IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13927

Wireless Body Area Network (WBAN): Monitoring of Health of Army Personnel for Enhanced Security and Increased Life Expectancy

Digambar Dhanagar[1], Shailesh Umesh Khot[2], Vedant Kulkarni[3], Suraj Suresh[4]

Student, MSc (Computer Science), Scaler Neovarsity, Bangalore, India [1]

Student, B.Tech (Electronics and Telecommunication Engineering), India [2-3]

Student, BE, Department of ECE, Dayananda Sagar College of Engineering, Bangalore, India [4]

Abstract: Wireless Body Area Network (WBAN) is an emerging field of networking with the miniaturization of sensors, increase in Bandwidth (BW) of channels and high speed internetwork of connectivity, WBAN is gaining importance. Any biological stimulus from a human body is converted to an electrical signal to be standardized and is forwarded to the internetwork, an internetwork is a huge network of networks which consists of thousands or even millions of nodes and links. This work considers the realisation of a human body implanted with biomedical sensors, operating wireless protocols of variable frequency, and measuring more than one physiological parameter of the body. Various nodes that are linked together to form a network of biomedical or other sensors placed at the nodes make up a wireless body area network. The implementation and introduction of the intra-body network were covered in our earlier publication, "Realization of Wireless Body Area Network utilising GNS3 tool for Health Monitoring," which has the DOI 10.17148/IJARCCE.2018.7459. Army personnel who are located in remote locations need continuous monitoring of their health and the packets need to be sent to the base station. Each base station needs to be connected to the headquarters (HQ). Also the information needs to be authenticated and encrypted. Any leak in the information or any intrusion will lead to advantage for the enemy. In the project paper we concentrate on building a network, authenticating the network and encrypting the same, we make use of various routing protocols to find the best path and forecasting path between the sender and the receiver. OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) are preferred. We also incorporate 2-way Authentication for traffic. This setup enables healthcare providers to aggregate data from multiple patients, enhancing clinical decision-making and supporting collaborative care models. For instance, healthcare professionals can analyze aggregated data for research purposes, such as understanding trends in chronic disease prevalence.

Keywords: WBAN, internetwork, authentication, encryption, OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol).

I.INTRODUCTION

Wireless Body Area Network (WBAN) is a type of Body Area Network (BAN) classified based on the span of the network based on the span of the network, networks can be classified as:

1. BAN: Body Area Network
2. PAN: Personal Area Network
3. LAN: Local Area Network
4. MAN: Metropolitan Area Network
5. WAN: Wide Area Network

Body Area Network (BAN) is the lowest span among the above mentioned types of networks Figure 1 shows the Body Area Network with wireless connectivity. WBAN can be further classified into a body or inter-body depending on the movement of packets. An intrabody network is specific to a particular body whereas interbody network is between 2 or more intrabody networks. Figure 2 shows an intrabody network and figure 3 shows the interbody Network. [1]

