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. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14227

Secured Wireless Body Area Network (WBAN) for Physiological Parameter Sensing for Military Personnel with AI: Podiatric Gait Analysis

Shashwitha Puttaswamy[1], Vishesh S[2]

Research Scientist[1]

Research Head, Konigtronics Pvt Ltd[2]

Abstract: As sensors become smaller, channel bandwidth (BW) increases, and internet connectivity speeds increase, Wireless Body Area Networks, or WBANs, are becoming more and more significant. An internetwork is a vast network of networks with thousands or even millions of nodes and links. Any biological stimulus from the human body is transformed into an electrical signal, standardized, and sent to the internetwork. This study examines the possibility of a human body implanted with biomedical sensors that measure many physiological parameters and run wireless protocols with various frequencies. This study examines the possibility of a human body implanted with biomedical sensors that measure many physiological parameters and run wireless protocols with various frequencies. A wireless body area network is made up of a number of nodes that are connected to one another to create a network of biomedical or other sensors positioned at the nodes. Military personnel stationed in remote areas require constant health monitoring, and the packets must be transmitted to the base station. The headquarters (HQ) must be connected to each base station. Additionally, the data must be encrypted and authorized. The enemy will get an advantage from any incursion or information breach. The research paper focuses on network construction, authentication, and encryption. To determine the optimal way and anticipate the path between the sender and the recipient, we employ specific routing protocols. EIGRP (Enhanced Interior Gateway Routing Protocol) and OSPF (Open Shortest Path First) are recommended. For traffic, we also use two-way authentication. By combining data from several patients, this configuration helps medical professionals make better clinical decisions and promote collaborative care models. To better understand trends in the prevalence of chronic diseases, for example, researchers might use aggregated data. Podiatric abnormalities due to improper gait of Army men with and without Diabetes Mellitus is also dealt with using Artificial Intelligence (AI) models developed using supervised classification algorithms- Support Vector Machine (SVM).

Keywords: Wireless Body Area Network (WBAN), internetwork, authentication, encryption, OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol), Podiatric abnormalities, improper gait, Diabetes Mellitus, Artificial Intelligence models (AI), Supervised Classification Algorithms, Support Vector Machine (SVM).

I.INTRODUCTION

The advent of Wireless Body Area Networks (WBANs) [1-4] has revolutionized the way we monitor health metrics, especially in environments where real-time monitoring is critical. WBANs are typically made up of small, low-power wireless sensors embedded in or worn on the body. These sensors continuously capture various biological parameters, such as heart rate, blood pressure, temperature, oxygen levels, foot pressures and glucose levels. The signals generated by these sensors are then converted into electrical signals, standardized, and transmitted to an external network, often through a gateway or base station. These networks are typically designed to provide continuous and real-time monitoring of an individual's physiological data, allowing healthcare professionals to intervene promptly when necessary. The miniaturization of sensors, the increase in bandwidth (BW) of communication channels, and the rapid advancement in high-speed internet connectivity are some of the key factors driving the development and adoption of WBANs. The next-generation WBANs are capable of supporting the simultaneous transmission of multiple physiological parameters from a subject, while ensuring low power consumption and minimal interference with the user's daily activities.

A. Role of Routing Protocols in WBAN

In a WBAN, data packets from multiple sensors are collected, transmitted, and routed efficiently to ensure reliable communication. With the complexity of networks and the possibility of real-time physiological data being transmitted over varying distances and environments, routing protocols become crucial.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14227

OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) are commonly used for their robustness, scalability, and ability to adapt to network changes:

1. OSPF is a link-state routing protocol that dynamically adjusts routing tables based on network topology changes. This is particularly useful in a WBAN environment where nodes (sensors) may come and go, or the network topology may change due to varying body positions or external interferences. OSPF's ability to provide the shortest path between nodes ensures minimal latency in transmitting critical health data.
2. EIGRP, an advanced distance-vector routing protocol, is known for its faster convergence and scalability. Its ability to find efficient paths even in larger, more complex networks helps maintain the reliability of data transmission in large WBAN systems.

Using these protocols together ensures the network is both resilient and responsive in real-time applications, such as monitoring military personnel, where any network downtime could have severe consequences.

B. Security and Privacy Concerns

As WBANs handle sensitive medical data, ensuring the confidentiality, integrity, and authenticity of the transmitted data is paramount. Data leaks or unauthorized access could lead to privacy violations or provide adversaries with critical health information. To mitigate these risks, your system must employ strong encryption and authentication protocols.

