks on Data Aggregation Process

Data aggregation, a service provided by the appliance layer, ensures meaningful combination of information from the sensors to enable the accurate estimation of the sensed environment.

Possible attacks on this service include the malicious modification of information before it's forwarded to the base station and also the complete disruption of the service. With the bottom station having wrong information about the sensed environment, the network could then be compromised in several other ways if the base station triggers

actions supported the incorrect information fed to that.[25] [26]

2.4 Intrusion Detection in WBAN

Although Security mechanisms are capable of ensuring security at some level they are not able to eliminate most of the security attacks. An IDS is one possible solution to address big range of security attacks in WBANs. In a network or a system, any type of unauthorized or unapproved activities are called intrusions. An Intrusion Detection System (IDS) might be collection of the tools, methods, and resources to assist identify, assess, and report intrusions. Intrusion detection is often one a part of an overall protection system that's installed around a system or device. Intrusion is additionally defined as: "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" and intrusion prevention techniques (such as encryption, authentication, access control, secure routing, etc.) are presented because the first line of defense against intrusions. [31]

However, as in any type of security system, intrusions can't be totally prevented. The intrusion and compromise of a node ends up in confidential information like security keys being revealed to the intruders. This ends up in the failure of the preventive security mechanism. Therefore, IDSs are designed to reveal intrusions, before they'll disclose the secured system resources. IDSs are always considered as a second wall of defense from the safety point of view. [35]

2.4.1 IDS components

There are two main components of IDS, features extraction and modeling algorithm. Features extraction defines measured attributes that are linked to the IDS functionalities. Modeling algorithm is that the main component; the accuracy and also the efficiency of detecting and responding to intrusions depend upon the modeling algorithm. IDS may have components that depend upon the network characteristics and possible intrusions. Most of IDS have six common components: [32]

2.4.1.1 Monitoring component

this is often used for local activity monitoring or for monitoring neighbor sensor nodes. This component mostly monitors internal activities, traffic patterns, and resource utilization.

2.4.1.2 Analysis component

It contains all records of normal and abnormal behaviors for all nodes within the network.

2.4.1.3 Detection component

this can be the most component that's built upon the modeling algorithm. It works after analyzing network behaviors. Decisions are made to work out whether such behaviors are malicious or not.

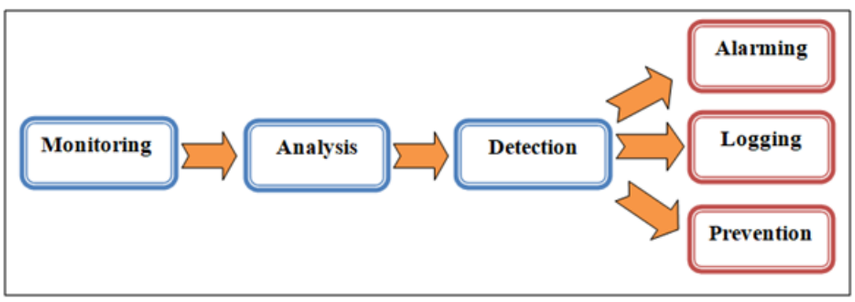

Figure 2.3: IDS components according to [32]

According to [32] the other three components of IDS consist of actions that can be taken, either one, two, or all of them :

- **Logging:** storing each packet in a log file so that security administrator can use it for later analysis.
- **Alarming:** a responding generating component in case of detection of an intrusion. The response may trigger an alarm to announce the misbehaving node(s).
- **Prevention:** an advanced step that can be added to IDS to enable it to take

an action to prevent dealing with an attack once detected. This can be done, for example, by excluding harmful nodes from the network.

2.4.2 Categories of IDS

2.4.2.1 Signature-Based Intrusion Detection Systems

Signature based IDS, also called rule-based IDS, has predefined rules of various security attacks. When the network's behavior shows any deviation from the predefined rules, it's classified as an attack. Signature-based IDSs are compatible for known intrusions. The advantage of this kind of detection is that it can accurately and efficiently detect known attacks; hence they need a coffee false positive rate. The disadvantage is that if the attack could be a new kind (that wasn't profiled before), then it would not be able to detect it.[23][30][32]

2.4.2.2 Anomaly based Intrusion Detection Systems

In this form of intrusion detection. Normal operations of the members are profiled and a specific amount of deviation from the traditional behavior is flagged as an anomaly. The disadvantage of this detection type is that the traditional profiles must be updated periodically, since the network behavior may change rapidly. this could increase the load on the resource constrained sensor nodes. [23][30][32]

2.4.2.3 Hybrid Intrusion Detection Systems

Hybrid IDSs are a combination of both anomaly-based and signature-based approaches. Hybrid mechanisms usually contain two detection modules, the first module is responsible of detecting common attacks using signatures, and the second module is responsible for detecting and learning normal and malicious patterns or monitor network behavior deviation from normal profile. Hybrid IDS are more accurate in terms of attack detection with less number of false positives. However, such mechanisms consume more energy and more resources. Hybrid IDSs are generally not recommended

for a resource constraint networks such as a WSN; however they are still an active research area. [29]

2.5 Conclusion

This chapter covered a lot of concepts related to security in WBAN including WBAN requirements and threat models classified according to the layer it compromised.also we had explain in details the Intrusion Detection System its components and its categories .

In the next chapter we will introduce in details our intrusion detection mechanism.

Chapter 3

Conception of Intrusion detection system in WBAN

3.1 Introduction

This chapter primarily reviews the available literature in the field of intrusion detection in Wireless body area network Accordingly, it will account for the definitions of black hole attack in EEG network (Electroencephalogram) with Ad-hoc on Demand Distance Vector (AODV) routing protocol. The first part of this chapter will be an overview on EEG (Electroencephalogram) and network AODV routing protocol. The second part of this chapter will present in detail the black hole attack. The third and the final part of this chapter describes the proposed solution of the black hole attack .

3.2 Electroencephalography EEG

3.2.1 what is an Electroencephalography (EEG) ?

Electroencephalography (EEG) is a tool for recording spontaneous electrical activity generated within the cerebral cortex using multiple electrodes placed on the scalp. EEG signal could be a reflection of electrical currents flowing within the extracellular space generated by the algebraic summation of excitatory and inhibitory

postsynaptic potentials occurring on many cortical neurons. The summated EPSP (Excitatory PostSynaptic Potentials) and IPSP (Inhibitory PostSynaptic Potentials) are then conducted through the skull and picked up by electrodes placed on the scalp. One estimate suggests that $6cm^2$ of cortical area must be synchronously activated for a possible to be recorded at the scalp. [33][34]

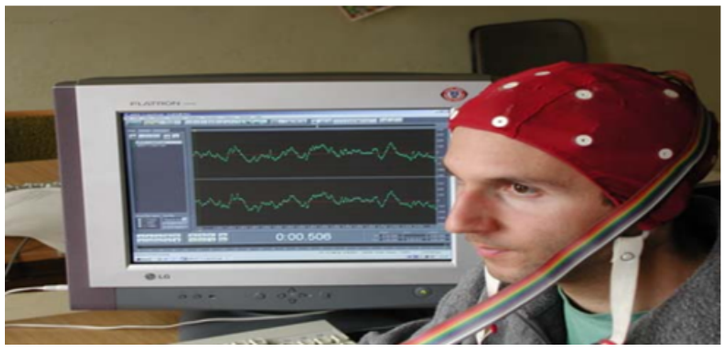

Figure 3.1: EEG Electrode cap [33]

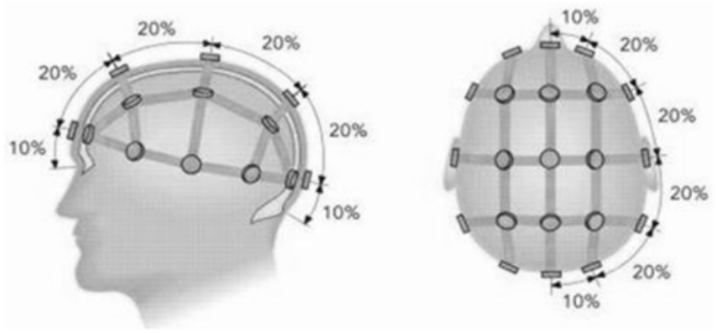

Figure 3.2: EEG Electrode placement [34]

3.2.2 Wireless Electroencephalogram EEG

Wireless EEG (electroencephalogram) is a new sensor technology that changes the way we interact with the world. Using EEG headphones, EEG sensors measure the electrical activity of the brain or brain waves. In early research, EEG tests were invasive and complex. They usually involved the use of needles and silver electrodes on the scalp, and had to be done in hospitals or research centers. [35]

Figure 3.3: Examples of some mobile EEG systems [35]

3.3 Ad-hoc on Demand Distance Vector Routing Protocol (AODV)

AODV is a reactive routing algorithm designed by Charles E. Perkins and Elizabeth M. Royer. It is suitable for highly dynamic topology networks and is based on the distance vector routing philosophy. Due to node mobility, network topology changes frequently which make the active route out of service and new route should be discovered. AODV uses a sequence number as route freshness indicator. [36]
Routes in AODV are discovered on demand. When a node needs a route to a destination, it broadcasts a route request RREQ within the network. Each neighboring node that receives the broadcasted packet must check the freshness of the routing information through sequence number to update its routing table. This request will be forwarded to either the destination node or a node with an active route to the destination. A destination will unicast a response packet RREP to the source trough the preceding node choosing the shortest path with a sequence number greater than or equal to that which was received in the RREQ. [36]

AODV employs control messages to discover a route to the destination node in the network. There are three kinds of control messages in AODV that are discussed as following:

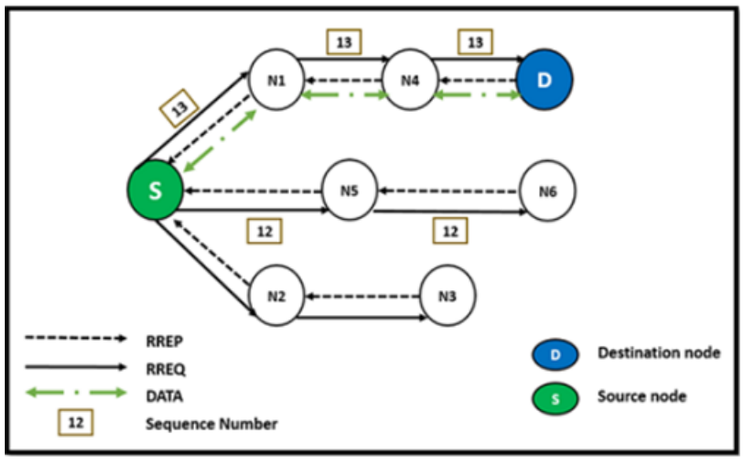

Figure 3.4: Process of AODV [36]

3.3.1 Route request message (RREQ)

When source node needs to communicate with another node in the network, it sends RREQ message. AODV broadcasts RREQ message.[37]

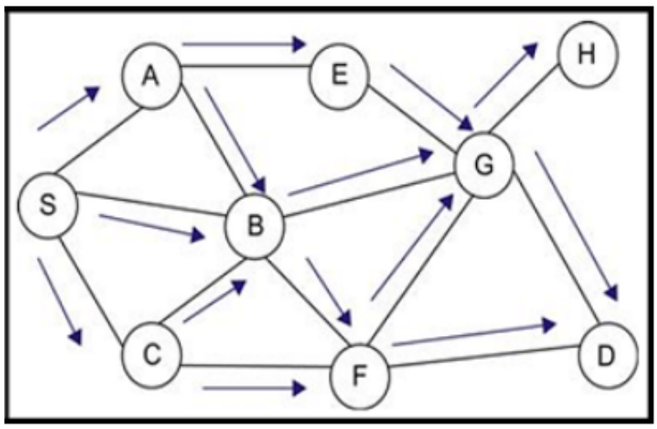

Figure 3.5: Flooding RREQ in AODV [37]

3.3.2 Route reply message (RREP)

A node that have a requested identity or any mediatory node that has a route to the requested node creates an RREP message and sends it back to the originator node.