DOI: 10.17148/IJARCCE.2024.13927

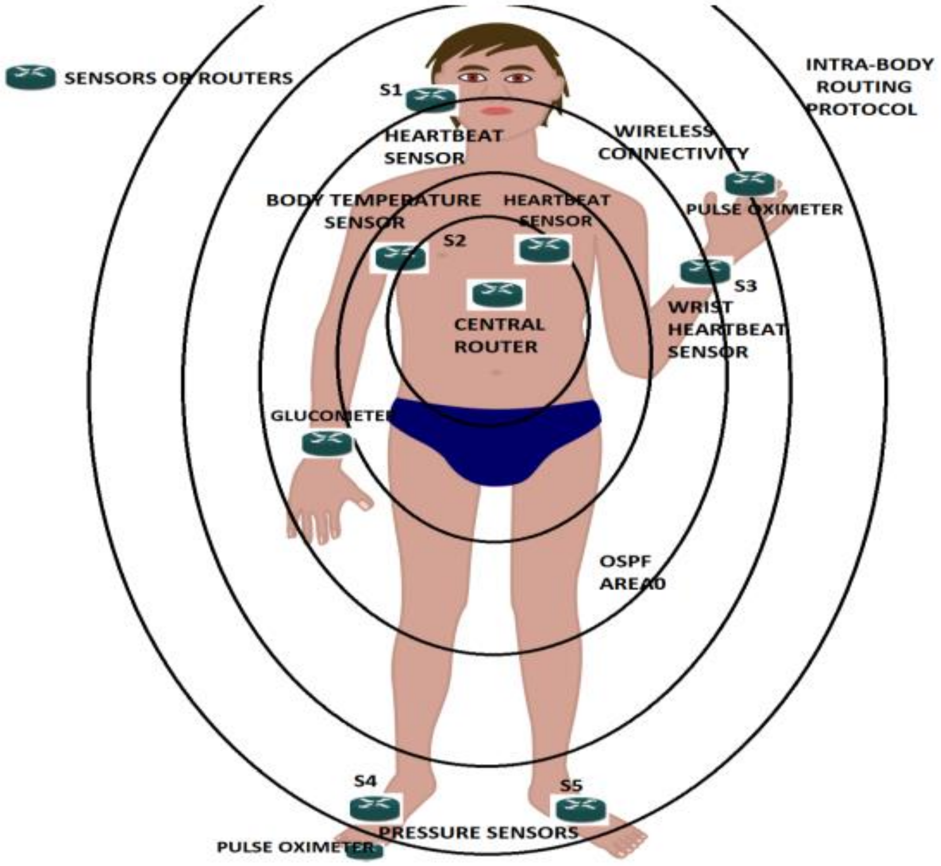


Figure 1 shows Body Area Network with wireless connectivity.