1. Two-Way Authentication: This authentication mechanism involves validating both the sender and the receiver of the data. This ensures that the data is only exchanged between trusted nodes, such as healthcare providers and authorized military personnel. By employing mutual authentication, the risk of unauthorized access is significantly reduced, protecting the privacy of the user and the integrity of the data.
2. Encryption: For confidentiality, it is essential that data be encrypted both during transmission and storage. This prevents potential attackers from intercepting sensitive health information. Common encryption techniques like AES (Advanced Encryption Standard) or TLS (Transport Layer Security) can be applied to ensure that the data remains unreadable to unauthorized entities.
3. Intrusion Detection and Prevention Systems (IDPS): Given the security concerns, the integration of IDPS helps detect and mitigate any malicious activity in the network, such as hacking attempts or unauthorized data access.
4. Secure Communication Channels: Using secure communication technologies such as VPNs (Virtual Private Networks), SSL/TLS tunnels, and WPA3 encryption in wireless communication can further ensure the safety of the data in WBANs. Implementing robust security protocols protects not only the individual's health data but also the overall integrity of the military network.

C. Application in Military and Remote Areas

The role of WBANs becomes even more critical in military operations, especially for army personnel stationed in remote areas. Soldiers engaged in combat or stationed in areas where access to healthcare services is limited require continuous health monitoring. WBANs can enable:

1. Real-Time Health Monitoring: Continuous monitoring of health parameters, including heart rate, blood oxygen levels, body temperature, and fatigue levels, is essential for soldiers who may be operating in extreme conditions or facing physical strain. Any abnormal readings can trigger immediate alerts to medics or base stations, enabling timely medical intervention.
2. Transmission to Base Stations and Headquarters: The sensors implanted in the soldier's body transmit data to a base station which aggregates the information and sends it securely to the headquarters (HQ) for analysis. This allows commanders and healthcare professionals to track the health status of soldiers across the battlefield or in remote camps, ensuring their safety and quick response if any medical emergencies arise.
3. Security and Authentication: Due to the sensitive nature of military operations, ensuring the authenticity and security of data is crucial. Any leak or breach of health data could provide an advantage to adversaries. By employing strong encryption, two-way authentication, and secure routing protocols, the system guarantees that the data reaches its destination only to authorized personnel.

D. Data Aggregation and Collaborative Healthcare

Beyond military applications, WBANs have transformative potential for healthcare delivery in remote areas. By aggregating health data from multiple patients, the network can help healthcare professionals make more informed decisions:

1. Data Aggregation: With WBANs, data from multiple patients can be aggregated and sent to a central cloud platform or database, where healthcare professionals can access it for analysis. This enables real-time monitoring and early intervention for patients suffering from chronic diseases, such as diabetes, heart disease, or respiratory conditions.

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. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14227

2. Collaborative Care: By connecting multiple patients to healthcare providers, WBANs support collaborative care models. This collaboration can involve shared decision-making between patients, doctors, and specialists, improving outcomes for patients requiring continuous health monitoring.
3. Research and Analytics: Aggregated health data can also be analyzed for research purposes. For example, trends in chronic disease prevalence can be studied, which may inform the development of new medical treatments or public health policies. WBANs contribute to data-driven research by providing a real-time stream of reliable physiological data from diverse populations.

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 1 shows an intrabody network and figure 2 shows the interbody Network. [1]