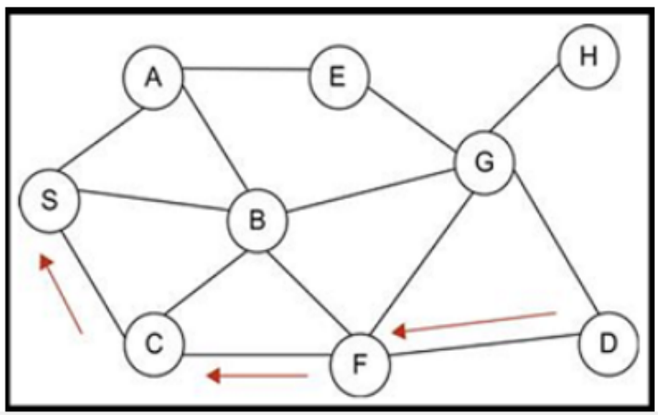

Figure 3.6: Route Reply in AODV [37]

3.3.3 Route error message (RERR)

During active routes, each node in the network keeps monitoring the link status to its neighbor's nodes. When the node discovers a link crack in an active route, RERR message is created by the node in order to inform other nodes that the link is down. [37]

3.4 Black hole attack

In black hole attack, a malicious node pretends to have a fresh enough route to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. [36]

We suppose that the node S wants to send data packets to node D, and M is a malicious node that does not have a valid a route to D. The node M responds directly to the RREQ sent to D, as if it has an active route to the destination using a false

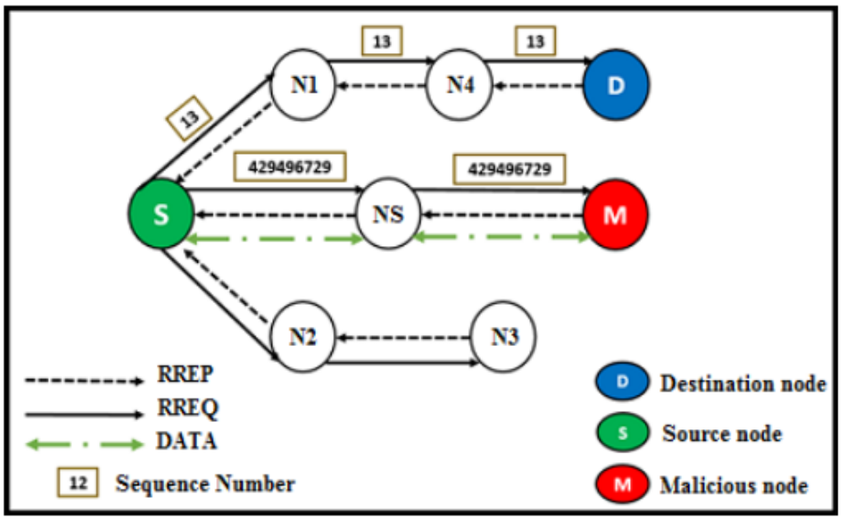

Figure 3.7: Black hole attack [36]

RREP packet. In this case, the node M practices a black hole attack in the network. The attacker node can easily ignore and reject any data traffic and conduct a crisis at the network.

3.5 Related Works

In [38] Malasri et al,proposed the elliptic-curve cryptography (ECC) algorithm to construct symmetric keys between sensor nodes and the base station. In [39], He et al. provided a lightweight system with hash-chain aided key updating mechanism, which was capable of countering powerful mobile attacks and had a high feasibility for real-time application. Given that the human body physiological state was quite random and time variant, relying on the physiological signals obtained from the patient, Wang et al. proposed a biometric encryption technique in order to achieve a mutual authentication, which derived a non-linkable session key between each biosensor and the sink node [40].

Some other mechanisms were also proposed. Specifically, in [41], Thamilarasu et al. presented a multi-objective genetic algorithm based intrusion detection system to provide optimal attack detection in WBAN, Salem et al. in [42] provided an anomaly detection algorithm to detect nodes' abnormal behaviors.

However, some of the previous mentioned mechanisms are not workable for resource-constrained nodes in WBANs. Biometric encryptions ignore the fact that these sensor nodes are generally single-function devices which can sense only one physiological parameter for every node.for example. moreover, some lightweight cryptography mechanism cannot resist against inside attacks like Black hole attack , So an Intrusion Detection System is necessary to detect and prevent such attacks .

3.6 Proposed Solution

In our study , we simulated Black Hole attack in Wireless Body Area Network Specifically In Electroencephalography Network "EEG " and evaluated its affects on the EEG Network Performance . We use Network Simulator Version 2.35(ns 2.35) as a tool for our simulation , we performed tests to evaluate and compare the network performance with and without black hole in the network. As expected, We measured both of Packet Delivery Ratio (PDR) and Throughput which deteriorated considerably in the presence of a black hole.

Also To reduce the adverse effects of the black hole node in the network using AODV as a routing protocol We proposed a solution based on ignoring the first established route. We implemented this solution also in ns-2 and evaluated the results as we did for the black hole implementation. The Main Steps of our proposed solution is described in the flowchart below :

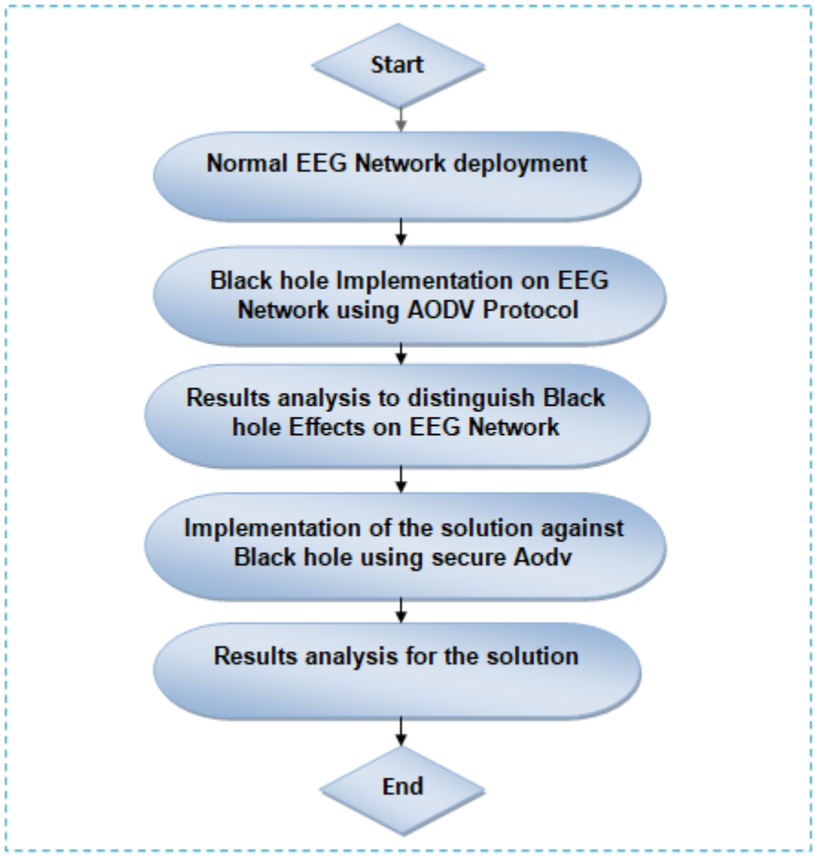

Figure 3.8: Flowchart of the proposed solution

3.7 Conclusion

In this chapter we explained in details many aspects related to EEG network and AODV routing protocol that we will use in our study .we also present the Black Hole attack in EEG network using AODV routing .Finally we demonstrate our proposed solution against this attack .

The next chapter will be an experimental study of the proposed solution presented in chapter 3 including the simulation and the evaluation of the metrics.

Chapter 4

Experimental Study and analysis of the results

4.1 Introduction

In this chapter we will discuss the Black hole effects on Electroencephalogram Network (EEG), a new routing protocol that drops all the packets is implemented in order to simulate the Black Hole attack .The first section of this chapter will focus on evaluating the Black hole attack effects on EEG network performance. The other section will be on the implementation of a new routing protocol that prevents the Black hole attack and helps to enhance the EEG network performance under the presence of Black hole attack.