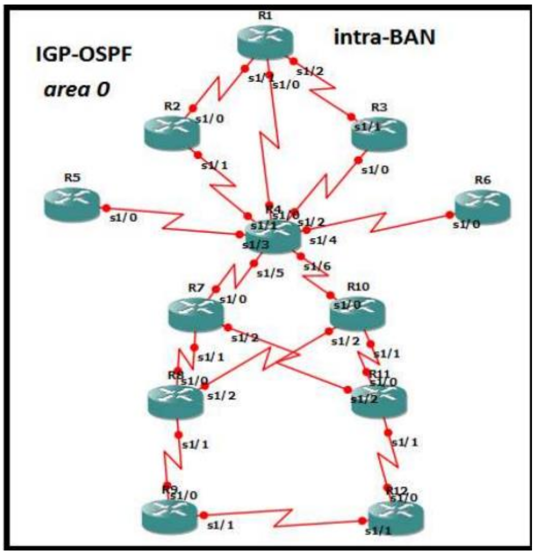


Figure 2 shows intrabody network belonging to BAN

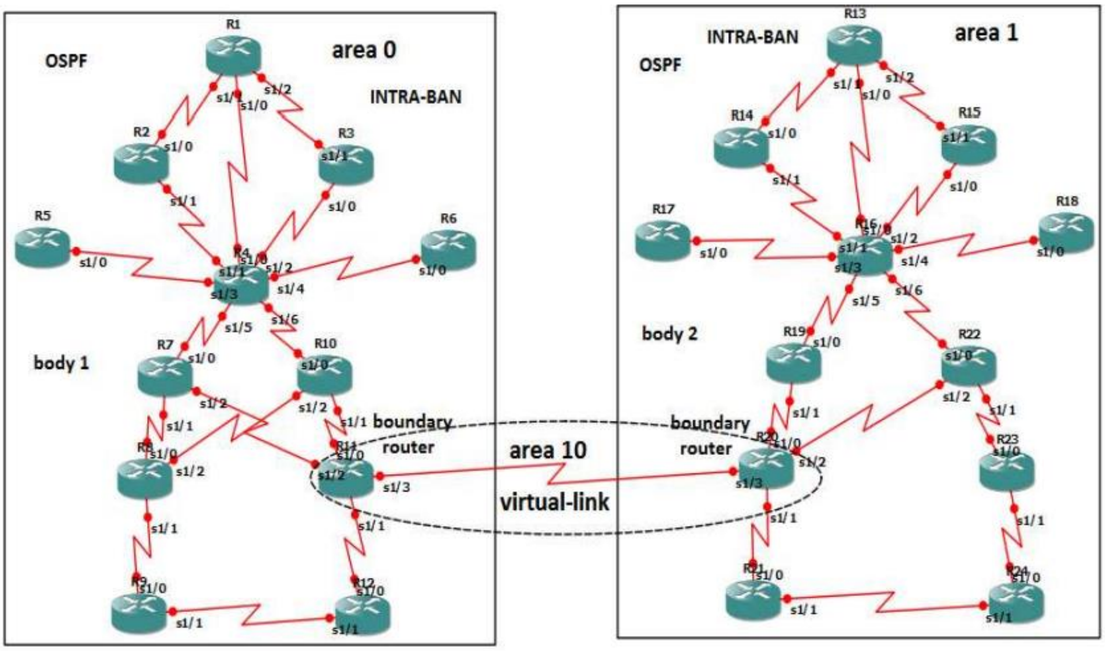


Figure 3 shows the interbody network belonging to BAN

II.MOTIVATION

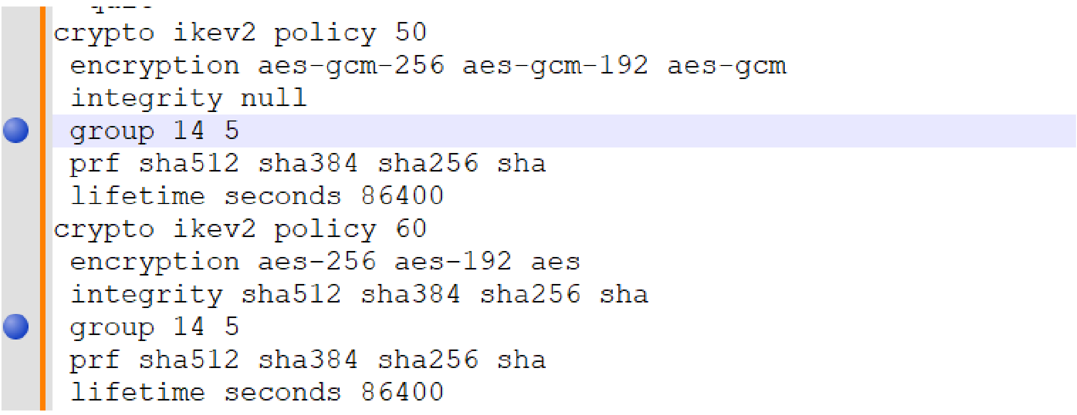
Health parameters of the army personnel is vital as they are located or posted to very high altitude or remote locations. Biological sensors can monitor the soldiers continuously with low power consumption, efficient routing protocols like OSPF and EIGRP can efficiently forward the package in the networks. Since military data is considered TOP-SECRET encryption algorithms can avoid misuse of data, 2-way authentication can prevent intrusion.[2]

III.OSPF PROTOCOL

Open Shortest Path First (OSPF) is a hierarchical routing protocol. It has a backbone area called area 0. Other than area 0 are called non-backbone areas. Due to the hierarchical nature of routing OSPF is best suited for routing in a Body Area Network. Since OSPF is a LSA protocol it is relatively slow compared to other modern routing protocols.