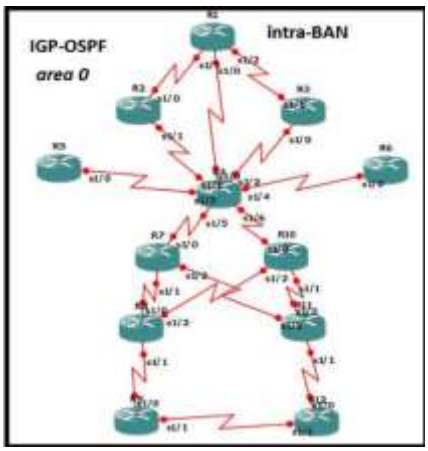

Figure 1 shows intrabody network belonging to BAN

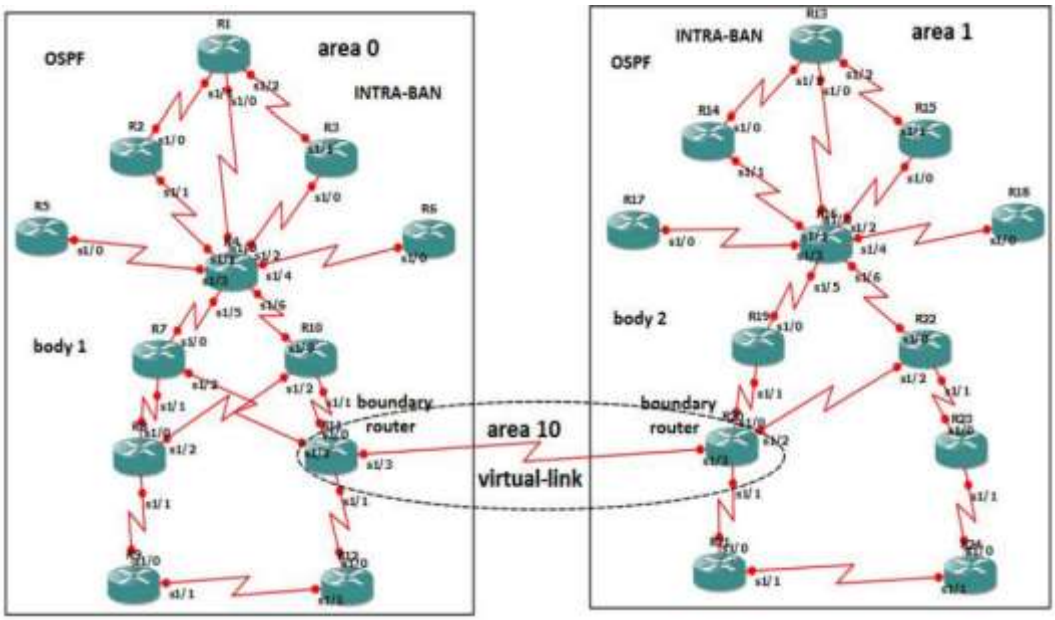

Figure 2 shows the interbody network belonging to BAN

II.MOTIVATION

Health parameters of the Military personnel are 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, and 2-way authentication can prevent intrusion. This ensures that sensitive information about the soldiers' health status is only accessible to authorized personnel.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14227

Additionally, these measures allow for real-time monitoring and timely interventions in case of medical emergencies. The use of robust security protocols also mitigates the risk of cyber-attacks or data breaches, ensuring mission-critical information remains protected. As a result, the overall safety and operational efficiency of military personnel in remote or hazardous environments is significantly improved. This technology not only enhances healthcare delivery but also contributes to strategic defence capabilities.

III.OSPF PROTOCOL

Open Shortest Path First (OSPF) is a routing protocol that follows a hierarchical structure. It includes a central backbone area known as area 0, while other areas are referred to as non-backbone areas. Because of this hierarchical design, OSPF is particularly well-suited for routing in a Body Area Network (BAN), where various sensors or nodes can be organized into distinct areas depending on their physical location or specific function. OSPF allows for efficient routing by maintaining separate link-state databases within each area, reducing the overall network complexity and improving scalability. Since OSPF is a Link-State Advertisement (LSA) protocol, it requires each router to exchange information about the state of its links to construct a comprehensive topology map. While OSPF provides a high level of robustness and flexibility, it can be relatively slow compared to more modern routing protocols due to the frequent updates and the need for recalculating the routing table as the network topology changes. In a Body Area Network, where frequent changes in node status and location might occur, this latency may become an issue. However, OSPF's ability to dynamically adjust routes based on link-state changes makes it resilient in environments where sensor nodes or devices are frequently being added or removed. To enhance performance in BANs, OSPF can be used in combination with other optimizations or hybrid routing protocols to reduce overhead and improve real-time responsiveness. Additionally, OSPF is highly suitable in networks with complex and diverse topologies, where scalability and fault tolerance are critical for ensuring reliable data transmission. [4]