4.2 The Simulation

4.2.1 Definition of a simulation

Simulation is the process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system. [43]

4.2.2 Simulation tool (NS2)

In this study, an event-driven network simulator tool known as NS2 (version 2.35) is used, it has been proved efficiently capable in the study of dynamic nature of communication networks. Furthermore, wired and wireless network-related protocol can be simulated using NS2. Practically, NS2 provides a way for users to specify network protocols in the field or wired and wireless network and also simulating their individual behaviors based on predefined parameters. [43]

The simulation is done to analyze the performance of Electroencephalogram Network without black hole attack and with black hole attack, in terms of below metrics:

- **Throughput**
- **Packet Delievery Ratio (PDR)**

NS is an event-driven network simulator program, developed at the University of California, Berkley. It includes several network objects such as protocols, applications, and traffic source behavior. The NS-2 at the simulation layer, interprets user simulation scripts by using OTcl (object-oriented tool command language) programming language. OTcl language is an object-oriented extension of the Tcl Language which is fully compatible with the C++ programming language. At the top layer, NS is an interpreter of users' Tcl scripts; both make use of C++ codes.[44]

The figure below demonstrates the basic architecture of ns2

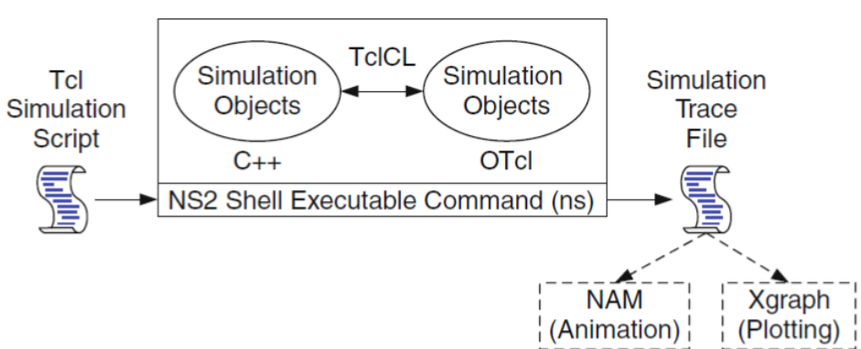

Figure 4.1: basic architecture of ns2 [44]

In this study, NS-2 version 2.35 of "all-in-one package" was installed in Ubuntu17.10 . The ".tcl" files was written in Sublime text editor and the results of the ".tr" file have been analyzed using "awk" commands in UNIX operating system. The implementation phase of the black hole behavior to the AODV protocol is written using C++.

4.3 Simulation of Normal EEG Network (without attack)

Firstly , in order to simulate a normal EEG network we have to create a topology similar to a real EEG , as shown in figure below :

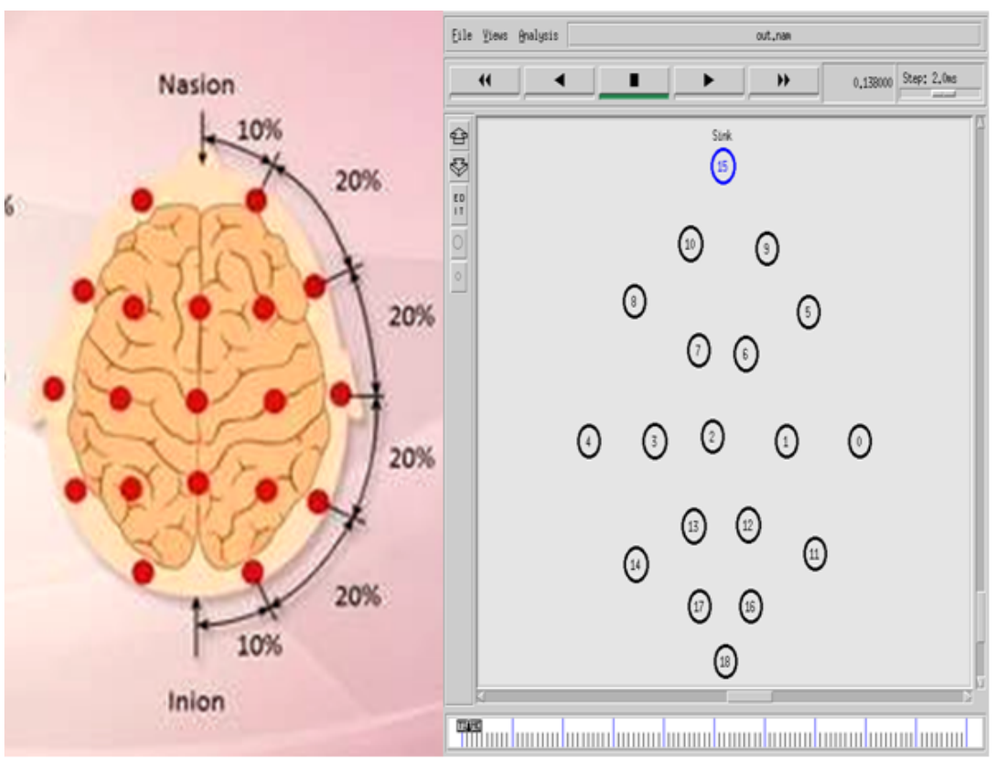

Figure 4.2: EEG Topology in NS2

In the topology above we have 19 nodes with one Sink node , the other simulation parameters of the Normal EEG Network are listed in the table below :

Parameters	Value
Simulator	Network Simulator (Version 2.35)
Total Nodes	20, 25 and 30
Simulation Area	1186x600
Radio Propagation Model	Propagation/Tworayground
MAC Protocol	Mac_802.11
Antenna	Antenna/Omni antenna
Routing Protocol	AODV
Traffic	FTP
Simulation Time	40s

Table 4.1: Normal EEG Simulation Parameters

We simulate an EEG with 20, 25 and 30 sensor nodes with 1 Sink node and 1 source node and 1 Destination node as shown in the figures below :

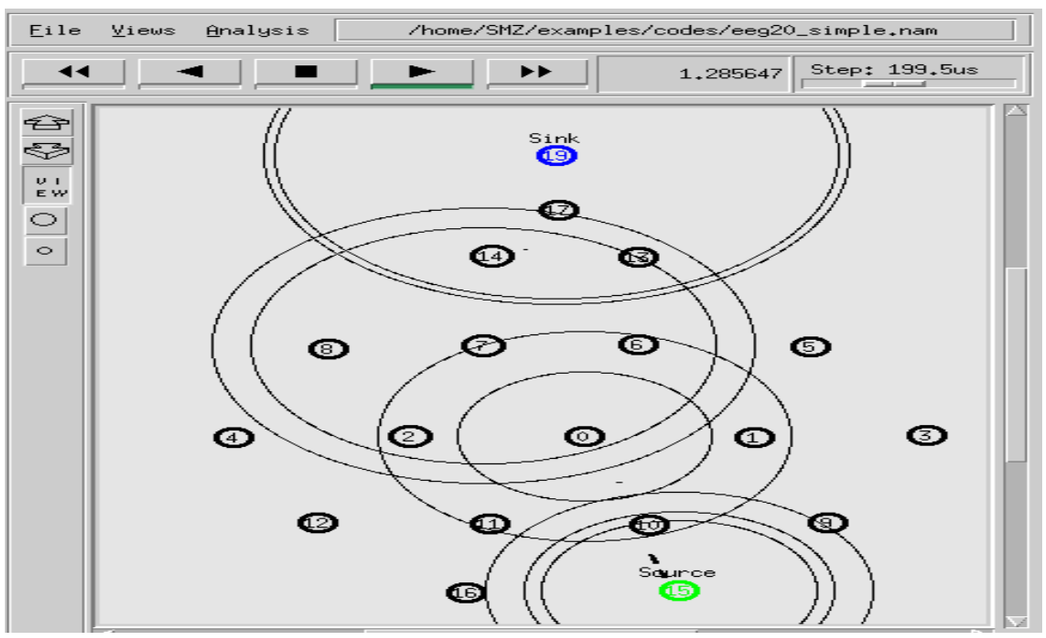

Figure 4.3: Normal EEG with 20 nodes

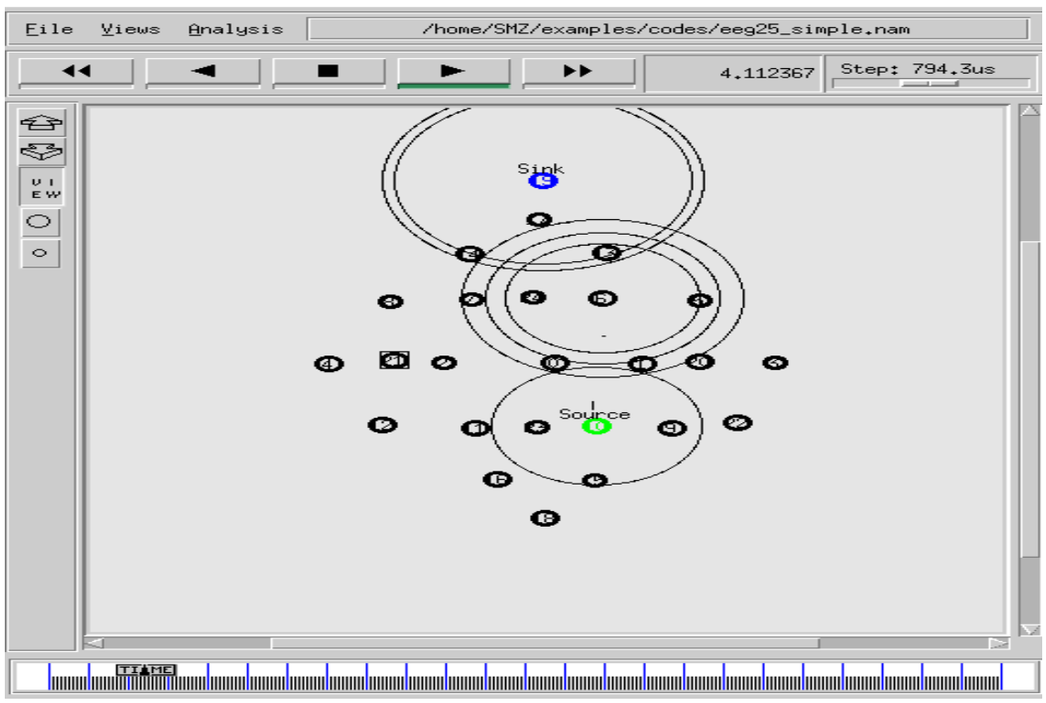

Figure 4.4: Normal EEG with 25 nodes

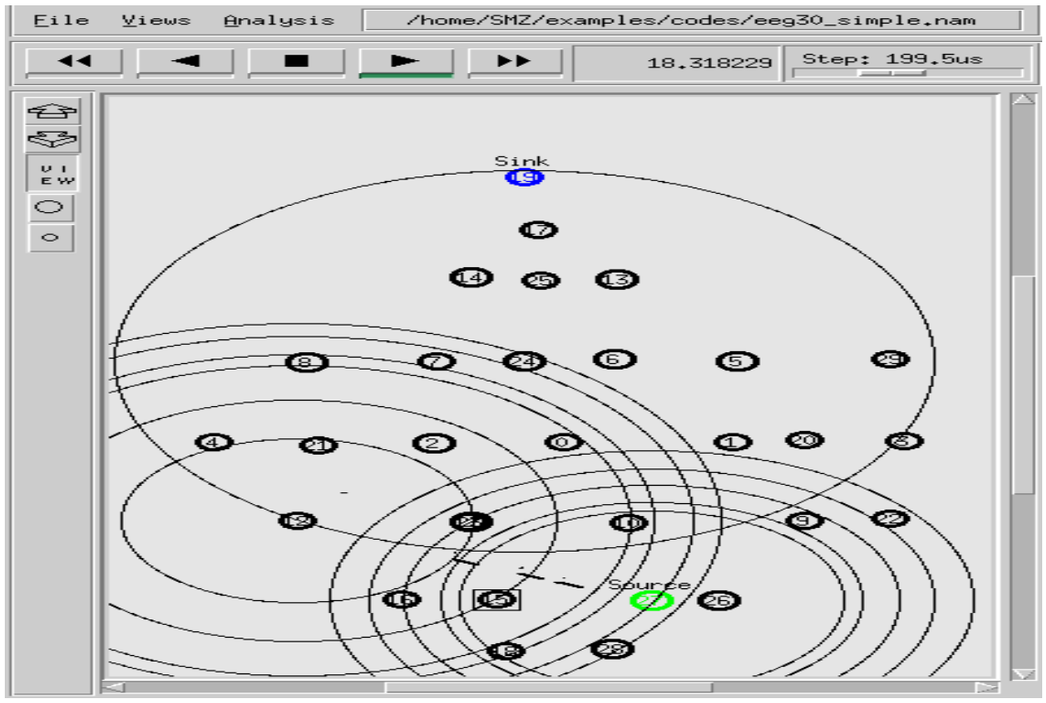

Figure 4.5: Normal EEG with 30 nodes

As we can see from the figures below the FTP traffic is transmitting correctly from the source to the Sink node.

