CHAPTER 1

INTRODUCTION

1.1 Literature Survey

The method may efficiently find rogue nodes by inspecting network traffic in real time. Our system is capable of creating a dynamic blacklist of Network nodes that may be used to block nodes whose trust levels are below a certain minimum. The detection of malicious nodes and the computation of node trust levels are handled by a central server. To increase the network and infrastructure's security, the method may be used in conjunction with other security tools including database activity monitoring, white listing, and data loss prevention. Session based encrypt is used to secure the node from the compromised attacker. Attacker request will be accepted by unique key of individual node validation process. Intruders wouldn't be able to steal TOP-SECRET data or information if this were done.. [1]

There is a need for a serious breakthrough in Body Area Networking. It would be a failure on the part of researchers to see physical connections like wires or foils running all round the body. A high impedance shoe is essential in situations where electrons flow through the body and carry the information/data. Since the human body conducts electricity very well and serves as a short to the movement of charges within the body. The wireless Body Area Network is a very good substitute for the aforementioned. The transmission and reception of data takes place within the circumference of a body (an AS) or between two or more AS. The former is called Intra-AS Communication and the latter is called Inter-AS communication. We have adopted a wireless data routing and sharing system using various protocols that suits the present technological scenario. [2]

The cutting-edge technology in the electronics and telecom industries is called wireless body area networking. A new generation of wireless sensor networks has been made possible by the fast advancement of wireless connectivity, low power integrated circuits, and physiological sensors.These networks are being utilised for monitoring traffic, infrastructure, gaming, and health, among other things. The BAN is a multidisciplinary field that could provide low-cost ongoing health monitoring using real-time online updating

of medical information. The sensors utilised in WBAN would need to be simple, have a tiny form factor, be lightweight, require little power, be simple to use, and be customizable. Additionally, the storage devices must provide remote patient data storage and viewing, as well as Internet connectivity to third-party processing and analysis tools. [3]

In the modern and unique discipline of body area networking (BAN), packets are sent to a specified location within the human body using wireless technology. Only when all nodes are reachable and the sensors, computers, or other electrical components are correctly integrated would this be achievable. In this research, efforts were made to use a dynamic routing system like OSPF to connect each node inside an autonomous body. [4]

1.2 PROBLEM STATEMENT

Any Country consisting of a huge Border or Area would contain a large amount of military, air force and navy personnel. They may be commissioned to operate even at remote areas, away from the national capital or military base communication between these nodes is of top most importance a network. needs to be setup to security exchange information between the nodes these men need to be monitored carefully, to increase these efficiency in serving the nation health monitoring of these mean by embedding various body sensors and encrypting the data between the nodes is of top most priority.

1.3 MOTIVATION

Health departments and computer networking are only two examples of the many domains in which networking media are used today. For the purpose of locating the illness within the human body, a network was created. The BAN, or body area network, is the name of this network. Body area networks are typically referred to as the many types of n/ws that deal with the monitoring and detection of the complete human body system. The BSN is another name for it (body sensor network). This article talks about the body area network (BAN), a technology that is utilised to offer accessible, affordable healthcare worldwide. In the event of military applications, a separate internetwork is required. It must be capable of quickly transferring private information as well as other kinds of data. It is not surprising

that information and communication technologies (ICT) now serve as the foundation for many parts of the industry given their fast growth and interconnection. The sensitivity of the information and the quantity and variety of devices that may be used to target the system make these networks the subject of stricter regulation than traditional networks.

OBJECTIVE

In light of the current environment, the objective of this work is to identify and choose from among the available In terms of patient mobility, secure and reliable data, power consumption, and the requirements needed for several sensor nodes to cohabit in a relatively small space, technologies and protocols that satisfy the main objectives of WBANs for the application of healthcare are needed. Consider the various requirements in a medical network requires a thorough understanding of the protocol stack and each protocol layer. This book offers a summary of the state-of-the-art for WBAN. It mainly focuses on healthcare network topologies and communication protocols that are WBAN-based. We examine the protocols applied at each protocol layer as well as the most recent implementation approaches for this kind of network. Each implementation has unique traits, benefits, and drawbacks that are thoroughly documented and compared in a number of comparative tables. Additionally, as well as procedures for nonproprietary WBANs on unlicensed radio frequency bands, we present a comparison of contemporary and historical radio technologies.

SCOPE OF PROJECT

Due to their characteristics and dependability, body area networks are utilised in a variety of applications. These networks are utilised for illness monitoring and detection.
Following are some of the typical BAN applications.

- • BANs are employed in the medical industry for the purpose of monitoring and spotting interior ailments in people.
- • BANs are used to identify a number of chronic conditions, including asthma, heart attacks, and others.
- • BANs are also utilised in communication, on the sports, and by security organisations.

.

Future applications for this BAN (body area network) include monitoring, detection, networking, etc. If the issues with BANs could be resolved, then the entire technical community would be covered by this technique. The new technologies that will be developed with the benefit of humanity will also be supported by its applications.

CHAPTER 2

METHODOLOGY

2.1 ABOUT ROUTER

A router is a networking device that forwards data packets in computer networks. Routers are responsible for directing traffic on the Internet. The fundamental building elements of information transferred via the internet, such as a web page or email, are known as data packets. Typically, packets are sent across an internetwork (like the Internetnetworks) from one router to another until they reach their destination node.

A router's primary function will be for the connecting to different networks with also forward packets that are headed to one of personal networks or another network. Because it bases its major forwarding choice on the information contained in the layer-3 IP packet, namely the destination IP address, a router was referred to a layer-3 device. When a packet is received, a router looks through its to find the address in the routing table that most closely matches the packet's destination IP address. If a match is found, the packet is subsequently enclosed in the layer-2 data link frame for the outgoing interface listed in the table item. The layer-3 addresses are normally all that a router looks at to decide whether to forward a packet, with the option of also looking at extra details in the header for advice on matters like service quality (QOS). A router made to reduce state information associated with individual packets for pure IP forwarding. After a packet is forwarded, the router does not retain any history information about it.

2.2 OPERATION

A routing protocol is used by routers in networks with numerous interconnected routers to communicate data about destination addresses. Each router creates a routing table that details the best paths between any two computers on connected networks.

Two different kinds in components of network elements are arranged in a router.

1) Plane of control: the router maintains a routing table with information on which physical interface connection and route should be used to forward a data packet. It accomplishes these tasks either by utilising a routing protocol to learn routes on the fly or by using internal predefined directives known as static routes. The routing table contains information about

static and dynamic routes. After removing all but necessary directives from the table, the control-plane logic creates a forwarding information base (FIB) that the forwarding plane can use.

2) Forwarding plane: Data packets are forwarded by the router between connections on the incoming and outgoing interfaces. Using data from header packet compared with entries of FIB provided by plane of control, it sends them to the appropriate network type.

2.3 APPLICATION

- The router might include interface for only a range of physical layers communications, including wireless transmission, fibre optics, and copper wires. Additionally, it can handle several transmission protocols at the network layer. Data packets can be forwarded from one transmission system to another using each network interface. Additionally, routers can be used to link two or more subnets—logical groups of computer equipment with their own unique network prefix—together.
- Router can provide connection for companies, for companies and the Internet, and for customers or across the networks of internet service providers (ISPs). Larger routers (like the Cisco CRS-1 or Juniper PTX) are used in big enterprise networks or to connect different ISPs. Typical home and workplace networks are typically connected by smaller routers.
- In businesses, routers come in all shapes and sizes. In ISPs, academic institutions, and research centres, the most potent routers are typically found. To handle the escalating demands of intranet data traffic, large enterprises may also require more potent routers. For connecting routers in big networks, a hierarchical internetworking model is commonly used..

2.4 TYPES OF ROUTER

1) ACCESS ROUTERS

It includes small office or home office (SOHO) models that were situated in customer's sites like branch office and don't require their own hierarchical routing. Typically, they are cost-optimized. Free Linux-based alternative firmware like Openwork, or DD - WRT can be run on some SOHO routers.

2) ROUTERS FOR DISTRIBUTION

Traffics onto various access to router combined. Routers for distribution may contain a significant amount of installed RAM, many interface connections of WAN, also significant onboard processing the data algorithms because it is frequently in charge of assure quality service over the wide area networks (WAN). Additionally, it might offer connection for collections in file server or the other outside network.

At large enterprise sites or campuses, the core routers might act as collapses backbone connect the distribution layer routers various building. Although they frequently have high bandwidth optimization, they don't have all of edge routers' features..

2.5 OSI MODEL

A layer benefits from the service of layers above and below them. To instance, the layer which ensures errorless network connection offers a road need to programmes although calling layer below it for transmitting and receiving the packet which make up a path's matters.

1st Layer – Physical layer

2nd Layer - Data Linking Layer

3rd Layer - Network Layer

4th Layer - Transport Layer

5th Layer - Session Layer

6th Layer - Presentation Layer

7th Layer - Application Layer

2.6 SECURITY

The overall security plan for the local network must properly take into account external networks. the firewall and VPN handling and other security features might included in a router, or they may be handled by different devices. Network address translation, which is frequently carried out by routers and limits connections started through outer connections, that was not universally regarded security features. Because errors can be promptly detected and fixed with open source routers, some experts contend that they were more dependable ,also secure more of closed source routers.