IV.EIGRP PROTOCOL

The OSPF protocol is slower than the Enhanced Interior Gateway Routing Protocol. EIGRP is a distance-vector routing technology that expedites and improves data processing. Taking into consideration the particular needs or circumstances of the network, it uses a number of measures, such as Bandwidth (BW), delay, dependability, load, and MTU (Maximum Transmission Unit), to establish the best route across networks. This enables EIGRP to make routing decisions more quickly and reliably while also adapting to various network settings. Strong security for data transmission is provided by the use of the AES 256-bit encryption technique. Furthermore, SHA-384 is used to guarantee data integrity, ensuring that no information has been changed while in transit. Together, these encryption techniques protect private network traffic from attacks and tampering.One of the key advantages of EIGRP is its backward compatibility with older versions of IGRP (Interior Gateway Routing Protocol), which allows for smooth integration into existing networks without the need for a complete overhaul. EIGRP enhances traditional IGRP by adding more flexibility and advanced features, such as rapid convergence and improved scalability, making it suitable for both small and large networks. Furthermore, EIGRP reduces the overall routing overhead by only sending updates when necessary, rather than frequently broadcasting full routing tables. This efficiency helps conserve bandwidth and reduces the processing load on routers. EIGRP also supports VLSM (Variable Length Subnet Masking), allowing for more efficient use of IP address spaces by enabling networks of varying sizes. In dynamic environments, such as Body Area Networks (BANs), where nodes may frequently change their locations or configurations, EIGRP's ability to quickly adapt to changes is a significant benefit. In addition, the protocol's DUAL (Diffusing Update Algorithm) ensures that it consistently selects the most reliable and efficient paths, helping to maintain the stability and reliability of the network even in cases of failure or route changes. By combining rapid convergence, flexibility, and advanced security features, EIGRP is an ideal choice for modern networks, offering both high performance and robust protection. EIGRP's scalability is another standout feature, as it is capable of supporting large networks with complex topologies, which is essential in environments like Body Area Networks (BANs) where multiple devices or sensors may need to communicate and exchange information. This makes EIGRP a highly efficient routing protocol for maintaining seamless connectivity across vast and diverse network infrastructures. Additionally, EIGRP's support for multiple network layer protocols, including IP, IPX, and AppleTalk, gives it flexibility and allows it to be used in a variety of network environments beyond traditional IP-based systems. Moreover, EIGRP's automatic route summarization feature can reduce the size of routing tables and decrease the workload of routers by grouping similar network addresses into a single summary address. This feature significantly improves the efficiency and manageability of the network, especially when the network scales or changes frequently. In environments with high mobility, like military or Body Area Networks (BANs), the protocol's dynamic and adaptive routing capabilities ensure continuous and optimal performance, even as sensor nodes or devices shift locations. Another advantage of EIGRP in such environments is its ability to manage and prioritize network traffic efficiently.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14227

By using multiple metrics to evaluate path quality, EIGRP ensures that critical health data or mission-essential information is transmitted with minimal delay and maximum reliability. This is particularly crucial in contexts where real-time data transmission is essential for making quick decisions regarding the health and safety of personnel. In conclusion, EIGRP stands out as a highly efficient, flexible, and secure routing protocol for modern networking environments. Its ability to support dynamic topologies, ensure rapid convergence, and prioritize security and performance makes it an optimal choice for both traditional and innovative network applications, including Body Area Networks (BANs) and other critical infrastructure systems.

V.COMMUNICATION MODEL

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). [4]
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) 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 [5][6]

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
- 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

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14227

- 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] Figure 3 shows implementation of intraban on wireless network using IP addressing scheme. Figure 4 shows the backup network for the main system.

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. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14227