4.3.1 Evaluation Metrics

At the end of each one of the simulation above we calculate the Packet Delivery Ratio using the next formula

$$PDR = Receivedpackets * 100/sentpackets$$

We also calculated the Throughput which is the amount of data effectively handover from source node to destination node within certain amount of time over communication channel , we measured both metrics using **.awk** script and we found the results below :

Number of sensor nodes	**20 nodes**	**25 nodes**	**30 nodes**
PDR %	99.10	99.37	99.10
Throughput [kbps]	227.56	340.23	227.63

Table 4.2: Measured metrics of Normal EEG

4.4 Simulation of EEG Network under Black hole attack

In this Scenario we add a one malicious node with Black hole attack implemented using AODV routing Protocol under the name Blackhole aodv , in order to create this attack in our Simulation we had to access to : ns-allinone2.35 system files to make the necessary modifications, some of these modifications are listed below :

The first modified file is `"\tcl\lib\ns-lib.tcl"`such that protocol agents are implemented as a procedure. In the case of the nodes using blackholeaodv protocol, this agent is scheduled at the beginning of the simulation and it is designated to the nodes that will use blackholeaodv protocol. The agent procedure for blackholeaodv is shown in the Figure below :

We also need to make some changes in Makefile in ns2.35 folder the changes are the following :

After all this modification , the blackhole attack is not yet implemented in blackholeaodv To do this we need to make the changes in blackholeaodv.cc , the main

```
    blackholeAODV {
        set ragent [$self create-blackholeaodv-agent $node]
    }

Simulator instproc create-blackholeaodv-agent { node } {
# Create blackholeAODV routing agent
set ragent [new Agent/blackholeAODV [$node node-addr]]
$self at 0.0 "$ragent start"
$node set ragent_ $ragent
return $ragent
}
```

Figure 4.6: modification made in ns-lib.tcl

```
blackholeaodv/blackholeaodv_logs.o blackholeaodv/blackholeaodv.o \
blackholeaodv/blackholeaodv_rtable.o blackholeaodv/blackholeaodv_rqueue.o \
```

Figure 4.7: modification made in Makefile.in

change will be on the recvAODV function in the case of blackholeaodv the node will ignore and drop all the packets as long as does not belong to it self , the Figure below contains the if else statement that allows the black hole node to accept or drop the packets.

```
//If this node is a destination
if ( (u_int32_t)ih->saddr() == index)
  forward((blackholeaodv_rt_entry*) 0, p, NO_DELAY);
else
// For blackhole attack in the EEG Network ,
//after taking the path over itself, misbehaving node drops all packets
 drop(p, DROP_RTR_ROUTE_LOOP);
```

Figure 4.8: packet drop in blackholeaodv.cc

In our case when the malicious node receives a RREQ (route request) it immediately replies with a false RREP (route reply) to the source node so it pretends that it has a fresh route to the destination , this RREP function is explained in the figure below :

After all the modifications above we need to configure the ns2 by running the following commands in the terminal.

```
    sendReply(rq->rq_src,           // IP Destination
              1,                    // Hop Count
              index,                // Dest IP Address
              4294967295,           // Highest Dest Sequence Num
              MY_ROUTE_TIMEOUT,     // Lifetime
              rq->rq_timestamp);    // timestamp

    Packet::free(p);
}
```

Figure 4.9: route reply in blackholeaodv.cc

./configure

Make clean

Make

4.4.1 Simulation and evaluation

In this case we create a scenario similar to previous scenario but here we add one black hole node , we maintain the same other parameters ,the figures below shows the EEG simulation under Black hole with 20,25 and 30 nodes :

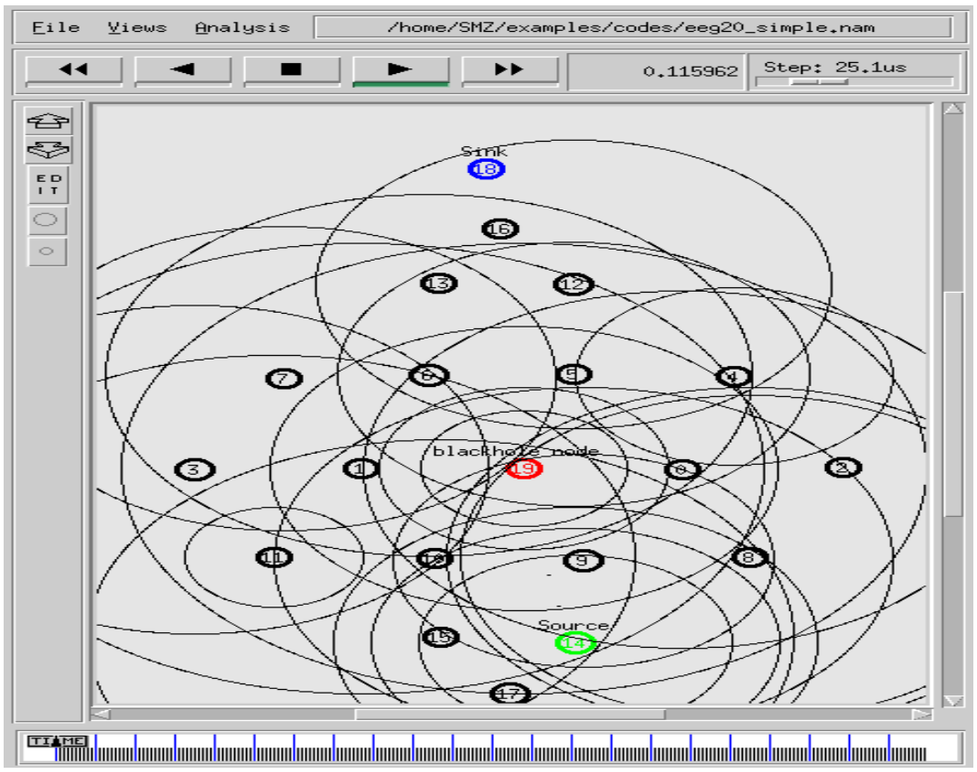

Figure 4.10: 20 nodes EEG under blackhole attack

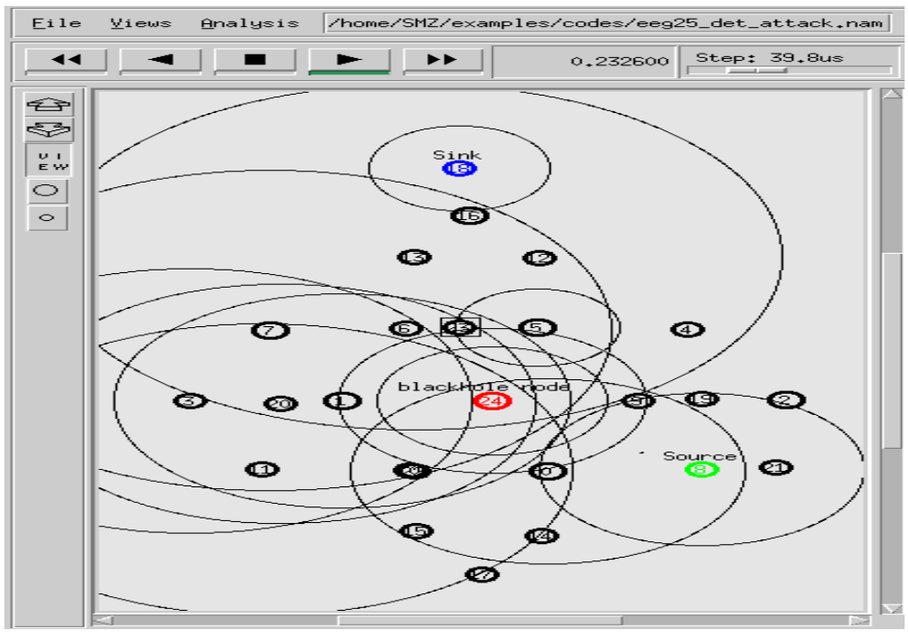

Figure 4.11: 25 nodes EEG under blackhole attack

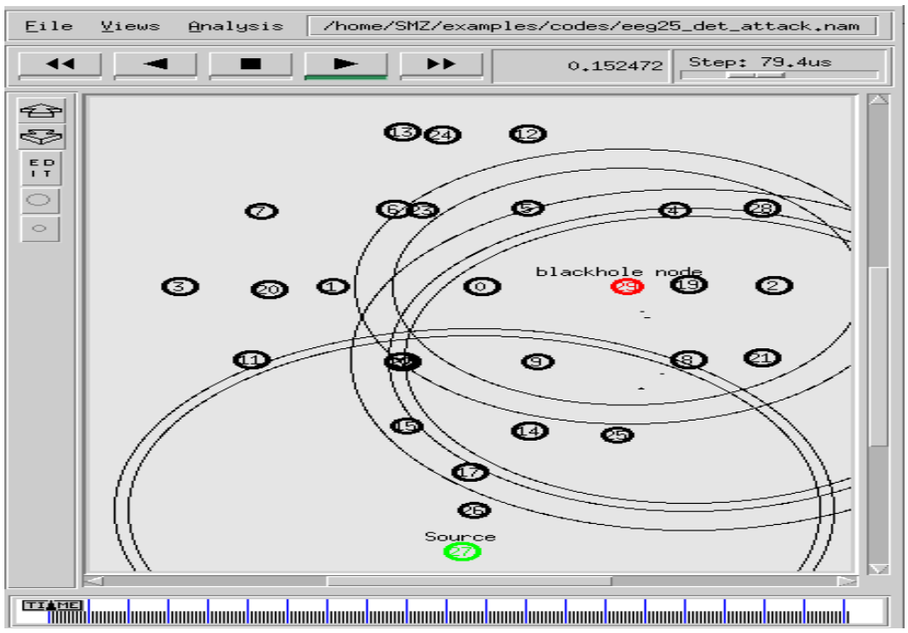

Figure 4.12: 30 nodes EEG under blackhole attack

As we can see from the Screenshots above all the malicious node is in the red color,it doesn't forward any packets from the source to the Sink node, and every time it drops the packets sent to it.