2.7 DIFFERENT NETWORKS OF ROUTERS

Routers are typically separated from one another based on the network they operate in. A router that is a component of a single company's local area network (LAN) is known as an inside router. A router utilised as a component of the Internet backbone is known as an external router. A router that links a local area network (LAN) to the Internet or a wide area network is referred to as a "border router" or "gateway router" (WAN).

2.8 IP ADDRESS

Every device connected with computer networks that makes use of a Internet Protocol was given a numerical label called as the Internet Protocol (IP) address.

An IP address has two primary purposes:

1. Network interface or host identifier

2. Geographic addressing

A 32-bit number is what the Internet Protocol version 4 (IPv4) defines as an IP address. However, a new version of IP (IPv6), utilising 128 bits for the IP address, was established in 1998 in response to the expansion of the Internet and the exhaustion of IPv4 addresses. Deployment of IPv6 has been happening since the middle of the 2000s.

The Internet Assigned Numbers Authority (IANA) oversees the management of the IP address space on a global scale, and five regional Internet registries (RIRs) are in charge of managing it in their respective regions for assignment to local Internet registries, such as Internet service providers and other end users.

IANA allocated IPv4 addresses to the RIRs in blocks of roughly 16.8 million addresses each, however the supply has been depleted at the IANA level since 2011. In Africa, only one RIR still has a supply of local assignments available. Some IPv4 addresses are not globally unique and are set aside for private networks.

Each device linked to a network is given an IP address by network administrators. Depending on network procedures and software features, such assignments may be static (fixed or permanent) or dynamic.

2.9 FUNCTION

Two main purposes are served by an IP address. It gives the host location in network and, thus, ability to create a path to that host. Additionally, the host's network interface, or more particularly, its host, is identified.Its function has been described as follows: "What we want is indicated by a name. An address identifies its location. How to get there is shown by a route." Each IP packet's header includes the sending host's and destination host's IP addresses.

2.10 IP VERSIONS

IP address provides 2 key functions. they provides host position inside the network, making it possible to build a path to that host. Additionally, the host's network interface, or more particularly, its host, is identified. The following is an explanation of its purpose: "A name tells us what we want. Its position is determined by its address. A path demonstrates how to get there."

These two Internet Protocol iterations are currently used concurrently. among other technical modifications. The IPv4 addresses are still commonly referred to by the general term "IP address" due to IPv4's historical dominance. The experimental Internet Stream Protocol, which was given version 5 in 1979 but was never referred to as IPv5, caused the gap between IPv4 and IPv6 in the version sequence.

Only v4 and v6 ever saw significant adoption among the other versions, which ranged from v1 to v9. Since there is no different IP definition at time, the TCP protocols were referred to as V1 and V2 in 1974 and 1977, respectively. The first time TCP and IP were split was in version 3.1, which was defined in 1978. V6. P Internet Protocol and version 9 of TUBA were created by combining the indicated versions v6 Simple Internet Protocol, v7 TP/IX: The Next Internet, and v8 PIP.

2.11 SUB-NETWORKS

All IPv4 and IPv6 allowed to the division of Internet Protocol networks into subnetworks. The high-order bits of the network prefix, also known as remainder field and host identification, or interfaces identifier (IP v 6), are recognised as the two components of an IP address for this purpose and are used to hosting number with in the network. A division of the I P address in to the network, host components was controlled from a subnet mask or CIDR notation.

Only in IPv4 is the phrase "subnet mask" utilised. However, the CIDR idea and syntax are used in both IP versions. In this, the routing prefix—also known as the network part—is followed by the IP address, a slash, and the amount of bits (in decimal). An IPv4 address might be 192.0.2.1 and its subnet mask might be 255.255.255.0, for instance.

2.12 PROTOCOLS

[1] Open Short Path First (OSPF)

It's a route mechanism to networks using the Internet Protocol IP. They belongs to the class of interior gateways protocol IGPs, operates with-in the single autonomouses system, makes use of link state routing (LSR) algorithm. For IPv4, it's described to be O S P F Version 2 in RFC - 2328 (1998). In RFC 5340, upgrades to IP v6 were described to be OSPF Version 3. (2008). The Classless Inter-Domain Routing (CIDR) addressing model is supported by OSPF.

The popular I G P in huge industrial network's OSPF. Large service provider networks tend to use IS-IS more frequently than other LSR-based protocols. As the inner gateway protocol (IGP) for usage in an autonomous system like a LAN, OSPF was created (LAN). The SPF algorithm, widely known as Dijkstra's algorithm, is implemented. It was based on the IS-IS routing protocol and the link-state algorithm created in 1980 for the ARPANET as a link-state routing system. RFC 1131, now referred to as OSPF version 1, was the name of the RFC that initially specified OSPF in 1989. The Digital Equipment Corporation, which created its own proprietary decent protocols, carried out the majority of the development work for OSPF prior to its codification as an open standard.

An algorithm is used by routing protocols like OSPF to find the shortest route across the network to a given location. The very first commonly utilized routing protocol, known as the Routing Information Protocol (RIP), calculated the shortest path based on hops, or the number of routers an IP packet had to transit through in order to reach the target host. RIP has successfully developed dynamic routing, in which routing tables update anytime the topology changes. To adjust for changing network factors, such as connection speed, RIP did not influence its routing. Growing in popularity is a route optimization system that might identify the shortest route.

OSPF was developed to enable the calculation of the shortest path over a network using the cost of route, which takes into consideration bandwidth, latency, and load. OSPF employs link-cost parameters that can be weighted by the administrator to determine route costs. OSPF was quickly used because it had a reputation for properly determining routes across large local area networks.

Network topology diagrams known as link state databases are maintained by each router that employs OSPF as its link state routing protocol. The OSPF algorithm allows each router to calculate the cost of the routes to any given accessible destination. A route's cost is determined by where it resides in the network.

The bit rate of the interface—1 Gbit/s & 10 Gbit/s, etc.—determines connection cost of the path connected to a router unless the administrator has set a configuration. The next step, called as the hello operation, involves routers interfaces with O S P F advertising it's linking cost to nearby routers over multicast. In order to inform neighbouring routers when the cost of their links changes, all routers that employ OSPF continue to broadcast hello packets. The cost of a link or the speed of a point-to-point connection between two routers is subsequently cascaded across the network since OSPF routers broadcast the information they get from one adjacent router to all other neighbouring routers. The process of flooding the network with link status information is known as synchronisation. All routers employing OSPF constantly update their routing tables and link state databases with the network topology based on this data.

[2]Enhance Interior Gate-way Route Protocol (**EIGRP**)

To automate routing configuration and choices on a computer network, a complex distance-vector routing protocol is utilised. Cisco Systems developed the unique protocol, which is only supported by Cisco routers. The functionality of EIGRP was converted into an open standard in 2013 and released as RFC 7868 with informational status in 2016.

A router utilises EIGRP to exchange routes with other routers in the same autonomous system. In contrast to other well-known routing protocols like RIP, EIGRP simply broadcasts incremental updates, which lessens the load on the router and the amount of data that has to be broadcast.

Interior Gateway Routing Protocol (IGRP) was superseded by EIGRP in 1993. The Internet Protocol's switch to classless IPv4 addresses, which IGRP could not handle, was one of the main causes of this.

FEATURES

i. Support for Classless Inter-Domain Routing and Variable Length Subnet Masking. Routes are not totaled at the class complete network boundary if auto summary is not enabled.
ii. Support for load balancing across several sites using parallel links.
iii. The capacity to alternate between various login passwords.
iv. Authentication using MD5 and SHA-2 between two routers.
v. When a route is updated, topological modifications are sent rather than the complete routing table.
vi. Routing changes are propagated to neighbouring routers if they occur and a route is found to be accessible.
vii. Compatibility with IGRP routing techniques in the past.
viii. Lowest Bandwidth Minimum bandwidth between the router and the destination network, in kilobits per second.
ix. a load value between 1 and 255, where 255 is the saturation load
x. Overall Delay The amount of time, in tens of microseconds, required to get from the router to the destination network.
xi. a number for trustworthiness that ranges from 1 to 255, with 255 being the most reliable .
xii. Minimal Transmission Unit, or MTU (never used in the metric calculation)

[3] Route Informations Protocol (RIP)

One of the early distance-vector routing metrics employed by this protocol is hop count. Routing loops are avoided by RIP by limiting the number of hops that may be made from source to destination. The size of networks that RIP can handle is capped at 15, which is the maximum number of hops that it is allowed to give.

To stop spread of false routing information, RIP uses the split horizon, route poisoning, and hold-down methods.

RIPv1 routers send updates including their routing table every 30 seconds. Routing tables used in earlier deployments were so tiny that traffic was hardly detectable. Although routers were initialised at random intervals, it became evident that there may be a major traffic surge every 30 seconds as networks grew in size.

Since RIP has a slower time to convergence and less scalability than EIGRP, OSPF, or IS-IS, it is not the recommended routing protocol in the majority of networking scenarios. Contrary to other protocols, RIP does not call for any parameters, making configuration easy.

RIP employs the User Datagram Protocol (UDP) as its transport protocol and has been assigned the reserved port number 520.