IV.EIGRP PROTOCOL

Enhanced Interior Gate way Routing Protocol (EIGRP) is relatively faster than OSPF protocol. EIGRP is a distance vector routing protocol and consumes less time, EIGRP uses Bandwidth (BW), delay, Reliability load and MTU (Maximum Transmission Unit) as its metrics to decide the best path between the networks based on specific requirements or conditions of the network. Figure 4 shows the encryption algorithms used the network, secure them from intruders. AES 256 algorithm was used for 256 bit encryption with integrity SHA-384. The features which the the new protocol offers and is also backward compatible with old IGRPs[3-4]



```
crypto ikev2 policy 50
 encryption aes-gcm-256 aes-gcm-192 aes-gcm
 integrity null
 group 14 5
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
crypto ikev2 policy 60
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 14 5
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

Figure 4 shows the encryption being done on the network.

DOI: 10.17148/IJARCCE.2024.13927

1. Support for Classless Inter-Domain Routing (CIDR) and variable length subnet masking. Routes are not summarized at the class full network boundary unless auto summary is enabled.
2. Support for load balancing on parallel links between sites.
3. The ability to use different authentication passwords at different times.
4. Sends topology changes, rather than sending the entire routing table when a route is changed.
5. Periodically checks if a route is available, and propagates routing changes to neighboring routers if any changes have occurred.
6. Backwards compatibility with the IGRP routing protocols.
7. Bandwidth: Minimum Bandwidth (in kilobits per second) along the path from router to destination network.
8. Load: Number in range 1 to 255; 255 being saturated
9. Total Delay: Delay, in 10s of microseconds, along the path from router to destination network
10. Reliability: Number in range 1 to 255; 255 being the most reliable.

V.3-WAY HANDSHAKING

This could also be seen as a way of how TCP connection is established. Before getting into the details, let us look at some basics. TCP stands for Transmission Control Protocol which indicates that it does something to control the transmission of the data in a reliable way. The process of communication between devices over the internet happens according to the current TCP/IP suite model (stripped out version of OSI reference model).

The Application layer is a top pile of stack of TCP/IP model from where network referenced application like web browser on the client side establishes connection with the server. From the application layer, the information is transferred to the transport layer where our topic comes into picture. The two important protocols of this layer are – TCP, UDP (User Datagram Protocol) out of which TCP is prevalent (since it provides reliability for the connection established). However you can find application of UDP in querying the DNS server to get the binary equivalent of the Domain Name used for the website. TCP provides reliable communication with something called Positive Acknowledgement with Re-transmission (PAR). The Protocol Data Unit (PDU) [4][5] of the transport layer is called segment. Now a device using PAR resend the data unit until it receives an acknowledgement. If the data unit received at the receiver's end is damaged (It checks the data with checksum functionality of the transport layer that is used for Error Detection), then receiver discards the segment. So the sender has to resend the data unit for which positive acknowledgement is not received. [6] You can realize from above mechanism that three segments are exchanged between sender (client) and receiver (server) for a reliable TCP connection to get established. Let us delve how this mechanism works:

- Step 1 (SYN) : In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with.
- Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with