4.4.2 Measured metrics

As we did in the previous scenario ,at the end of each of these simulations we made some statistics on tracefile.tr using .awk script , and we got the results below :

Number of sensor nodes	20 nodes	25 nodes	30 nodes
PDR %	0.00	0.00	0.00
Throughput [kbps]	0.00	0.00	0.00

Table 4.3: Measured metrics of EEG under black hole

Inorder to compare the results we got from the two previous scenario (Normal EEG and EEG under attack), we created the graphs below :

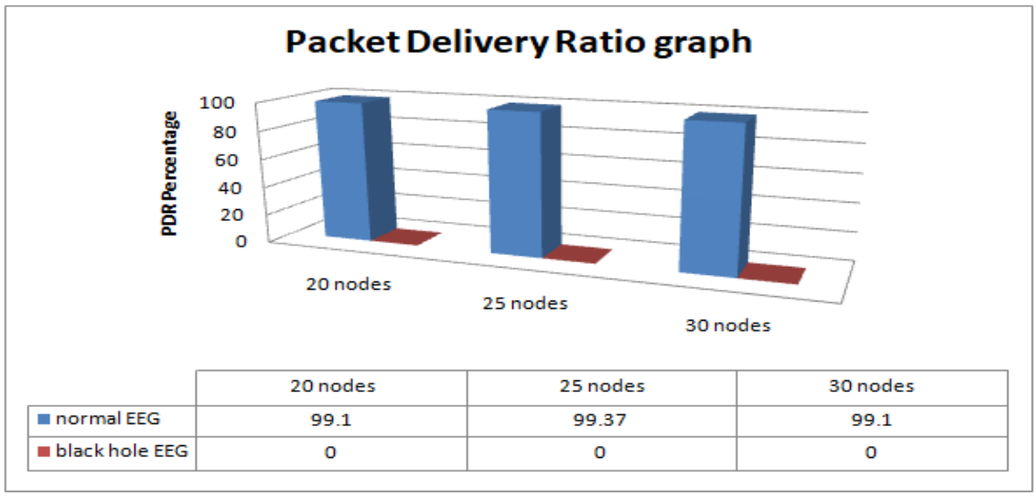

Figure 4.13: PDR comparison

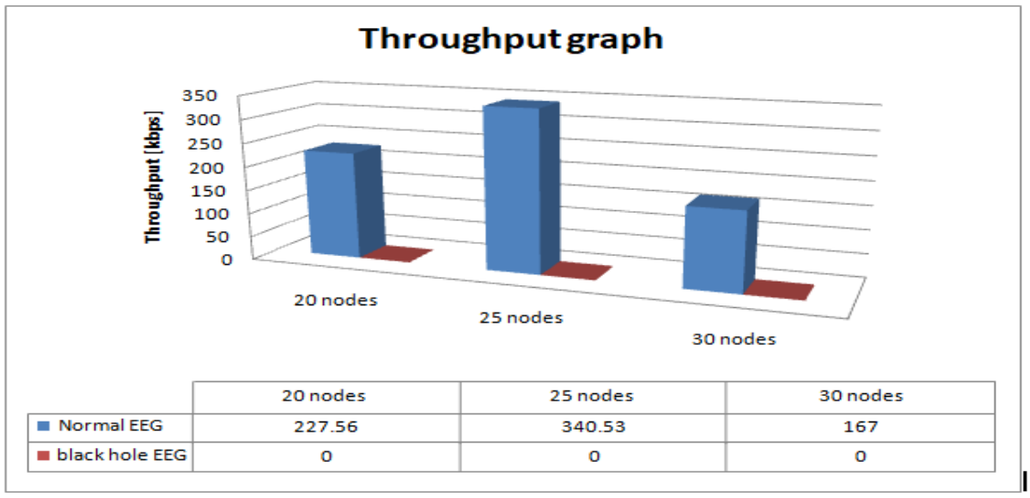

Figure 4.14: Throughput comparison

We observe that The EEG network performance metrics decrease to reach 0 in both of Packet reception ratio and Throughput which means that the black hole attack has a severe effect on the EEG network performance.

4.5 Solution of Black hole attack in EEG Network

4.5.1 Executing a New Routing Protocol IDSAODV to Simulate The Solution

To evaluate effects of the proposed solution, first, it needs to be implemented in NS-2. Therefore, should simulate the "AODV" protocol, changing it to "IDSAODV" as it did "blackholeAODV" before. To implement, the black hole the (recvRequest) function has been changed (the receive RREP) of the blackholeaodv.cc file but to implement the solution had to change the receive RREP function (recvReply) and create RREP caching mechanism to count the second RREP message.

In the "recvReply" function, first we control if the RREP message arrived for itself and if it did, function looks the RREP message up if it has already arrived. If it did not, it inserts the RREP message for its destination address and returns from the function. If the RREP message is cached before for the same destination address, normal RREP function is carried out. Afterwards, if the RREP message is not meant for itself the node forwards the message to its appropriate neighbor. The figure below shows how the RREP message function of the IDSAODV is carried out.

```
void
idsAODV::recvReply(Packet *p) {
//struct hdr_cmn *ch = HDR_CMN(p);
    struct hdr_ip *ih = HDR_IP(p);
    struct hdr_aodv_reply *rp = HDR_AODV_REPLY(p);
    idsaodv_rt_entry *rt;
    char suppress_reply = 0;
    double delay = 0.0;
    int count;

    idsBroadcastRREP *r = rrep_lookup(rp->rp_dst);

#ifdef DEBUG
    fprintf(stderr, "%d - %s: received a REPLY\n", index, __FUNCTION__);
#endif // DEBUG
    if (r == NULL) {
        count = 0;
        rrep_insert(rp->rp_dst);
    } else {
        r->count++;
        count = r->count;
    }
```

Figure 4.15: receive reply function in IDSaodv.cc

4.5.2 Evaluation of idsAODV routing Protocol

To evaluate the effect of idsAODV on the EEG network performance we maintain the previous simulations under the black hole attack but we just changed the line of the value of the routing on the head of the simulation file .tcl as the following :

```
#==================================
#     Simulation parameters setup
#==================================
set val(chan)   Channel/WirelessChannel    ;# channel type
set val(prop)   Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)  Phy/WirelessPhy            ;# network interface type
set val(mac)    Mac/802_11                 ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)     LL                         ;# link layer type
set val(ant)    Antenna/OmniAntenna        ;# antenna model
set val(ifqlen) 50                         ;# max packet in ifq
set val(nn)     20                         ;# number of mobilenodes
set val(rp)     idsAODV                    ;# routing protocol
set val(brp)    blackholeAODV              ;#here is malicious routing protocol
```

Figure 4.16: idsAODV declaration

The screenshots below show the simulation of an EEG network with the proposed solution using 20,25and 30 nodes respectively :