RFC 1058, which contains the first version of the RIP specification, was published in 1988. At startup and thereafter, each RIPv1 enabled interface on a router with RIPv1 implementation sends a request message to 255.255.255.255 every 30 seconds. Neighboring routers respond to the request message with a RIPv1 segment providing their routing table. The asking router modifies its own routing table using the accessible IP network address, hop count, and next hop—the router interface IP address from where the RIPv1 answer was delivered.

If a reachable network that is not already in the requesting router's routing table is discovered or if it is discovered that a network that is already in the routing table can be reached with fewer hops, the requesting router will only update the reachable networks in its routing table as it receives updates from various neighbouring routers. As a result, for an accessible network, a RIPv1 router frequently only has one entry—the one with the fewest hops. If a router learns from two separate neighbouring routers that the same network is reachable with the same hop count but through two different routes, it will add that network twice with unique next hop routers to the routing table.

RIPv1-capable routers additionally keep a look out for incoming requests from adjacent routers and reply by delivering their own routing table, in addition to requesting other routers' routing tables every 30 seconds. RIPv1 routing tables are updated as a result every 25 to 35 seconds. The RIPv1 protocol adds a minor random time variable to the update time to prevent routing tables from synchronising across a LAN. [8] Although it was hoped that the random initialization would cause the routing changes to disperse over time, this was not the case. Sally Floyd and Van Jacobson showed that the timings synchronised over time in 1994 without any small randomization of the update timer.

A router can request and process neighbouring routing tables in RIPv1's quiet mode, keep track of the hop count and routing table for reachable networks, and avoid sending its own routing table into the network needlessly. Silent mode is often installed on hosts.

RIP version 2

Due to shortcomings in the original RIP specification, RIP version 2 (RIPv2) was developed in 1993, published as RFC 1723 in 1994, and declared Internet Standard 56 in 1998. It could transmit subnet information, which enabled Classless Inter-Domain Routing (CIDR). The 15-hop restriction is still in place to maintain backward compatibility. RIPv2 has the ability to completely interoperate with RIPv1 if all Must Be Zero protocol fields in the RIPv1 messages are appropriately specified. Additionally, a compatibility switch mechanism allows for exact interoperability changes.

To lessen the load on sites that do not participate in routing, RIPv2 multicasts the whole routing table to all nearby routers at the address 224.0.0.9 as compared to RIPv1, which uses broadcast. In some cases, uncast addressing is still acceptable. The (MD5) authentication mechanism for RIP was first established in 1997.

Route tags were also introduced in RIP version 2. This functionality allows one to distinguish between routes learned using the RIP protocol and routes learned using other protocols.

2.13 3-WAYS HANDSHAKING

Another way to think about this is as the procedure for establishing a TCP connection. Before delving into the details, let's examine the principles. The phrase "Transport Control Protocol," or TCP, is used to refer to a technique for consistently controlling data transport.

Currently, the TCP/IP suite paradigm controls how devices interact with one another over the internet (stripped out version of OSI reference model).

The top tier of the stack in the TCP/IP paradigm is called the application layer, from which network-referenced client-side software, such a web browser, connects to the server. Our topic is covered as the data is transferred from the application layer to the transport layer. The two primary protocols of this layer are TCP and UDP (User Datagram Protocol), with TCP predominating (since it provides reliability for the connection established). However, the binary form of the website's domain name may be obtained by querying the DNS server using UDP. To ensure reliable communication, TCP employs a method called as Positive Acknowledgement with Re-transmission (PAR). The transport layer's Protocol Data Unit is known as segment (PDU). Thus, the sender must resend the data unit for which a positive acknowledgement was not received. A reliable TCP connection can only be established if three segments are transmitted and received by the sender (client) and receiver (server), respectively.

. With these, a full-duplex communication is established.

A TCP/IP network uses the three-way handshake, often known as a TCP three-way handshake, to connect the server and client. Before the actual data transmission process begins, there are three steps that call for the client and server to exchange synchronisation and acknowledgement packets.

- The 3-way handshake method was built so that both ends assist you in simultaneously initiating, negotiating, and severing TCP socket connections. You can use it to simultaneously transfer numerous TCP socket connections in both ways. A TCP or IP network uses the TCP 3-way negotiation, also known as the three-way handshake or TCP 3-way handshake, to join the servers and user.
- The ACK let the other side know that it received the SYN, and Sync is used to establish and maintain a connection.
- SYN-ACK is the result of combining the SYN message from a local device with the ACK from the previous packet.

- FIN can be used to break a connection.
- The TCP handshake procedure consists of the subsequent steps:
- The discussion must be initiated by the client by requesting a communication session with the server.
- Following that, the client and server connect.
- The SYN-ACK signal is set by the server in response to the client request.
- Following that, the client responds to the server's response.
- two endpoints' connection is then automatically severed using TCP.

2.14 REDISTRIBUTION ROUTER

Network routes are imported and exported during redistribution from one routing protocol (or static routing) to another during networking. Redistribution can be set up in routers that use two or more routing protocols. As an illustration, consider a router that can import network routes from OSPF into EIGRP and vice versa. You will need to manually assign a measure to redistributed routes because different routing protocols utilise different metrics.

The majority of networks you'll come across probably only use one routing protocol, such as OSPF or EIGRP. You might come across some outdated, small networks that are still using RIP and need to be upgraded to OSPF or EIGRP.

It's likely that our network uses numerous routing protocols, in which case we'll need a way to share routing data between them. We refer to this as redistribution. We'll investigate a few of the problems we run with. What will we do with these metrics? EIGRP utilises K-values, while OSPF uses costs, and the two are incompatible. Hop count is used by RIP.

Redistribution introduces still another issue. It is possible to construct routing loops if you "import" routing information from 1 route protocol in to other. One route protocol only could be challenging, but when you combine several of them, the fun truly begins...

Redistribution is the process of using a routing protocol to promote routes that have already been discovered by different techniques, such as through the use of another routing protocol, static routes, or routes that are immediately connected. Multi-protocol routing is frequently used in a variety of situations, including business mergers, multiple departments managed by different network managers, and settings with multiple vendors. While using a single routing protocol throughout your entire IP network is ideal, it is not always possible. A network design typically includes using several routing methods. In any case, redistribution is necessary in a multi-protocol context. Variations in the routing protocol's metrics, administrative distance, classful, and classless capabilities can have an impact on

redistribution. These disparities must be taken into consideration for redistribution to be effective.

CHAPTER 3

IMPLEMENTATION AND DESIGN ANALYSIS

A person's clothing, body, or under-skin nodes are all connected via a WBAN. A node is connected by a wireless communication channels, & the network are to covers the entire human body. These nodes are arranged in a star or multihop topology by the implementation.

With its unlimited mobility, a WBAN offers a wide range of cutting-edge applications, including remote health monitoring, home/health care, medicine, multimedia, sports, and many more. In the medical field, a patient could be fitted with a wireless body area network, which is made up of sensors that continually track a variety of biological processes, such as body temperature, blood pressure, heart rate, electrocardiogram (ECG), respiration, etc. The advantage is that the patient doesn't have to be in bed and may move around the room freely. They can even leave the hospital for a little while. Both the patient's quality of life and healthcare costs are improved. Furthermore, data collected over a longer time period and in the patient's natural surroundings yields more illuminating information, enabling a more precise and occasionally even quicker diagnosis.

A network's classification according to its span or range also serves as a measure of the network's overall complexity. One such classification is the Body Area Network (BAN). Although its range is limited to the circle of the person wearing it, the BAN's complicated architectural design necessitates considerable network setup and troubleshooting.

In the event that the topology of the network changes, the dynamic route protocol OSPF offers the solid foundation to network convergence. Areas are the logical subdivisions of an OSPF network. A logical connection between OSPF, EIGRP, RIP, routers, switches, and links that share the same area identity is called an area.

The protocols that govern the network allow it to function.

A protocol is a common set of guidelines that enables communication between electronic devices. These guidelines specify the permitted types of data transmission, the commands used to send and receive data, and the procedures for verifying data transfers. An analogy to a spoken language is a procedure. Every language has its own vocabulary and set of laws. If two people are speaking the same language, they can communicate effectively.Similar to software, hardware can connect with hardware regardless of the maker or type as long as both devices accept the same protocol.

There are protocols for numerous applications. Examples include Internet communication, wireless networking, and wired networking (such as Ethernet and 802.11ac) (e.g., IP). The

Internet protocol suite, which is used to transmit data across the Internet, has a wide variety of protocols. There are four groups of these procedures:

1. Layer of linking, including P P P, D S L, and Wi - Fi.
2. Layer of Internet, including IP v4 and IP v6.
3. Layer of Transport, including U D P and T C P.
4. Layer ofApplication, including H T T P, I M A P, and F T P

At the hardware level, link layer protocols set up communication between devices. The link layer protocol must be supported by the hardware of each device in order for data to be transmitted between them. Data transmissions are started and routed over the Internet using Internet layer protocols. Protocols at the transport layer specify how packets are sent, received, and verified. Commands for certain applications are contained in application layer protocols. For instance, a web browser employs HTTPS to safely download a webpage's contents from a web server. To send emails via a mail server, an email client uses SMTP. For many applications, a separate internetwork is required. It must be capable of quickly transferring private information as well as other kinds of data. It is not surprising that information and communication technologies (ICT) now serve as the foundation for many parts of the industry given their rapid growth and interconnection. The sensitivity of the information and the quantity and variety of devices that could be used to target the system make these networks the subject of stricter regulation than traditional networks. When it comes to wireless and mobile devices transferring TOP-SECRET information for the army, cyber dangers cannot be overlooked. In this research, we implement a network for intra- and inter-body communication. Each individual body is viewed as an autonomous system (AS) with mobility and a distinct autonomous system number (ASN) that may link to every other autonomous system (AS). This network would allow for the exchange of private information after it was linked and tested. Each node in the network must be password-protected in order for the information to be communicated through them. This would stop the burglars from stealing information or data. Routing and security are implemented on the network using the GNS 3 tool.