- Step 3 (ACK) : In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start the actual data transfer

The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.[7-9]

Three-Way Handshake or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.

Three-way handshake process is designed in such a way that both ends help you to initiate, negotiate, and separate TCP socket connections at the same time.[10-11] It allows you to transfer multiple TCP socket connections in both directions at the same time.

- TCP 3-way handshake or three-way handshake or TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between server and client.
- Sync use to initiate and establish a connection
- ACK helps to confirm to the other side that it has received the SYN.
- SYN-ACK is a SYN message from local device and ACK of the earlier packet.
- FIN is used for terminating a connection.
- TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server
- In the first step, the client establishes a connection with a server

DOI: 10.17148/IJARCCE.2024.13927

- In this second step, the server responds to the client request with SYN-ACK signal set
- In this final step, the client acknowledges the response of the Server
- TCP automatically terminates the connection between two separate endpoints.

VI.IMPLEMENTATION AND DESIGN

A Wireless Body Area Network (WBAN) connects independent nodes (e.g. sensors and actuators) that are situated in the clothes, on the body or under the skin of a person. The network typically expands over the whole human body and the nodes are connected through a wireless communication channel. According to the implementation, these nodes are placed in a star or multihop topology. A WBAN offers many promising new applications in the area of remote health monitoring, home/health care, medicine, multimedia, sports and many other, all of which make advantage of the unconstrained freedom of movement a WBAN offers. In the medical field, for example, a patient can be equipped with a wireless body area network consisting of sensors that constantly measure specific biological functions, such as temperature, blood pressure, heart rate, electrocardiogram (ECG), respiration, etc. The advantage is that the patient doesn't have to stay in bed, but can move freely across the room and even leave the hospital for a while. This improves the quality of life for the patient and reduces hospital costs. In addition, data collected over a longer period and in the natural environment of the patient, offers more useful information, allowing for a more accurate and sometimes even faster diagnosis. [10]

The classification of a network based on span or range of the network is also an indicator of the complexity of the network as a whole. The Body Area Network (BAN) is one such classification, though its span is restricted to the circumference of the human body wearing it, its complexity in architecture demands serious network build-up and troubleshooting. Open Shortest Path Fast (OSPF) protocol, which is a dynamic routing protocol provides a serious platform for network convergence in case of change in network topology. An OSPF network can be divided into subdomains called areas. An area is a logical connection of OSPF networks, EIGRP networks, RIP networks, routers, switches and links that have the same area identification. The network runs on set of rules called protocols. A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.

You can think of a protocol as a spoken language. Each language has its own rules and vocabulary. If two people share the same language, they can communicate effectively. Similarly, if two hardware devices support the same protocol, they can communicate with each other, regardless of the manufacturer or type of device. Protocols exist for several different applications. Examples include wired networking (e.g., Ethernet), wireless networking (e.g., 802.11ac), and Internet communication (e.g., IP). The Internet protocol suite, which is used for transmitting data over the Internet, contains dozens of protocols. These protocols may be broken up into four categories: [12]