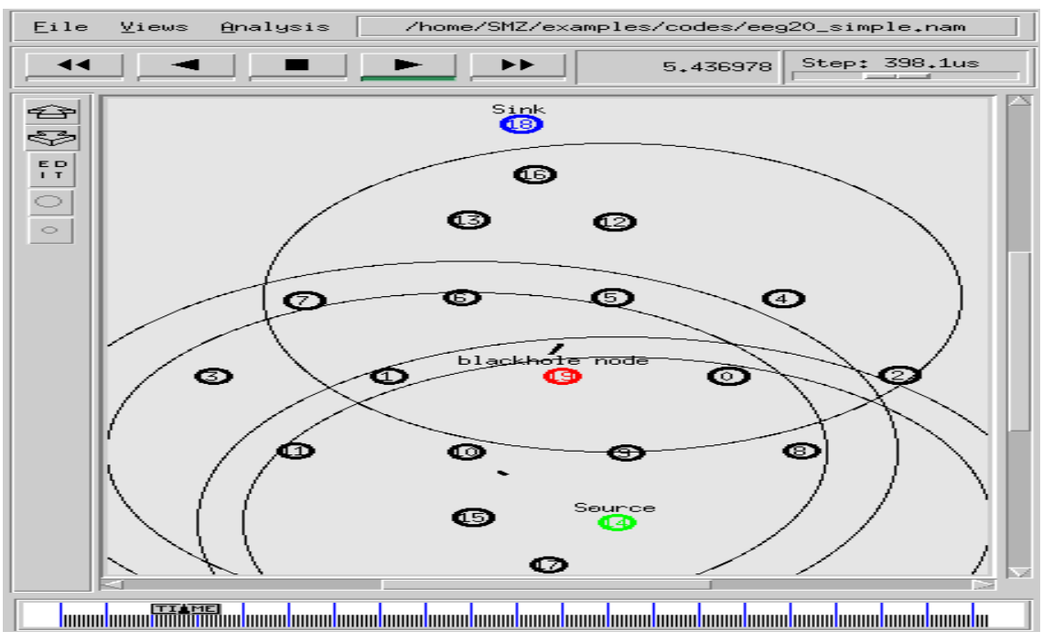

Figure 4.17: Source node prevents the black hole node

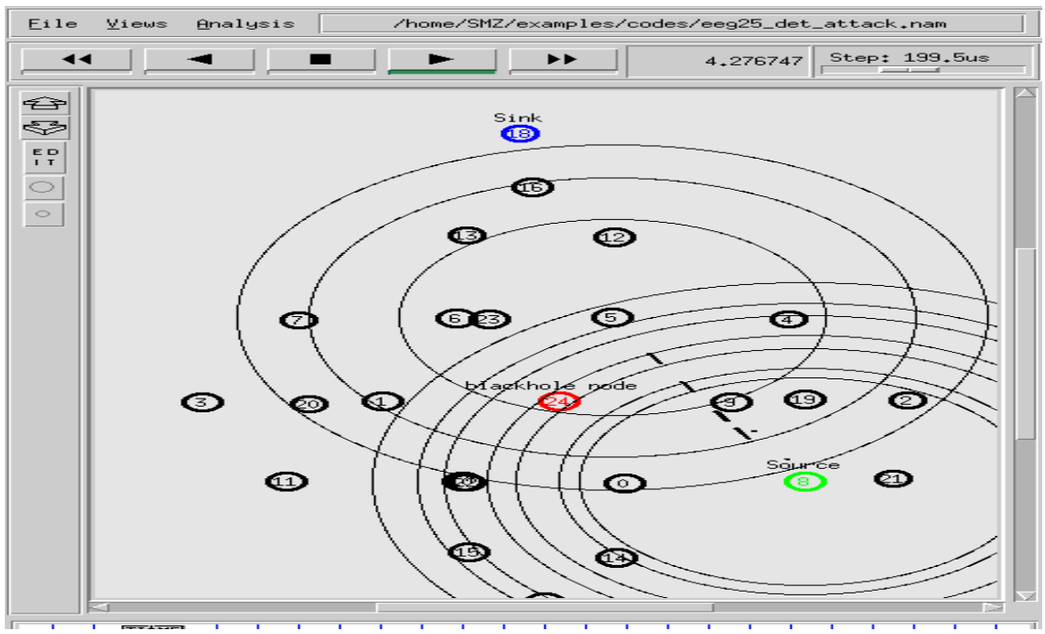

Figure 4.18: Source node prevents the black hole node

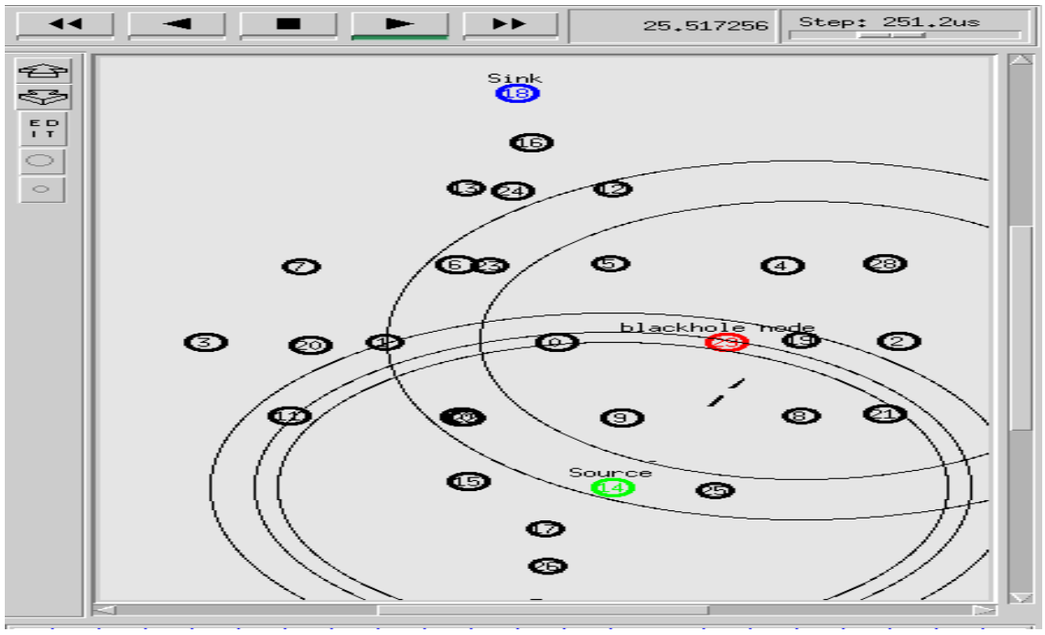

Figure 4.19: Source node prevents the black hole node

As we can see from the figures above the new routing protocol allows the source node to prevent the malicious node and chose another route to the Sink node .

Similarly to the previous examples, we calculated the metrics (PDR and Throughput) the results we got are shown in the next table :

Number of sensor nodes	20 nodes	25 nodes	30 nodes
PDR %	98.95	99.30	98.65
Throughput [kbps]	221.10	331.65	221.57

Table 4.4: Measured metrics of black hole EEG using our solution

4.6 Total comparison between all the simulations

in this section we going to make a comparison of packet Delivery Ratio PDR and throughput between the three previous scenarios we simulate (normal EEG , Black Hole EEG and Intrusion detection EEG) the following graphs demonstrate this comparison

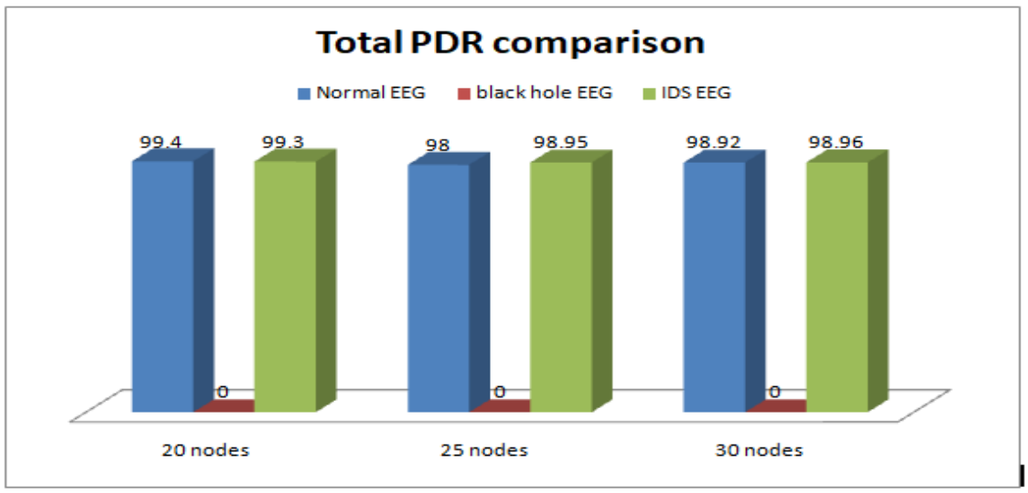

Figure 4.20: Total PDR comparison

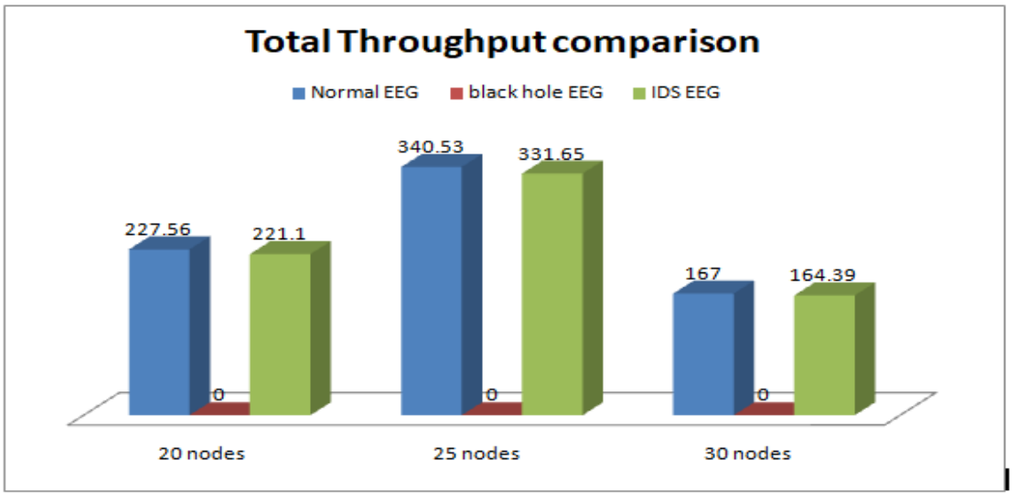

Figure 4.21: Total Throughput comparison

The graphs show that when using our solution under black hole attack the values

of the PDR and throughput increase to reach values near or even similar to a normal EEG .

4.7 Conclusion

In this chapter, at the first place we investigated the performance of an EEG network before black hole attack and after black hole attack. The results that we got after the simulation shows that the black hole attack works perfectly, we also examine the performance of the network under the black hole attack including the packet delivery ratio and throughput, at the second place we evaluate the proposed solution which shows that the our intrusion detection mechanism works correctly to detect and prevent the black hole in Electroencephalogram Network .

General Conclusion

In this study, we analyzed effect of the Black Hole in an ElectroEncephalogram Network. Using AODV protocol For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. We simulated three scenarios of EEG Network where each one has 20, 25 and 30 nodes that use AODV protocol and also simulated the same scenarios after introducing one Black Hole Node into the network. After that, we simulated IDSAODV solution with same scenarios to observe AODV behavior under this proposed solution. First, investigated effects of black hole attack on EEG network performance, which this attack increase number of drop packets and decrease packet delivery ratio.

After implementing IDSAODV on EEG network, both of throughput and packet delivery ratio improved. Other benefits of this solution are that the proposed solution requests minimum modification on AODV. It does not change packet format and can work together with AODV protocol.

Having simulated the Black Hole Attack, we saw that the packet loss is increased in the EEG network . In the last chapter, tables of simulation results show the difference between the number of packets Delivery Ration and throughput in the EEG network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall EEG network connectivity and the data loss could show the existence of the Black Hole Attack in the network.

We can understand from chapter 4, When we used IDSAODV protocol in the same EEG network,the PDR and Throughput increased as a normal EEG. These two results show that our solution reduces the Black Hole effects.

Bibliography

[1] Tifenn Rault. Energy-efficiency in wireless sensor networks. Université de Technologie de Compiègne, 2015. English. ffNNT .

[2] P. Bonato et al. IEEE EMBS Technical Committee on Wearable Biomedical Sensors and systems , Position paper. Proc. Int. Workshop on Wearable and Implantable Body Sensor networks (2006)

[3] Bestoon T. Hussain Jaff , Master thesis "A Wireless Body Area Network System for Monitoring Physical Activities and Health-Status via the Internet" University of Uppsala , published on : March ,2009

[4] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," IEEE Wireless Communications, vol. 24, no. 2, pp. 98–105, Apr. 2017

[5] Xuyang Hou et al , Article "A Sink Node Assisted Lightweight Intrusion Detection Mechanism for WBAN" Tsinghua University, Beijing, 100084, China, published on: May 2018.

[6] Adil sheraz et al , Article"Impact of Beacon Order and Superframe Order on IEEE 802.15.4 for Nodes Association in WBAN" University Peshawar, Pakistan, published on : January 2018

[7] Long Hu et al , Article "Integration of Wireless Body Area Networks (WBANs) and WAN, WiMAX and LTE " published May 31, 2013

[8] Rim Negra et al , Article “Wireless Body Area Networks: Applications and technologies” The Second International Workshop on Recent Advances on Machine-to-Machine Communications , King Saud University, Saudi Arabia, ,Elsevier , published2016.

[9] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao and Victor C. M. Leung, “Body Area Networks: A Survey”, Mob. Netw. Appl. Journal, April 2011

[10] Huasong Cao, Victor Leung, Cupid Chow and Henry Chan, “Enabling Technologies for Wireless Body Area Networks: A Survey and Outlook”, IEEE Communications Magazine, Volume 47, Issue 12, December 2009.