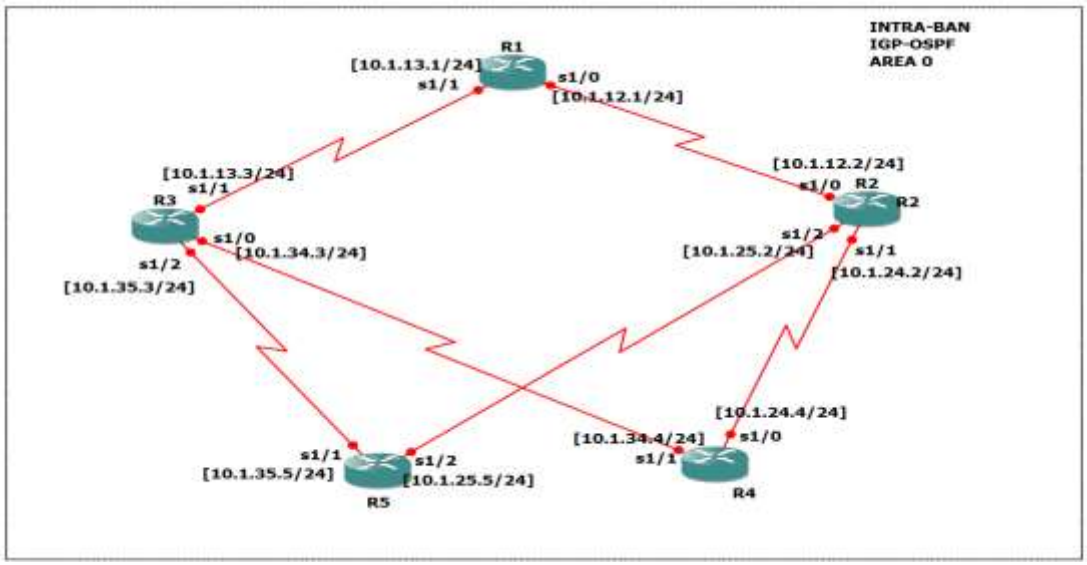

Figure 3 shows implementation of intraban on wireless network using IP addressing scheme.

VII.BACKUP NETWORK

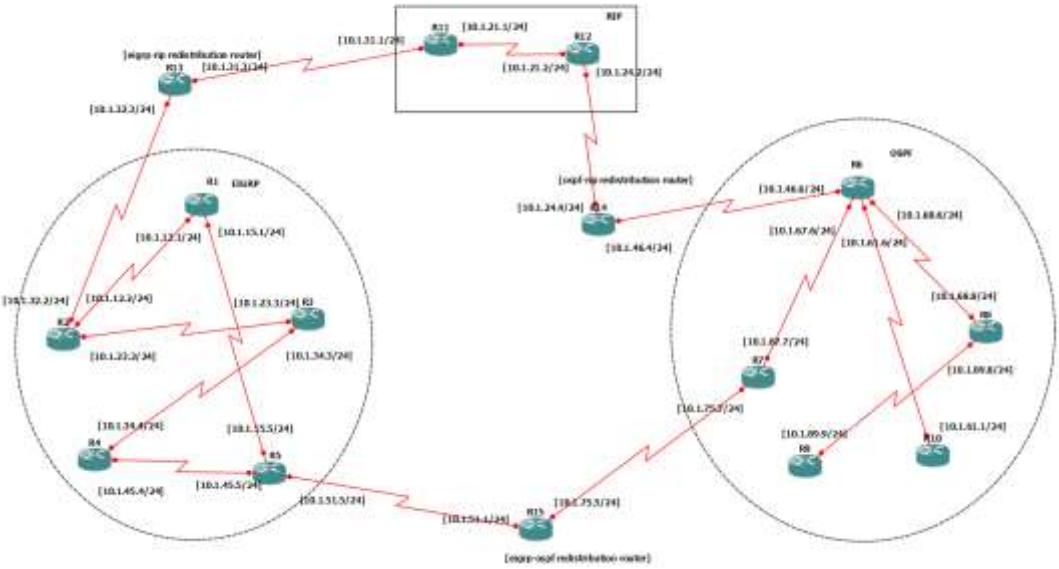

Figure 4 shows the backup network

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 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.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14227

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.[15-17]

VIII.WBAN IN PODIATRY

Wireless Body Area Networks (WBANs) are an emerging technology in healthcare [18] that involve wearable or implantable sensors communicating wirelessly to monitor various health parameters. In podiatry, WBANs can play a crucial role in foot health monitoring, diabetic foot care, gait analysis, and rehabilitation.

1) Applications of WBAN in Podiatry for Military Personnel

1. Diabetic Foot Monitoring
   - Sensors embedded in smart insoles or socks can detect temperature variations, pressure points, and moisture levels to prevent foot ulcers in diabetic patients.
   - Early detection of abnormalities can help reduce the risk of amputations.
2. Gait Analysis and Rehabilitation
   - WBAN-enabled pressure sensors in shoes or wearable IMUs (Inertial Measurement Units) can analyze walking patterns to detect abnormalities in gait.
   - Useful for patients with conditions like flat feet, plantar fasciitis, or post-surgery recovery.
3. Fall Detection and Balance Monitoring
   - Elderly personnel or those with neuropathy can benefit from real-time monitoring of stability.
   - WBAN-integrated motion sensors can provide alerts for potential falls, improving patient safety.
   - They can use WBAN-integrated footwear sensors to monitor stride, foot pressure, and balance to optimize performance and prevent injuries.
4. Custom Orthotics and Prosthetics
   - WBAN technology can be integrated into smart orthotics or prosthetic limbs to track pressure distribution and adjust support dynamically.