1. Link layer - PPP, DSL, Wi-Fi, etc.
2. Internet layer - IPv4, IPv6, etc.
3. Transport layer - TCP, UDP, etc.
4. Application layer - HTTP, IMAP, FTP, etc.

Link layer protocols establish communication between devices at a hardware level. In order to transmit data from one device to another, each device's hardware must support the same link layer protocol. Internet layer protocols are used to initiate data transfers and route them over the Internet. Transport layer protocols define how packets are sent, received, and confirmed. Application layer protocols contain commands for specific applications. For example, a web browser uses HTTPS to securely download the contents of a webpage from a web server. An email client uses SMTP to send email messages through a mail server. There is a need for a separate internetwork for various application. It must be capable of easily exchanging confidential and other miscellaneous data. With the rapid advancements and interconnectivity of information and communication technologies (ICT), it is no surprise that ICT form the backbone of many aspects of the industry these days. These networks are subject to more stringent scrutiny, in comparison to traditional networks, due to the sensitivity of information and the number and diversity of devices that could potentially be exploited to target the system. Cyber threats cannot be ignored when it comes to wireless and mobile devices exchanging TOP-SECRET information of the army. In this paper we realize a network consisting of intra-body and inter-body communication network. Each body is considered to be an Autonomous System (AS) capable of mobility and connectivity to every other Autonomous System (AS) with different Autonomous System Number (ASN). This network when connected and tested would enable exchange of confidential and essential data. The information in the network to be transmitted through the nodes with each node password protected. This would avoid the intruders from stealing data/information. GNS 3 tool is used for implementing routing and security on the network. [13][14]

DOI: 10.17148/IJARCCE.2024.13927

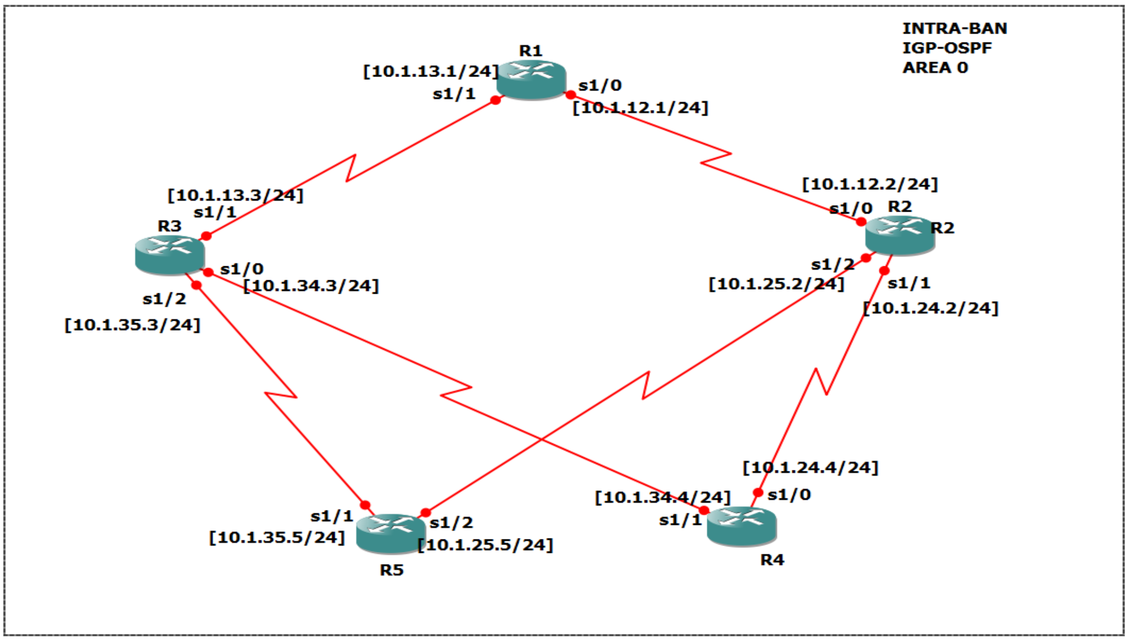


Figure 5 shows implementation of intraban on wireless network using IP addressing scheme.

VII.BACKUP NETWORK

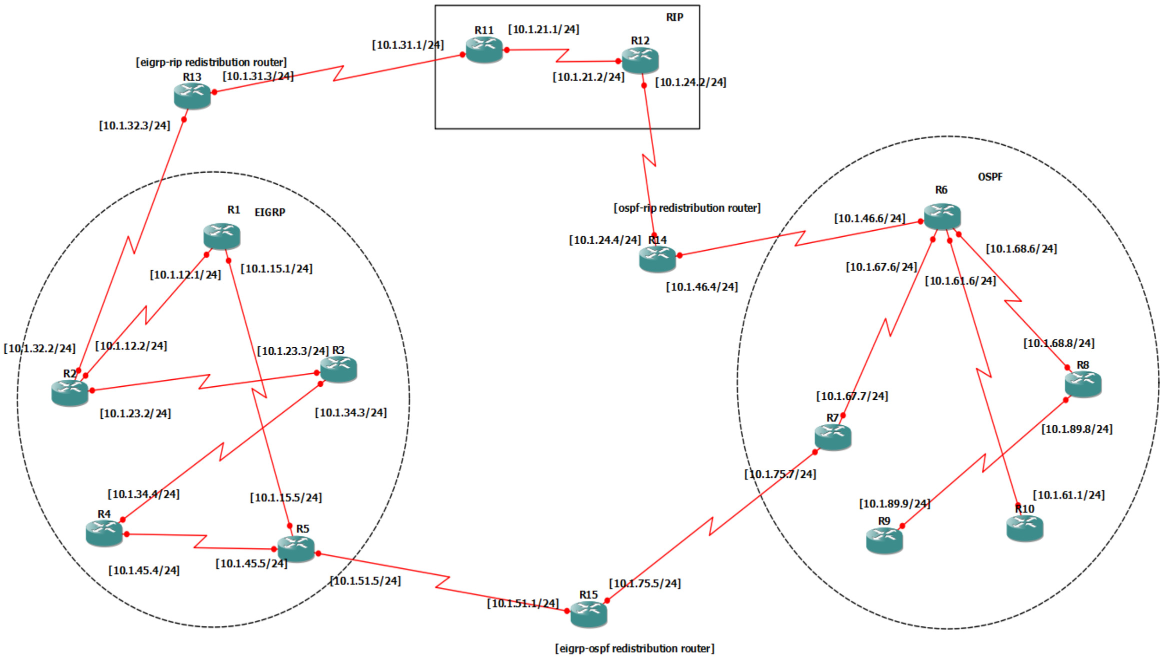


Figure 6 shows the backup network

Current and emerging communication and computing networks are expected to provide high reliability by achieving near-instantaneous restoration in the event that one or more network elements fail. This requires that network restoration plans be put in place such that in the event of failures, the network can immediately adjust, regroup, and/or revert to an alternative arrangement, usually in terms of a reroute, to continue and complete the given communication task [1]. Hence, developing network restoration models to cater for sudden failures, thereby improving the efficiency and reliability of our telecommunications and computing networks, is an imperative. Network (or routing) restoration (or recovery) is the field that describes the design and implementation of appropriate mechanisms and/or models for achieving desirable network reliability by creating proper backup plans for networks in the event of preconceived or unexpected failures [2]. The main goal of network restoration is to seek to instantaneously make available new routes

DOI: 10.17148/IJARCCE.2024.13927

once one or more network elements (e.g., links or nodes) fail, thereby avoiding disruption to network traffic. [5] The new routes are usually either computed immediately at the point of failure or are usually preplanned even before such failure occurs. Generally, in research works that involve developing appropriate network restoration mechanisms for protection against failures, several factors have to be put into consideration. The most important factors are the cost of network infrastructure, length of rerouting paths, amount of the total capacity that has to be reserved for restoration or recovery from failure, and the time taken to achieve such network restoration. The design goal is always to achieve optimal productivity for the network with as much less resource and cost as possible over the shortest amount of time.