[11] Mark A. Hanson, Harry C. Powell Jr., Adam T. Barth, Kyle Ringgenberg, Benton H. Calhoun, James H. Aylor, John Lach, “Body Area Sensor Networks: Challenges and Opportunities”, IEEE Computer, January 2009

[12] Monal Shinde et al , Article “Overview of Different Types of Sensors Used in eHealth Environment” University of Mumbai , India , January,2014

[13] Ramani Kannan et al , Article ‘Smart Wearable EEG Sensor’ Published by Elsevier, 2017

[14] Fawzi Abdulla Alazraq, Mini Tutorial “introduction to EEG Sensor”, july 2017

[15] Nadine Boudargham at al , “Study on Medical Sensors” Faculty of Engineering Notre Dame University, Deir El Kamar, Lebanon , 18 January 2019.

[16] Thang Vu Chien et al , “A Comparative Study on Operating System for Wireless Sensor Networks” January 2011.

[17]] Munir Hussain, et al , A Survey on Authentication Techniques for Wireless Body Area Networks, Journal of Systems Architecture, 4 October 2019

[18] P Usha, N Priya , “Survey on Security Issuses in WBAN”, International Journal of Advanced Research in Computer Science and Software Engineering, January 2015

[19] Asimakopoulos, “Datasets for Intrusion Detection for Wireless Body Area Networks” Athens, February 2019

[20] G. Thamilarasu, “iDetect: An Intelligent Intrusion Detection System for Wireless Body Area Networks,” Int. J. Secur. Netw., vol. 11, no. 1/2, p. 82–93, March 2016

[21] Sagarika Karchowdhury, Mainak Sen, “Survey on Attacks on Wireless Body Area Network” Proceedings of International Conference on Computational Intelligence IoT , 2018

[22] J. Sen, Article: "Security in Wireless Sensor Networks", Department of Computer Science and Engineering, National Institute of Science and Technology, INDIA. Published in: 2010.

[23] . Rehana, Article: "Security of Wireless Sensor Network", Editor: TKK T-110.5190 Seminar on Internetworking, Published at: 2009 April 27.

[24] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones, "Security in Wireless Sensor Networks", Springer, In book: Handbook of Information and Communication Security, pp.513-552,Published at: January 2010.

[25] Selmic, Rastko R., Phoha, Vir V., Serwadda, Abdul, Book: "Wireless Sensor networks", DOI: 10.1007/978-3-319-46769-6, Publisher: Springer International Published Published in: 2016.

[26] Yang, Shuang-Hua, "Wireless Sensor networks", DOI: 10.1007/978-1-4471- 5505-8, Publisher: Springer-Verlag London, Published in: 2014

[27] M. Saraogi, Article: "Security In Wireless Sensor Net Works", Published in: 2014, Department of Computer Science University of Tennessee.

[28] Emre ÜNSAL, Yalçın ÇEBİ” DENIAL OF SERVICE ATTACKS IN WSN” Dokuz Eylül University, İzmir, Turkey, published at: Jan,2015

[29] N. A. Alrajeh, S. Khan, B. Shams, Article: "Intrusion Detection Systems in Wireless Sensor Networks", Publisher: International Jour-

nal of Distributed Sensor Networks (IJDSN), Article ID: 167575 URL: "http://dx.doi.org/10.1155/2013/167575", Published in: 2013

[30] A. Ghosal, S. Halder, Book: "Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches", DOI: 10.1007/978-3-642- 36169-210, Print ISBN: 978-3-642-36168-5, Online ISBN: 978-3-642-36169-2, Series ISSN: 1860-4862, Publisher: Springer Berlin Heidelberg, Copyright Holder: Springer-Verlag Berlin Heidelberg, Published in: 2013.

[31] I. Butun, S. D. Morgera, R. Sankar, Article: "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", Publisher: IEEE Communications Surveys and Tutorials VOL.16 NO.1, Pusblished at: 2014.

[32] Iman Almomani, Bassam Al-Kasasbeh and Mousa AL-Akhras: "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks", Journal of Sensors (2):1-16, January 2016

[33] Teplan, Michal. (2002). Fundamental of EEG Measurement. MEASUREMENT SCIENCE REVIEW. 2.

[34] Paudel, Bishnu Hari Limbu, Nirmala Panta, Raju Ghimire, Nisha Shrestha, Binu Deo, Santosh. (2012). Electroencephalography (EEG).

[35] Alex Lau-Zhu, Michael P.H. Lau, Gráinne McLoughlin 'Mobile EEG in research on neurodevelopmental disorders: Opportunities and challenges' journal of Developmental Cognitive Neuroscience, March,2019

[36] A. Mohammed, "A Cross Layer for Detection and Ignoring Black Hole Attack in MANET", Publisher: I. J. Computer Network and Information Security (IJCNIS) DOI: 10.5815/ijcnis.2015.10.05, Published Online at: September 2015 in: MECS.

[37] A.P.Jadhao, Dr.D.N.Chaudhari, Article: "Security Aware Adhoc on Demand Distance Vector Routing Protocol in Vehicular Adhoc Network", Publisher: International Journal of Innovative Research in Computer and Communication Engi-

neering (IJIRCCE), ISSN Online: 2320-9801, Vol: 2, Issue: 12, Published at : December 2014.

[38] K. Malasri and L. Wang, “Design and implementation of a secure wireless mote-based medical sensor network,” Sensors, vol. 9, no. 8, pp. 6273–6297, Aug. 2009.

[39] D. He, S. Chan, and S. Tang, “A novel and lightweight system to secure wireless medical sensor networks,” IEEE journal of biomedical and health informatics, vol. 18, no. 1, pp. 316–326, Jan. 2014.

[40] H. Wang, H. Fang, L. Xing, and M. Chen, “An integrated biometricbased security framework using wavelet-domain HMM in wireless body area networks (WBAN),” in IEEE International Conference on Communications (ICC), Kyoto, Japan, Jul. 2011, pp. 1–5.

[41] G. Thamilarasu, “Genetic algorithm based intrusion detection system for wireless body area networks,” in IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, Jul. 2015, pp. 160–165

[42] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, and B. Furht, “Sensor fault and patient anomaly detection and classification in medical wireless sensor networks,” in IEEE International Conference onommunications (ICC), Budapest, Hungary, Jun. 2013, pp. 4373–4378.

[43] T. Issariyakul, E. Hossain, Book: "An introduction to network simulatorNS2", Publisher: Springer US, Copyright holder: Springer Science+Business Media, LLC, ISBN: 978-1441944122, DOI: 10.1007/978-1-4614-1406-3, Published in: 2012.

[44] Padiya, Sagar Pandit, Rakesh. (2013). Neighbouring node based system to detect selfish nodes in MANET using NS2.