3.1 IP address for nodes

Internet Protocol is referred to as IP. Every machine in a network is given an Internet Protocol address, or IP address, which serves as a unique identity. An IP address has two main purposes. Similar to a physical address for a house or place of business, it is used as an interface identification for a network of devices and also serves to offer a location of that machine. Computers may exchanges data through particular computers in the network because an IP address is a distinctive identification.

There are now two IP address standards. There are two versions of the Internet Protocol: IPv4 and IPv6 (IPv6). Pv4 is still in use today, however due to the Internet's rapid growth and IP address scarcity, a new version of Internet Protocol was created.

Each node should have its own address while being accessed, and this address should be different for each node as there will be hundreds of them. The node should have its own, distinct IP address because if it shares an IP address, the node may experience numerous security issues. This renders the node immune to attack, and a distinct IP address adds an extra degree of security and reliability.

An internet network is identified by its network address. This allows us to determine the network's address range and the total number of hosts that could be there.

The mask, a 32-bit binary value, provides the network address in the address block when the AND bitwise operation is done to it and any IP address in the block.

For various classes, the default mask is:

Type A: 255.0.0.0

255.255.0.0 for Class B

Type C: 255.255.255.0

Subnetting: A big block of addresses is divided into numerous contiguous sub-blocks by the process of subnetting, and these sub-blocks are then assigned to several smaller networks. This practise is frequent when classless addressing is used.

We utilise classless IP address with a subnet mask of 255.255.255.0 in our topology. Prior to pinging the packet transfer, this addressing is completed.

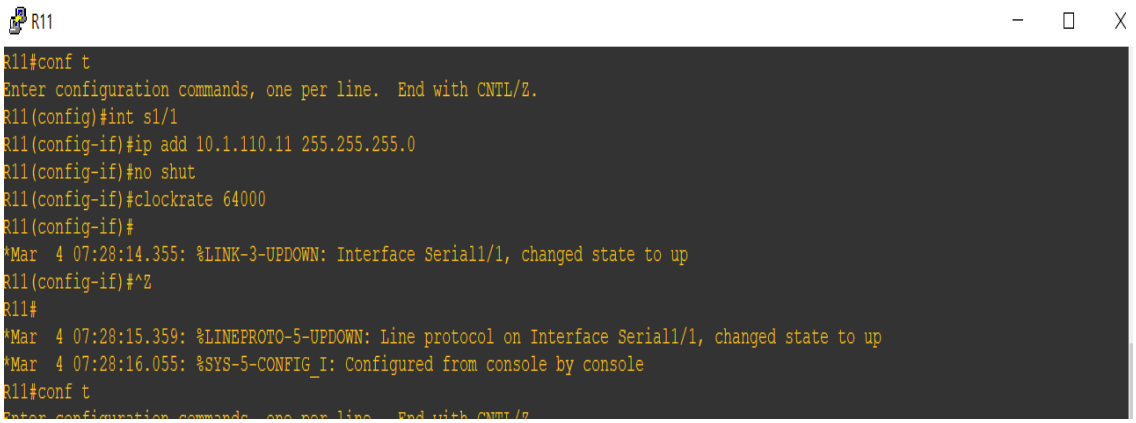

Fig. 3.1 IP address with subnet masking

Figure 3.10 shows assigning of IP address and its subnet masking for the nodes of the router each sub-block ranges from 0-255.

3.2 Intra-Body Network

In this project, we have established IGPs - OSPF on each node to dynamically route the packets between each and every router at the nodes. Each BAN on a human body is thought of as an autonomous/independent network. The Dijkstra algorithm and the link-state routing protocol are used by OSPF to determine the best path between any two nodes for communication. The logical subdivision of the network is made possible by the classless and hierarchical architecture of OSPF, which has a provision for dividing the BAN into logical areas. The OSPF implementation on intra-BAN as the dynamic routing protocol is shown in Figure 3.3.

Figure 3.2 shows the block diagram of intra-BAN network running on OSPF routing protocol this constitutes a single autonomous system.

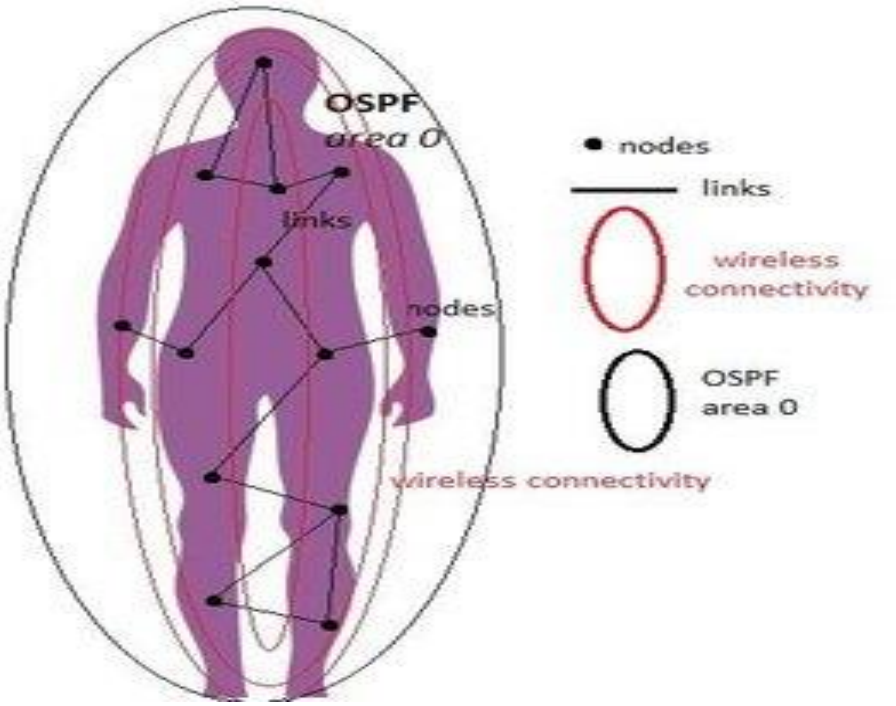

Fig. 3.2shows the intra-BAN.

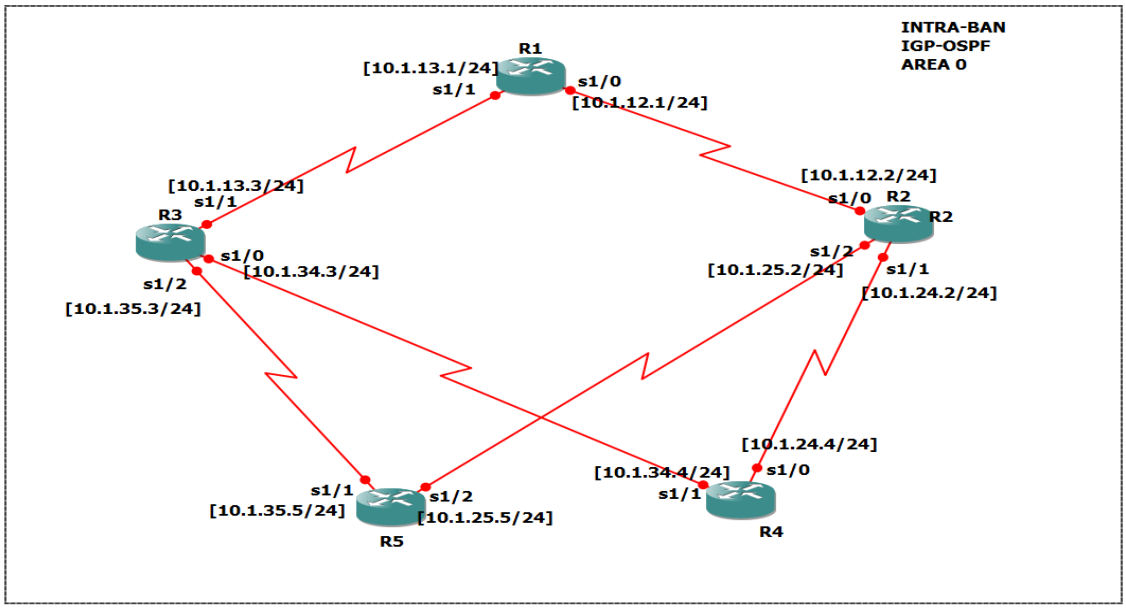

Fig. 3.3 Implementation of OSPF on intra-BAN network

Configure the nodes and interface the slots of the router by providing IP address and clock rate for each node. Applied the slot of PA-4T+, this enables the router to make 4 virtual connections.