VIII.PHYSIOLOGICAL PARAMETERS

- **Pulse -** Pulse of the soldiers needs to be monitored, pulse is a clear indicator of circulation in the body. The heart beats 72 times a minute and is considered as normal pulse rate, anything in between 60-100 is also considered normal.
- **Spo$_2$-** The oxygen levels in the blood needs to be monitored continuously. Spo2 also called as the oxygen saturation, it is a simple and non-invasive method of measuring blood oxygen.
- **Glucose Monitoring: -** It measures the blood glycemic values, it is an invasive method of measuring blood glucose levels, Lower the glucose level, the soldier is likely to perform weak. By measuring the parameters continuously immediate food supply, medicine and liquid can be sent from time to time.
- **Body Temperature: -** Body temperature measurement is essential. An optimum body temperature has to be maintained. The cell enzymes needs to have optimum body temperature to catalyse chemical reaction. In case the thermo-regulation does not take place, medicine are needed to be supplied.

IX.APPLICATIONS

Wireless Body Area Networks (WBANs) have several promising applications in defense, enhancing the capabilities of military personnel and operations. Here are some key applications:

1. Health Monitoring: WBANs can continuously monitor soldiers' vital signs (heart rate, temperature, etc.) in real-time, allowing for immediate medical responses and improving battlefield medicine.
2. Situational Awareness: Integrating sensors that monitor environmental conditions (such as toxic gas detection) enhances situational awareness, helping troops respond effectively to threats.
3. Data Communication: WBANs facilitate secure and efficient communication between soldiers and command centers, ensuring timely information sharing and coordination during missions.
4. Performance Tracking: Wearable sensors can track soldiers' physical performance and fatigue levels, optimizing training and mission planning based on their readiness.
5. Enhanced Combat Effectiveness: By providing real-time data on troop movements and health, commanders can make better tactical decisions, potentially reducing casualties.
6. Search and Rescue Operations: WBANs can aid in locating soldiers who are injured or lost in combat scenarios by providing location data and health status.
7. Augmented Reality Integration: Wearable devices can integrate with AR systems to provide soldiers with enhanced visual information, improving navigation and threat detection.
8. Logistics and Supply Chain Management: Tracking soldiers' health and performance can inform logistics decisions, ensuring that resources are allocated effectively.

These applications contribute to improving the effectiveness, safety, and overall performance of military operations.

X.CONCLUSIONS AND FUTURE SCOPE

A noble experimental approach to interconnecting remotely deployed army personnel for their continuous and rigorous health tracking with the base station or Head Quarters (HQ) was established using OSPGF and EIGRP routing protocols. 