Appendix 1

```
#===================================================
#  EEG under Blackhole using  25 nodes
#===================================================
#
#===================================
#      Simulation parameters setup
#===================================
set val(chan)    Channel/WirelessChannel     ;# channel type
set val(prop)    Propagation/TwoRayGround
;# radio-propagation model
set val(netif)   Phy/WirelessPhy
;# network interface type
set val(mac)     Mac/802_11                  ;# MAC type
set val(ifq)     Queue/DropTail/PriQueue
;# interface queue type
set val(ll)      LL                          ;# link layer type
set val(ant)     Antenna/OmniAntenna         ;# antenna model
set val(ifqlen) 50
;# max packet in ifq
set val(nn)      25
;# number of mobilenodes
set val(rp)       AODV                       ;# routing protocol
```

```
set val(brp)      blackholeAODV;
# Malicious node routing
set val(x)       1186
;# X dimension of topography
set val(y)       600
;# Y dimension of topography
set val(stop)    40
;# time of simulation end
set val(t1)      0.0                          ;
set val(t2)      0.0                           ;


#===================================
#        Initialization
#===================================
#Create a ns simulator
set ns [new Simulator]


#Setup topography object
set topo        [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)


#Open the NS trace file
set tracefile [open eeg25_det_attack.tr w]
$ns trace-all $tracefile


#Open the NAM trace file
set namfile [open eeg25_det_attack.nam w]
$ns namtrace-all $namfile
```

```
$ns namtrace-all-wireless $namfile $val(x) $val(y)
set chan [new $val(chan)];#Create wireless channel


#===================================
#      Mobile node parameter setup
#===================================
$ns node-config -adhocRouting  $val(rp) \
                -llType        $val(ll) \
                -macType       $val(mac) \
                -ifqType       $val(ifq) \
                -ifqLen        $val(ifqlen) \
                -antType       $val(ant) \
                -propType      $val(prop) \
                -phyType       $val(netif) \
                -channel       $chan \
                -topoInstance  $topo \
                -agentTrace    ON \
                -routerTrace   ON \
                -macTrace      ON \
                -movementTrace ON


#===================================
#        Nodes Definition
#===================================
#Create 20 nodes
```

```
set n0 [$ns node]
$n0 set X_ 638
$n0 set Y_ 99
$n0 set Z_ 0.0
$ns initial_node_pos $n0 20

#set n1 [$ns node]


set n2 [$ns node]
$n2 set X_ 501
$n2 set Y_ 200
$n2 set Z_ 0.0
$ns initial_node_pos $n2 20
set n3 [$ns node]
$n3 set X_ 797
$n3 set Y_ 201
$n3 set Z_ 0.0
$ns initial_node_pos $n3 20
set n4 [$ns node]
$n4 set X_ 399
$n4 set Y_ 199
$n4 set Z_ 0.0
$ns initial_node_pos $n4 20
set n5 [$ns node]
$n5 set X_ 730
$n5 set Y_ 301
$n5 set Z_ 0.0
```

```
$ns initial_node_pos $n5 20

set n6 [$ns node]

$n6 set X_ 631

$n6 set Y_ 303

$n6 set Z_ 0.0

$ns initial_node_pos $n6 20

set n7 [$ns node]

$n7 set X_ 543

$n7 set Y_ 302

$n7 set Z_ 0.0

$ns initial_node_pos $n7 20

set n8 [$ns node]

$n8 set X_ 453

$n8 set Y_ 299

$n8 set Z_ 0.0

$ns initial_node_pos $n8 20

set n9 [$ns node]

$n9 set X_ 740

$n9 set Y_ 102

$n9 set Z_ 0.0

$ns initial_node_pos $n9 20

set n10 [$ns node]

$n10 set X_ 698

$n10 set Y_ 199

$n10 set Z_ 0.0

$ns initial_node_pos $n10 20

set n11 [$ns node]

$n11 set X_ 546

$n11 set Y_ 101
```

```
$n11 set Z_ 0.0

$ns initial_node_pos $n11 20

set n12 [$ns node]

$n12 set X_ 447

$n12 set Y_ 102

$n12 set Z_ 0.0

$ns initial_node_pos $n12 20

set n13 [$ns node]

$n13 set X_ 632

$n13 set Y_ 402

$n13 set Z_ 0.0

$ns initial_node_pos $n13 20

set n14 [$ns node]

$n14 set X_ 548

$n14 set Y_ 404

$n14 set Z_ 0.0

$ns initial_node_pos $n14 20

set n15 [$ns node]

$n15 set X_ 633

$n15 set Y_ 8

$n15 set Z_ 0.0

$ns initial_node_pos $n15 20

set n16 [$ns node]

$n16 set X_ 550

$n16 set Y_ 15

$n16 set Z_ 0.0

$ns initial_node_pos $n16 20

set n17 [$ns node]

$n17 set X_ 586
```

```
$n17 set Y_ 463

$n17 set Z_ 0.0

$ns initial_node_pos $n17 20

set n18 [$ns node]

$n18 set X_ 593

$n18 set Y_ -47

$n18 set Z_ 0.0

$ns initial_node_pos $n18 20

set n19 [$ns node]

$n19 set X_ 578

$n19 set Y_ 529

$n19 set Z_ 0.0

$ns initial_node_pos $n19 20


set n20 [$ns node]

$n20 set X_ 740

$n20 set Y_ 202

$n20 set Z_ 0.0

$ns initial_node_pos $n20 20

set n21 [$ns node]

$n21 set X_ 459

$n21 set Y_ 196

$n21 set Z_ 0.0

$ns initial_node_pos $n21 20

set n22 [$ns node]

$n22 set X_ 789

$n22 set Y_ 105

$n22 set Z_ 0.0

$ns initial_node_pos $n22 20
```

```
set n23 [$ns node]
$n23 set X_ 548
$n23 set Y_ 100
$n23 set Z_ 0.0
$ns initial_node_pos $n23 20
set n24 [$ns node]
$n24 set X_ 561
$n24 set Y_ 301
$n24 set Z_ 0.0
$ns initial_node_pos $n24 20



$ns node-config -adhocRouting $val(brp)
set n1 [$ns node]



$n1 set X_ 601
$n1 set Y_ 200
$n1 set Z_ 0.0
$ns initial_node_pos $n1 20


$ns at 0.0 "$n1 label \"blackhole node \""


$n1 color red
$ns at 0.0 "$n1 color red"


#$n13 color red
#$ns at 0.0 "$n13 color red"
#$ns at 0.0 "$n13 label Attacker"
```

```
#-------------------------------------------------------------------------------

$n19 shape box
$n19 color blue
$ns at 0.0 "$n19 color blue"



$ns at 0.0 "$n19 label Sink"

#########################################

set tcp3 [new Agent/TCP]
$ns attach-agent $n18 $tcp3

set sink3 [new Agent/TCPSink]
$ns attach-agent $n13 $sink3
$ns connect $tcp3 $sink3
#################################

#set tcp4 [new Agent/TCP]
#$ns attach-agent $n8 $tcp4

#set sink4 [new Agent/TCPSink]
#$ns attach-agent $n19 $sink4
#$ns connect $tcp4 $sink4



#################################################
##############Traffic###############
```

```
set ftp [new Application/FTP]
$ftp attach-agent $tcp3

#set cbr1 [new Application/Traffic/CBR]
#$cbr attach-agent $tcp4



$ns at 0.2 "$ftp start"

#$ns at 0.1 "$cbr1 start"
$n13 color green
$ns at 0.0 "$n13 color green"



$n18 color green
$ns at 0.0 "$n18 color green"

$ns at 0.0 "$n18 label Source"
$ns at 0.0 "$n13 label Destination"

#############################################################################################

#=====================================
#        Termination
#=====================================
#Define a 'finish' procedure
```

```
proc finish {} {
    global ns tracefile namfile
    $ns flush-trace
    close $tracefile
    close $namfile
    exec nam eeg25_det_attack.nam &
    exit 0
}
for {set i 0} {$i < $val(nn) } { incr i } {
    $ns at $val(stop) "\$n$i reset"
}
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ; $ns halt"
$ns run
```

Appendix 2

Tracefile.tr

```
s 0.200000000 _17_ AGT --- 0 tcp 40 [0 0 0 0]
-------- [17:0 12:0 32 0] [0 0] 0 0
r 0.200000000 _17_ RTR --- 0 tcp 40 [0 0 0 0]
-------- [17:0 12:0 32 0] [0 0] 0 0
s 0.200000000 _17_ RTR --- 0 AODV 48 [0 0 0 0]
-------- [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)
s 0.200115000 _17_ MAC --- 0 AODV 106 [0 ffffffff 11 800]
-------- [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)
r 0.200963227 _14_ MAC --- 0 AODV 48 [0 ffffffff 11 800]
-------- [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)
r 0.200963252 _15_ MAC --- 0 AODV 48 [0 ffffffff 11 800]
-------- [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)
r 0.200963509 _0_ MAC --- 0 AODV 48 [0 ffffffff 11 800]
-------- [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)
r 0.200963512 _22_ MAC --- 0 AODV 48 [0 ffffffff 11 800]
-------- [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)
r 0.200963518 _10_ MAC --- 0 AODV 48 [0 ffffffff 11 800]
-------- [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)
r 0.200963695 _11_ MAC --- 0 AODV 48 [0 ffffffff 11 800]
-------- [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)
r 0.200963698 _8_ MAC --- 0 AODV 48 [0 ffffffff 11 800]
```

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200963824 _24_ MAC --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200963827 _21_ MAC --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200988227 _14_ RTR --- 0 AODV 48 [0 ffffffff 11 800]* ——— [17:255

r 0.200988252 _15_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200988509 _0_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200988512 _22_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200988518 _10_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200988695 _11_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200988698 _8_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

r 0.200988824 _24_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

s 0.200988824 _24_ RTR --- 0 AODV 44 [0 0 0 0]

——— [24:255 17:255 30 17] [0x4 1 [12 -1] 10.000000]

(REPLY)

r 0.200988827 _21_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [17:255 -1:255 30 0] [0x2 1 1 [12 0] [17 4]] (REQUEST)

s 0.201283824 _24_ MAC --- 0 ARP 86 [0 ffffffff 18 806]

——— [REQUEST 24/24 0/17]

s 0.201869453 _14_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

```
r 0.201972147 _9_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972157 _1_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972181 _5_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972182 _0_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972186 _23_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972201 _22_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972201 _10_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972215 _6_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972287 _19_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972297 _20_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972370 _4_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972391 _8_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972417 _7_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972432 _11_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
---------- [REQUEST 24/24 0/17]
r 0.201972463 _15_ MAC ---- 0 ARP 28 [0 ffffffff 18 806]
```

——— [REQUEST 24/24 0/17]

r 0.201972473 _14_ MAC —— 0 ARP 28 [0 ffffffff 18 806]

——— [REQUEST 24/24 0/17]

r 0.201972477 _2_ MAC —— 0 ARP 28 [0 ffffffff 18 806]

——— [REQUEST 24/24 0/17]

r 0.201972497 _3_ MAC —— 0 ARP 28 [0 ffffffff 18 806]

——— [REQUEST 24/24 0/17]

r 0.201972505 _12_ MAC —— 0 ARP 28 [0 ffffffff 18 806]

——— [REQUEST 24/24 0/17]

r 0.201972526 _21_ MAC —— 0 ARP 28 [0 ffffffff 18 806]

——— [REQUEST 24/24 0/17]

r 0.201972526 _13_ MAC —— 0 ARP 28 [0 ffffffff 18 806]

——— [REQUEST 24/24 0/17]

r 0.201972648 _17_ MAC —— 0 ARP 28 [0 ffffffff 18 806]

——— [REQUEST 24/24 0/17]

s 0.202062473 _14_ MAC —— 0 AODV 106 [0 ffffffff e 800]

——— [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.202910699 _17_ MAC —— 0 AODV 48 [0 ffffffff e 800]

——— [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.202910750 _15_ MAC —— 0 AODV 48 [0 ffffffff e 800]

——— [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.202910776 _0_ MAC —— 0 AODV 48 [0 ffffffff e 800]

——— [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.202910890 _22_ MAC —— 0 AODV 48 [0 ffffffff e 800]

——— [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.202910897 _10_ MAC —— 0 AODV 48 [0 ffffffff e 800]

——— [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.202910947 _8_ MAC —— 0 AODV 48 [0 ffffffff e 800]

——— [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

```
r 0.202911085 _21_ MAC --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202911121 _24_ MAC --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202911145 _9_ MAC --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202911167 _11_ MAC --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202911211 _19_ MAC --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202911249 _1_ MAC --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202935699 _17_ RTR --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202935750 _15_ RTR --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202935776 _0_ RTR --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.202935890 _22_ RTR --- 0 AODV 48 [0 ffffffff e 800]
-------- [14:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.204587171 _24_ MAC --- 0 ARP 28 [13a 18 11 806] --------
[REPLY 17/17 24/24]
s 0.204597171 _24_ MAC --- 0 ACK 38 [0 11 0 0]
r 0.204901994 _17_ MAC --- 0 ACK 38 [0 11 0 0]
s 0.205151548 _22_ MAC --- 0 AODV 106 [0 ffffffff 16 800]
-------- [22:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
s 0.205399985 _15_ RTR --- 0 AODV 48 [0 ffffffff 11 800]
-------- [15:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)
r 0.205999555 _10_ MAC --- 0 AODV 48 [0 ffffffff 16 800]
```

——— [22:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.205999831 _15_ MAC --- 0 AODV 48 [0 ffffffff 16 800]

——— [22:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.205999848 _0_ MAC --- 0 AODV 48 [0 ffffffff 16 800]

——— [22:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.206918528 _8_ MAC --- 0 AODV 48 [0 ffffffff f 800]

——— [15:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.206918618 _9_ MAC --- 0 AODV 48 [0 ffffffff f 800]

——— [15:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.206918625 _3_ MAC --- 0 AODV 48 [0 ffffffff f 800]

——— [15:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)

r 0.206943083 _17_ RTR --- 0 AODV 48 [0 ffffffff f 800]

——— [15:255

s 0.207172817 _1_ RTR --- 0 AODV 48 [0 ffffffff e 800]

——— [1:255 -1:255 28 0] [0x2 3 1 [12 0] [17 4]] (REQUEST)

r 0.207341295 _17_ MAC --- 0 RTS 44 [5ae 11 18 0]

s 0.207351295 _17_ MAC --- 0 CTS 38 [474 18 0 0]

s 0.207377349 _8_ RTR --- 0 AODV 48 [0 ffffffff 11 800]

——— [8:255 -1:255 29 0] [0x2 2 1 [12 0] [17 4]] (REQUEST)