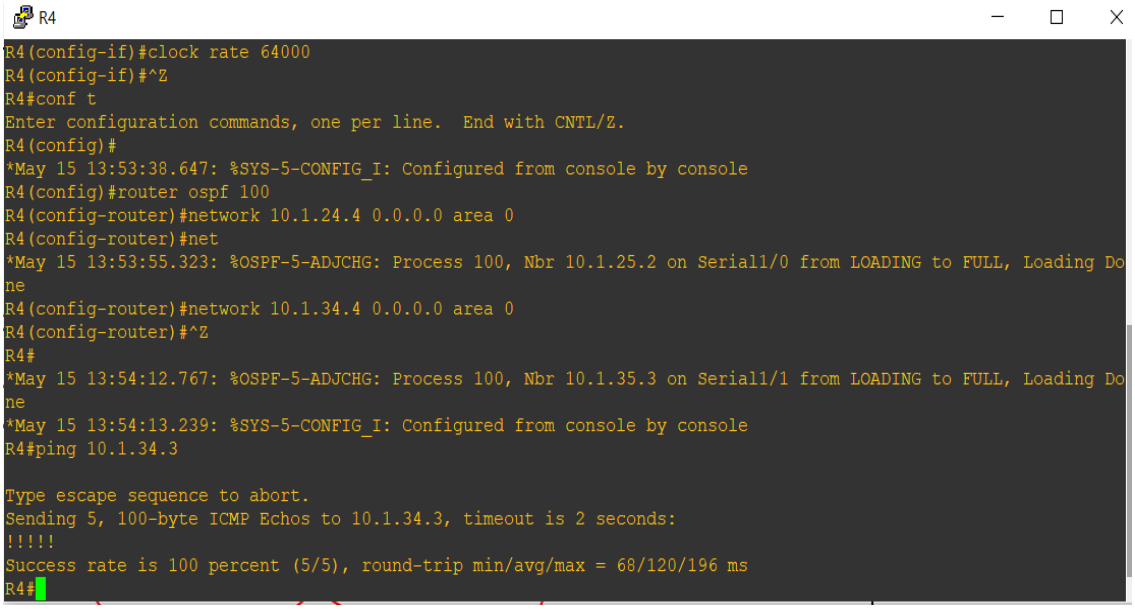

Fig. 3.4 Packet sending in intra-BAN network

Packet sent in intra-BAN network through the routers with the success rate of 100 percent is shown in Figure 3.4.

3. 3 Inter-Body Network

Inter-BAN, also known as inter body communication, is a networking model in which communication occurs between two autonomous bodies that run their own internal dynamic routing protocols and are connected to each other by means of Virtual-Links. This is in contrast to intra body area networks, which function as autonomous systems. Three-way handshaking is the only method that allows for this communication. The block diagram and network topology of inter-BAN are shown in Figure 3.4. EIGRP's inter-BAN network implementation is shown in Figure 3.5. On a computer network, EIGRP is a sophisticated distance-vector routing protocol used to automate routing configuration and decisions. Figure 3.6 shows the use of Virtual-Link to link area 1 to area 0.

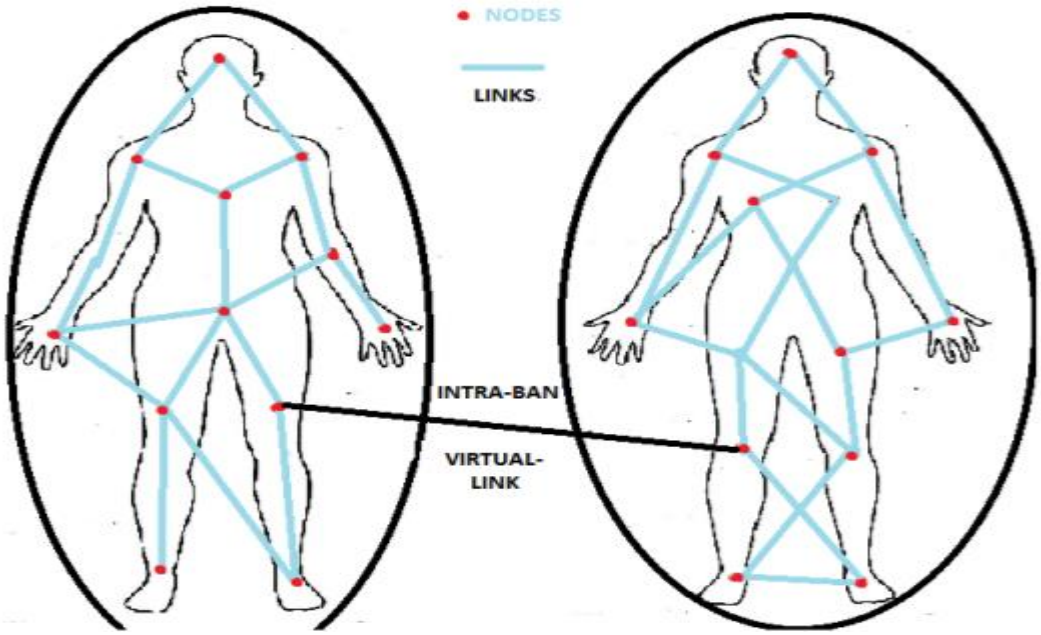

Fig. 3.5 Block diagram/Network topology of inter-BAN

3. 3.1 Inter-BAN communication with systems using same routing protocols

To connect a non-backbone location to a backbone area, virtual links can be employed. Area border routers make virtual links with one another. In the network below the two autonomous systems are with the EIGRP routing protocol hence only a virtual link is enough to make communication between them. As both the systems are of same EIGRP routing protocol it is easy for them to communicate between them without any translator. For example 2 people communicating with a same language and they doesn't need any translator.

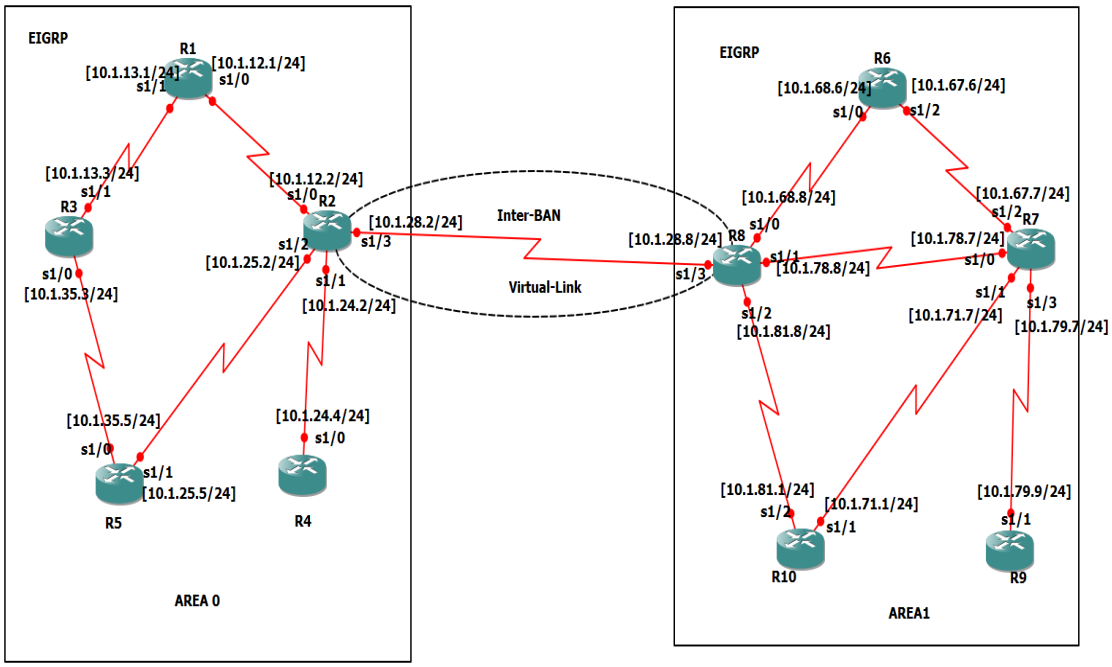

Fig. 3.6 Implementation of EIGRP network on inter-BAN network through virtual-link

Figure 3.7 shows the packet sending within the autonomous system and in between the autonomous system through the virtual link and the EIGRP routing protocol with the success rate of 100 percent. This is for the inter network which are using same routing protocols but the systems using different routing protocols will be dealt differently.