2) Benefits of WBAN in Podiatry

1. Non-invasive monitoring – Continuous tracking without hospital visits.
2. Early detection – Prevents complications in diabetic and elderly personnel.
3. Improved mobility and rehabilitation – Provides personalized feedback for recovery.
4. Data-driven insights – Helps podiatrists make better treatment decisions.[19-20]

IX.SUPPORT VECTOR MACHINE (SVM) TO DEVELOP ML MODEL

Support Vector Machines (SVM) can be effectively used for podiatric foot analysis in military personnel, helping to detect gait abnormalities, prevent injuries, and enhance performance. Military personnel experience extreme physical stress, making them prone to foot-related issues such as stress fractures, plantar fasciitis, and Achilles tendinitis. SVM is ideal for this task due to its ability to handle high-dimensional data, robustness to noise, and effectiveness in classification problems such as distinguishing normal vs. high-risk foot conditions. The development of an SVM-based ML model involves several steps, starting with data collection from wearable smart insoles, motion capture systems, and medical records. Key features extracted include plantar pressure distribution, gait cycle parameters (step length, cadence, symmetry), foot posture index, and stress markers. Data preprocessing is crucial and involves normalization, feature selection using PCA or LASSO regression, and handling class imbalance with techniques like SMOTE. For model building, different SVM kernels can be selected based on the data's complexity—linear for simpler cases and RBF for nonlinear patterns. Hyperparameter tuning through grid search or Bayesian optimization ensures optimal model performance. The training process involves splitting the dataset, standardizing inputs, and fitting the SVM model using an appropriate kernel, followed by evaluation with accuracy, precision, recall, F1-score, and AUC-ROC curve. Real-world validation includes K-Fold cross-validation and deployment in military training environments using real-time foot sensors. SVM can be applied in several ways, including injury prediction, custom orthotics recommendations, performance optimization, and post-injury rehabilitation. Figure 5 shows the workflow diagram of building a ML model using python script. However, challenges such as the need for large-scale military foot data, real-time system integration, and potential improvements through deep learning-based hybrid models must be addressed. Future work could focus on deploying the model on wearable edge AI devices and integrating CNNs for foot image classification.

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. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14227

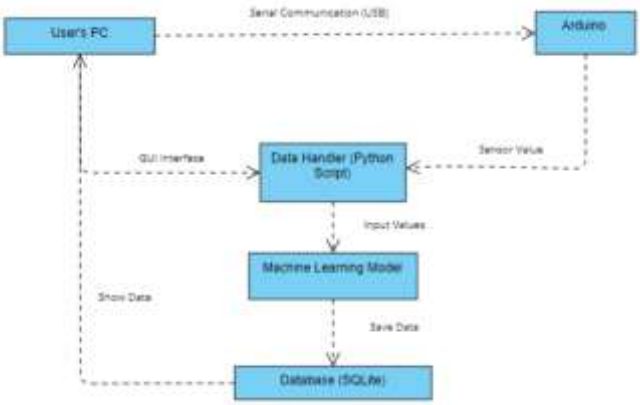

Figure 5 shows the workflow diagram of building a ML model using python script

```python
from sklearn.svm import SVC
from sklearn.model_selection import train_test_split, GridSearchCV
from sklearn.preprocessing import StandardScaler

# Load dataset
X = foot_sensor_data  # Features (e.g., plantar pressure, gait cycle)
y = labels  # 0: Normal, 1: High Injury Risk

# Train-test split
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Standardization
scaler = StandardScaler()
X_train = scaler.fit_transform(X_train)
X_test = scaler.transform(X_test)

# Define SVM model
svm_model = SVC(kernel='rbf', C=1, gamma='scale')

# Train the model
svm_model.fit(X_train, y_train)

# Predict
y_pred = svm_model.predict(X_test)

# Evaluate performance
from sklearn.metrics import classification_report
print(classification_report(y_test, y_pred))
```