2-way authentication was done on the network. Encryption algorithm AES-256 with integrity SHA-384 was deployed to encrypt data. Deployed in a central server that calculates node trust levels and identifies malicious nodes. To further improve network and infrastructure security, the method may be used in conjunction with additional security measures including white listing, database activity monitoring, and data loss prevention. In order to protect the node from the compromised attacker, session-based encryption is employed. The attacker's request will be approved by the particular node validation process's unique key. By doing this, the hackers would be prevented from taking TOP-SECRET data or information. In addition to these, multi-factor authentication (MFA) can be employed to fortify identity verification, requiring users to authenticate using multiple factors such as passwords, biometric data, or one-time passcodes. This limits access even if credentials are compromised, preventing attackers from gaining unauthorized entry into the network. Another critical aspect is network segmentation. By dividing the network into smaller, isolated segments, the blast radius of potential breaches can be minimized. Even if an attacker gains access to one part of the network, they are restricted from moving laterally to access more sensitive areas, thus containing the scope of an intrusion. In order to protect individual nodes from being compromised, session-based encryption is employed. Each communication session between nodes is encrypted uniquely, ensuring that even if an attacker intercepts the data, they would be unable to decipher it without the correct decryption key. This prevents eavesdropping and data tampering, securing the integrity of the transmission. Moreover, every request made by an entity must pass through a node validation process that uses a unique key for each node. This key ensures that only authorized and verified requests are processed, filtering out any malicious requests that do not meet the validation criteria. By doing so, hackers are prevented from injecting malicious traffic or gaining access to restricted areas of the network. To enhance protection, intrusion detection and prevention systems (IDPS) can be integrated to monitor network traffic for malicious activity and take action in real time. These systems not only detect threats but can also automatically block suspicious activities or alert security teams to take swift action. Additionally, employing threat intelligence services allows for proactive defense by integrating real-time threat data from external sources. This helps to recognize evolving attack patterns and vulnerabilities, allowing the security team to stay ahead of potential threats. In the event of an attack, a robust incident response plan is essential. This plan ensures that in the case of a breach, the organization can quickly contain the threat, minimize damage, and recover operations efficiently. Regular penetration testing and vulnerability assessments should be conducted to continuously evaluate the security posture of the system and address any weaknesses before they can be exploited.

REFERENCES

[1] Route Redistribution-A Case Study - ijarcce- www.ijarcce.com/upload/2017/june-17/IJARCCE%2042.pdf
[2] Open Shortest Path First- A Case Study - ijarcce- www.ijarcce.com/upload/2017/june-17/IJARCCE%2096.pdf
[3] Conceptual Study of Wireless BAN using Bluetooth/IEEE 802.11n - DOI-10.17148/IJARCCE.2016.51184
[4]Open Shortest Path First (OSPF) Routing Protocol and the Use of Virtual-LinksDOI10.17148/IJARCCE.2017.6733-http://www.ijarcce.com/upload/2017/july-17/IJARCCE%2033.pdf
[5] Mahesh R Khairawadagi, Pooja Ganesh, Vanitha Raju, Nalini MK4, "Session Secured Attack Detection Scheme for Network Communication",IJARCCE,Vol. 8, Issue 3, March 2019.
[6] Vishesh S, Pradhyumna M, SuchitShavi, Sujaya HS, Suraj N, Kavya P Hathwar, "WBAN and Cloud Computing2", IJARCCE, Vol. 6, Issue 11, November 2017.
[7] Vishesh S, Hem Bhupaal Reddy M, Kavya A, "WBAN and Cloud Computing", IJARCCE, Vol. 6, Issue 9, September 2017.
[8] 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.
[9] 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.
[10] 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.
[11] 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).
[12] 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.
[13] 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.
[14] 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.