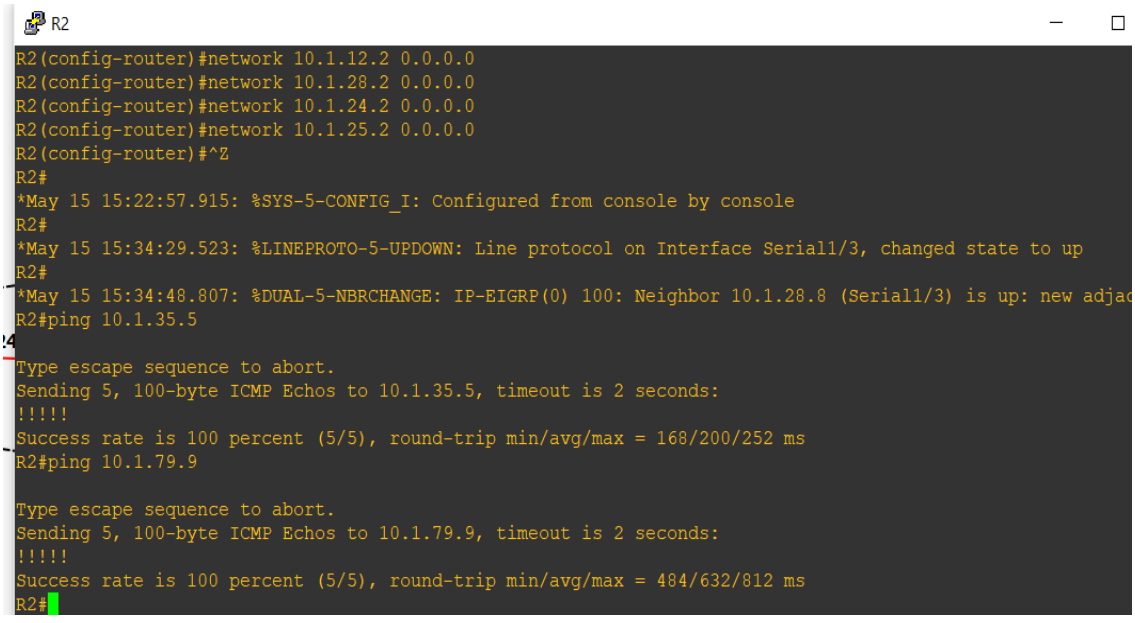

Fig. 3.7 Packet sending in inter-BAN network

3. 3.2 Inter-BAN communication with systems using different routing protocols

Two systems using different routing protocols cannot communicate with each other directly with a virtual link instead there is a need for an extra device. In our topology that extra device is the redistribution router. Network routes are imported and exported during redistribution from one routing protocol (or static routing) to another during networking. As an illustration, consider a router that can import network routes from OSPF into EIGRP and vice versa.

In Figure 3.8 router name R11 is the redistribution router that redistribute between OSPF routing protocol and EIGRP routing protocol. The redistribution works on the metric of the routing protocols. OSPF utilises cost as the value of the measure and calculates costs using a preset reference bandwidth of 100 Mbps. EIGRP metric updates contain 5 metrics, minimum bandwidth (default B=100000 Kbit/sec), delay (default D=100 micro sec), load (default L (tx/rx) =1), reliability (default R=255), maximum transmission unit (MTU) (default M=1500 bytes).

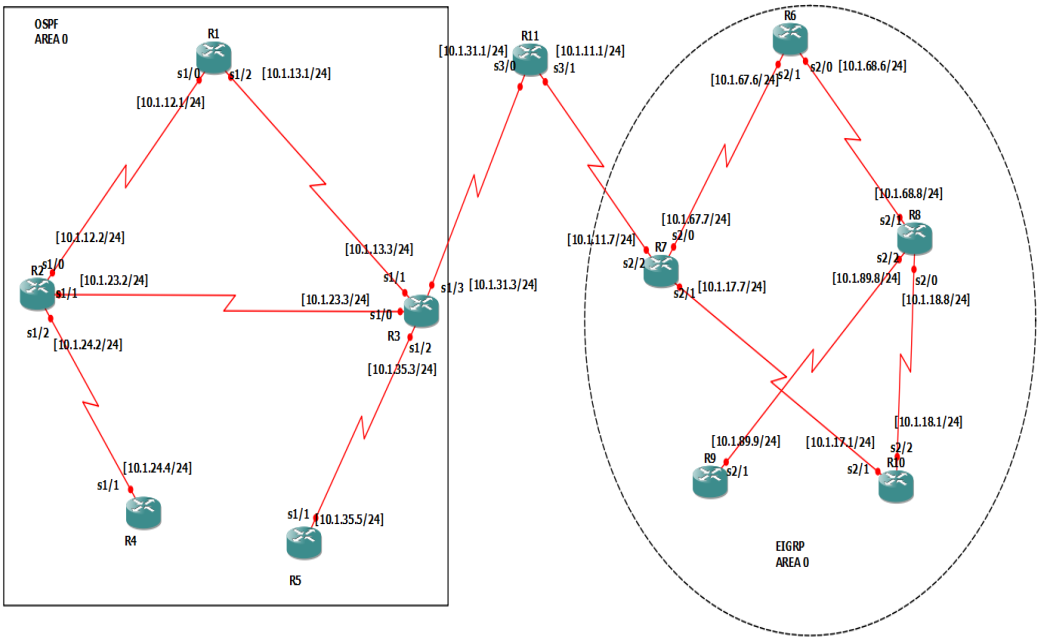

Fig. 3.8

Implementation of inter-BAN network of OSPF and EIGRP routing protocol using redistribution

The above figure shows the topology of inter-BAN network with different routing protocols.

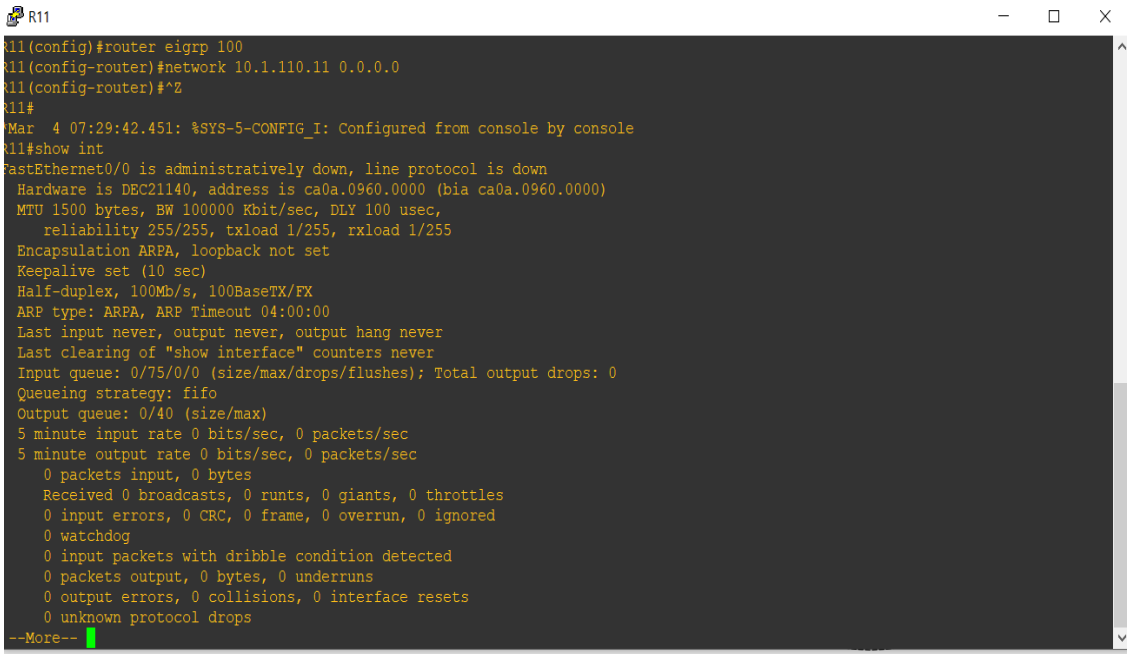

Fig. 3.9 Parameters of router redistribution for constructing the metric

The parameters in the Figure 3.8 is used by the routing protocols for calculating the cost and metric for efficient route choosing.

Redistribution is of two ways

- The practise of transferring routing information from one routing protocol or domain to another without doing so in the other direction is known as one-way route redistribution.To offer connectivity, static or default routes are needed in the other way.
- Redistribution of routing data in both directions, from one routing protocol or domain to another, is known as two-way route redistribution. Because all routing data is exchanged between two entities, static or default routes are not necessary.

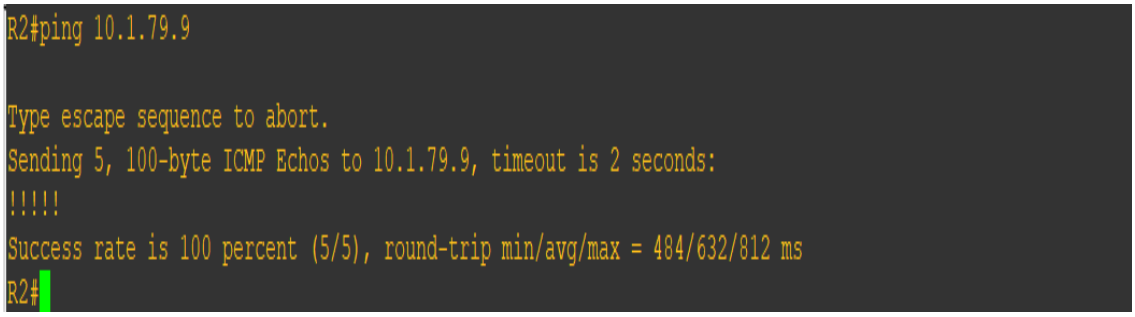

Fig. 3.10 Packet sent through the redistribution router

The above packet sent output is through OSPF and EIGRP redistributed with the success rate of 100 percent. By implementing the topology shown in Figure 3.8 we can communicate or send packets between any routing protocols just by knowing their metric.

3. 4 Security in Topology

We add security to the topology by including a password. A CISCO router can only be accessed with a password. The console line and virtual terminal lines both accept passwords.

On a network where the router needs to be accessible by several persons, a console password is helpful. The router is inaccessible to anyone who are not authorised. As a result, it stops unauthorised individuals from using the router. In Figure 3.11, the console password configuration is displayed.

CISCO router console password configuration:

1. Switch the C.I,S.C.O router into global configuration mode.
2. Connect the command line of the router to 0.
3. Use password command to enter the password. For instance, the command would be password cisco if you wanted to enter the password "cisco".
4. Finally, enter the login command.

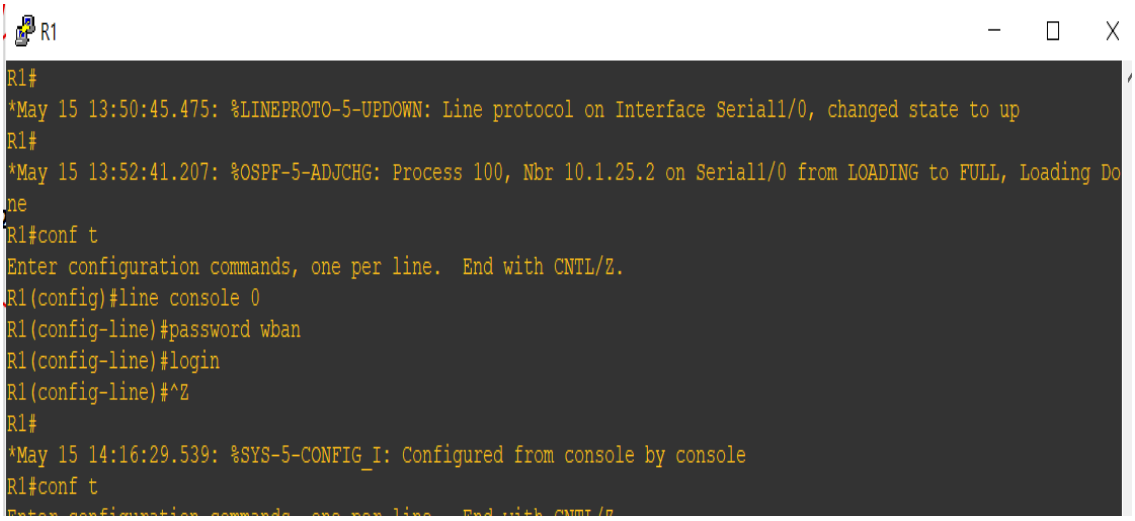

Fig. 3.11 Configuring console password

Telnet password is referred to as the virtual terminal password. You may get into the router and make any changes using telnet. Therefore, it's crucial to secure telnet usage by providing a strong password. As seen in Figure 3.11, this is how it's done.

Different hardware has varying numbers of designated VTY lines. Cisco offers vty lines in the 0 to 4 range. It indicates that there are 5 virtual telephone lines. The steps listed below can be used to establish the vty lines' passwords:

1. Switch the CISCO router into global configuration mode.
2. Connect the router's vty 0 to the command line.
3. Use the password command to enter the password. For instance, the command would be password cisco if you wanted to enter the password "cisco".
4. Finally, enter the login command.

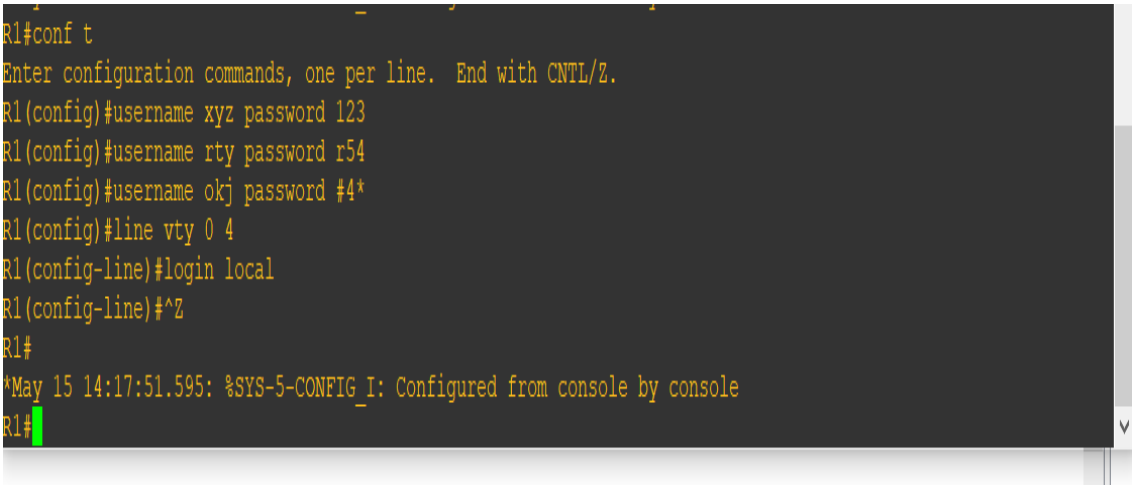

Fig. 3.12 Setting up password of vty lines

Over a TCP/IP network, Telnet is a protocol that enables connections to distant computers (also known as hosts) (such as the internet). Your computer's telnet client software allows you to connect to the telnet server. Your telnet client creates a virtual terminal once it connects to the remote host, opening up communication between your computer and the distant host.You'll typically need to log into the remote host, which calls for a user account on that system. It's possible to sign in occasionally without creating an account as a visitor or public.

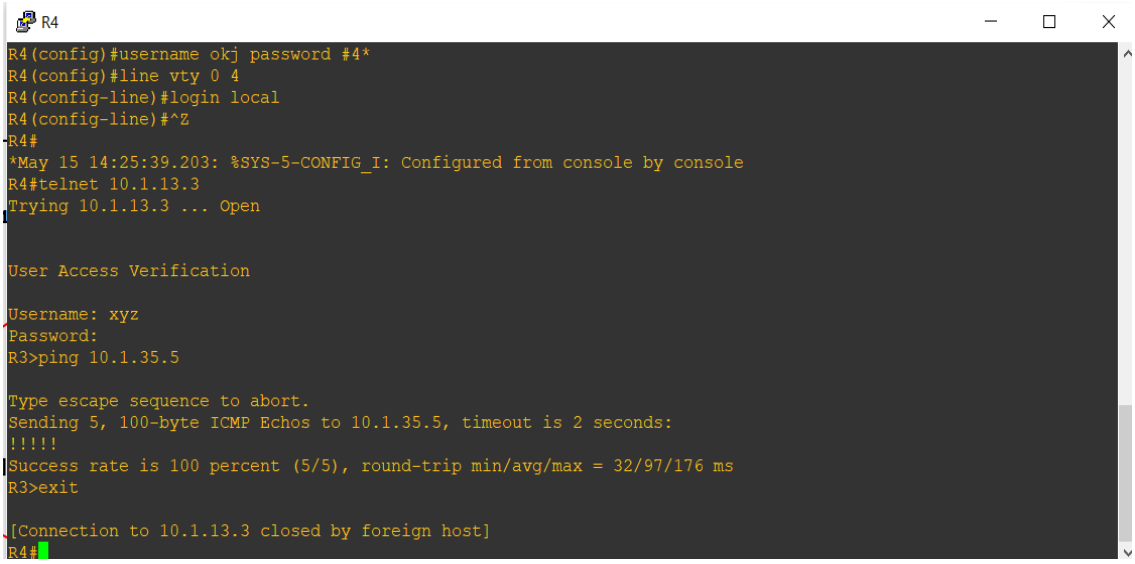

Fig. 3.13 remote accessing the node using telnet protocol

In the above Figure the router R3 is remote accessed from the R4 router and packets are sent from R3 with success rate of 100 percent.

3.5 Backup network

Backup network in the topology is implemented with RIP protocol. If any of the link in the topology is lost or damaged the data is sent to the desired destination through this backup network.

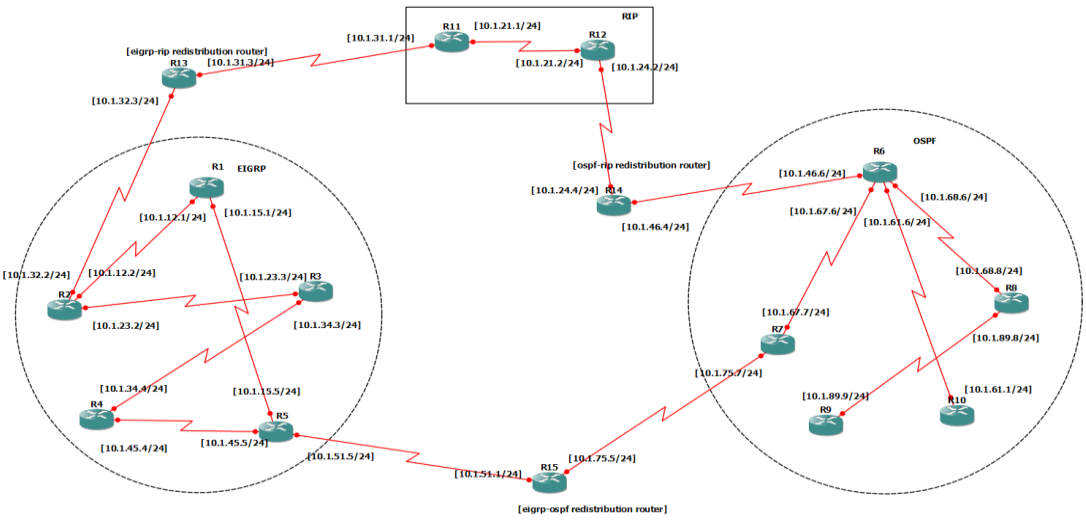

Fig. 3.14 Topology with Backup network

The above topology consists of an intra-body network which is implemented with EIGRP and OSPF routing protocols. The inter-body communication is established by using a redistribution router that imports and exports RIP to OSPF and vice versa, OSPF to EIGRP and vice versa, RIP to EIGRP and vice versa.

Each console line and virtual terminal is protected by password and the nodes are remote accessed by telnet protocol.

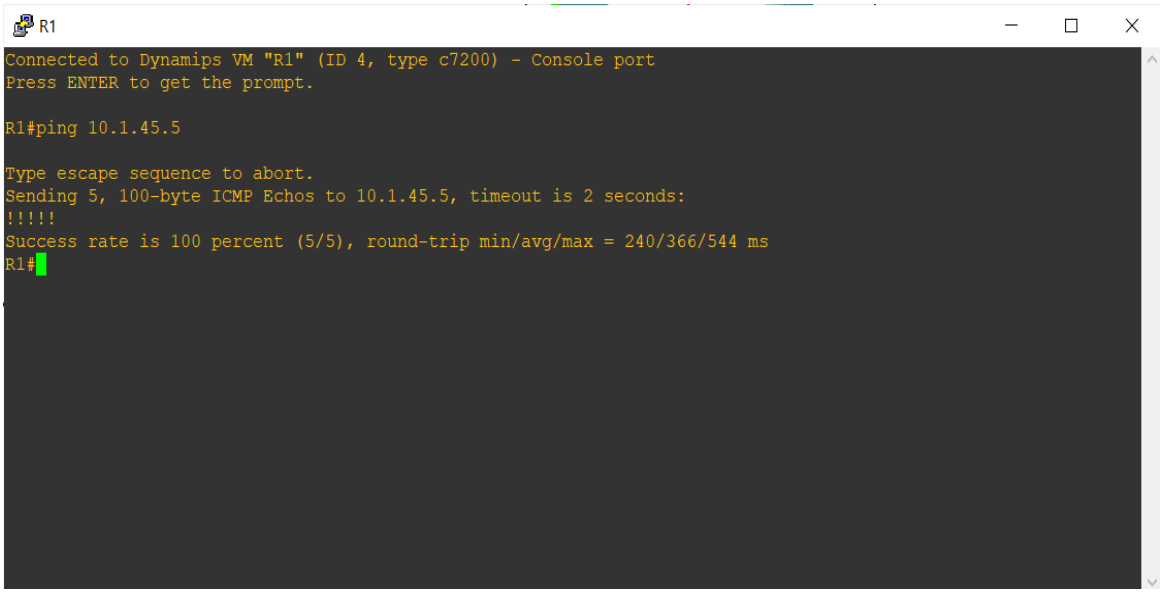

Fig. 3.15 Packet tracing at interbody network

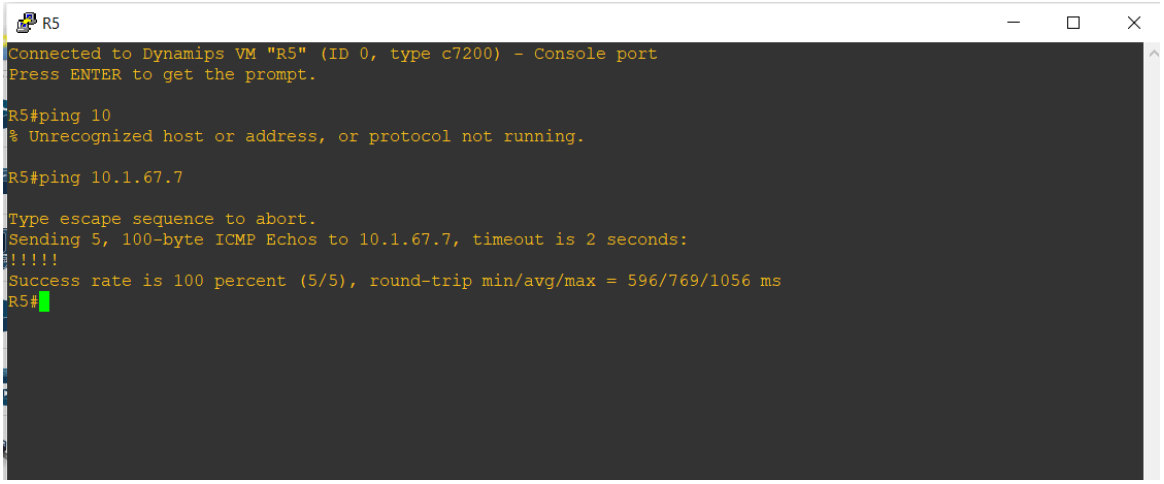

Fig. 3.16 Packet tracing at intrabody network using redistribution router

Figure 3.14 and 3.15 shows the result of the topology that used redistribution router and the backup network this backup network is used to send data packets when any of the link looses connection.

CHAPTER 5

RESULT

Packet sent with the success rate of 100 percent and using of RIP, OSPF, EIGRP and TELNET protocols, connection is made within the autonomous system, between the autonomous systems and to the remote router. Communication is verified, packets are traced all these results are shown and analysed in the previous chapter in detail.

4.1 Applications

- Monitoring the health.
- Training in military.
- Sport's training.
- Interaction gaming, and
- Sharing of the personal data.

4.2 Advantages

- Location independent monitoring.
- Can be used when involves many autonomous system with different protocols.
- In patient monitoring it has increased mobility due to use of portable electronic devices.
- Assists communication between individual and machine.
- Information is shared with privacy and security.

CHAPTER 6

SUMMARY AND FUTURE PERSPECTIVE

5.1 Summary

We gave a quick summary of the existing WBAN suggestions and potential applications in this project.Four design challenges have been tackled: network architecture, security, packet tracing and connectivity. It would be a failure on the part of researchers to see physical connections like wires or foils running all round the body. A high impedance shoe is essential in situations where electrons flow through the body and carry the information/data. The human body functions as a short to the passage of charges in the body and is a very excellent conductor of electricity. A very good alternative for the above is the wireless Body Area Network. The transmission and reception of data takes place within the circumference of a body (an AS) or between two or more AS. The former is called Intra-AS Communication and the latter is called Inter-AS communication. We have adopted a wireless data routing and sharing system using various protocols that suits the present technological scenario.

A complex network made up of sensors at nodes that are built to function independently and link to different additional sensors and equipment Controlled redundancy in the network and load balancing. Effective dynamic routing protocols on routers. Static routing and tunnels configured wherever necessary.

To increase the network and infrastructure's security, the method may be used in conjunction with other security tools including database activity monitoring, white listing, and data loss prevention. We have also employed a backup network that makes the communication on even in some connectivity problem.

5.2 Future Scope

Many improvements could be implemented to increase the security strength, increase these efficiency in serving the nation health monitoring of these mean by embedding various body sensors and encrypting the data between the nodes.

REFERENCES

1. Mahesh R Khairawadagi, Pooja Ganesh, Vanitha Raju, Nalini MK4, “Session Secured Attack Detection Scheme for Network Communication”,IJARCCE,Vol. 8, Issue 3, March 2019.
2. Vishesh S, Pradhyumna M, SuchitShavi, Sujaya HS, Suraj N, Kavya P Hathwar, “WBAN and Cloud Computing- 2”, IJARCCE, Vol. 6, Issue 11, November 2017.
3. Vishesh S, Hem Bhupaal Reddy M, Kavya A, “WBAN and Cloud Computing”, IJARCCE, Vol. 6, Issue 9, September 2017.
4. Vishesh S, MoulanaIzhar Ahmed, KarthikSrinivas, Srikrishna BS, Sukruth L Babu, Veeresh Kumar U, Sachin R, “BAN: intra-BAN and inter-BAN”, IJARCCE, Vol. 6, Issue 7, July 2017.
5. Muhammad Sheraz Arshad Malik, Muhammad Ahmed, Tahir Abdullah, NailaKousar, MehakNigar Shumaila, “Wireless Body Area Network Security and Privacy Issue in E-Healthcare”, IJACSA, Vol. 9, No. 4, 2018.
6. Muhammad Usman, Muhammad Rizwan Asghar, Imran Shafique Ansari, and Marwa Qaraqe, “Security in Wireless Body Area Networks: From In-Body to Off-Body Communications”, IEEE Access, DOI 10.1109/ACCESS.2018.2873825.
7. Rahat Ali Khan and Al-Sakib Khan Pathan, “The state-of-the-art wireless body area sensor networks: A survey”, International Journal of Distributed Sensor Networks 2018, Vol. 14(4).
8. Hassan J. Hassan, Noor Kadhim Hadi, Ali Kamal Taqi, “Implementation of Wireless Body Area Network Based Patient Monitoring System”, Journal of Information Engineering and Applications, Vol.8, No.4, 2018.
9. Khalid Awan, KashifNaseer Qureshi, Mehwish, “Wireless Body Area Networks Routing Protocols: A Review”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 4, No. 3, December 2016.
10. H. Fotouhi, A. Cauevic, K. Lundqvist, "Communication and Security in Health Monitoring Systems--A Review," in Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual, pp. 545-554, 2016