Figure 6 shows the implementation of SVM on the Podiatric dataset

X.CONCLUSIONS AND FUTURE SCOPE

A sophisticated experimental approach was developed to establish a secure and efficient method for interconnecting remotely deployed army personnel with the base station or Headquarters (HQ) for continuous and rigorous health monitoring. The OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) routing protocols were employed to optimize network performance and reliability. To safeguard communications, a two-way authentication mechanism was implemented, ensuring only authorized personnel could access the network. Data security was further strengthened through AES-256 encryption, coupled with SHA-384 integrity verification, to maintain confidentiality and protect against data breaches. A centralized server was deployed to calculate node trust levels and detect potential threats by identifying malicious nodes in real time. Additional security measures, such as whitelisting, database activity monitoring, and data loss prevention, were incorporated to enhance the network's resilience against cyber threats. To mitigate the risk of compromised nodes, session-based encryption was utilized, ensuring that each communication session was uniquely encrypted. This method prevents attackers from intercepting and deciphering sensitive data without the correct decryption key. Furthermore, an advanced node validation process with unique keys was established to authenticate requests, blocking unauthorized access attempts and safeguarding classified military intelligence from cyber intrusions.

To further strengthen security, multi-factor authentication (MFA) was implemented, requiring personnel to verify their identities using multiple authentication factors such as passwords, biometrics, or one-time passcodes.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14227

This additional layer of security limits unauthorized access, even in cases where login credentials are compromised. Network segmentation was also introduced, isolating different parts of the network to minimize the impact of potential breaches. Even if an intruder gains access to a specific segment, their movement within the network is restricted, preventing lateral attacks and containing potential damage. Intrusion Detection and Prevention Systems (IDPS) were integrated to continuously monitor network traffic, detect suspicious activities, and automatically mitigate threats in real time. Additionally, threat intelligence services were incorporated to provide proactive defense mechanisms by analyzing external threat data and adapting to evolving cyber threats. A comprehensive incident response plan was developed to ensure rapid containment and recovery in the event of a breach. Regular penetration testing and vulnerability assessments were conducted to evaluate security measures and reinforce system defenses before potential vulnerabilities could be exploited.

In parallel with the security infrastructure, a Support Vector Machine (SVM)-based machine learning model was developed to analyze podiatric gait patterns in military personnel. Given the physically demanding nature of military activities, this SVM model was designed to predict gait abnormalities, identify potential foot injuries, and optimize mobility. The system utilized sensor-based smart insoles and motion capture devices to collect real-time data on plantar pressure distribution, step cadence, foot posture, and balance. After preprocessing the data using normalization, feature selection, and noise reduction techniques, the SVM classifier was trained to differentiate between normal and abnormal gait patterns. The RBF (Radial Basis Function) kernel was applied to handle non-linearity in gait variations, ensuring precise classification and prediction of potential injuries before they manifest. Hyperparameter tuning through grid search optimization improved model accuracy, while cross-validation techniques ensured the model's robustness across different military training environments.

By integrating the SVM-based gait prediction system with the secure communication network, military personnel could receive real-time feedback on foot health, enabling early intervention for injury prevention. This AI-driven approach not only enhances soldier endurance and performance but also minimizes downtime due to musculoskeletal injuries. Future advancements could involve integrating deep learning models such as CNNs (Convolutional Neural Networks) for gait image analysis and incorporating IoT-based real-time monitoring systems to further enhance predictive accuracy. This holistic framework, combining secure military networking with AI-powered podiatric analysis, establishes a robust and intelligent system to improve both the security and health of military personnel deployed in remote locations.

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.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14227

[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.

[15]. A. Majumder, M. A. Rahman, M. A. Ahamed, M. Mukherjee, “Wearable Sensors for Remote Health Monitoring: Current Trends and Future Prospects”, Sensors, 2017, DOI: 10.3390/s17071498.

[16]. M. R. Islam, M. A. Azim, T. K. Barua, "IoT-Based Remote Health Monitoring System: A Review", Journal of Biomedical and Health Informatics, IEEE, DOI: 10.1109/JBHI.2019.2952978.

[17]. B. Latr, B. Braem, I. Moerman, C. Blondia, P. Demeester, “A Survey on Wireless Body Area Networks”, Wireless Networks, Springer, 2009, DOI: 10.1007/s11276-008-0052-7.

[18]. S. Ullah, H. Higgins, B. Braem, B. Latr, C. Blondia, P. S. Thompson, R. B. Stewart, H. Yi, K. S. Kwak, “A Comprehensive Survey of Wireless Body Area Networks”, Journal of Medical Systems, 2012, DOI: 10.1007/s10916-011-9805-6.

[19]. M. M. Hossain, G. Muhammad, “Cloud-Assisted Secure Data Transmission in WBAN: A Survey”, Future Generation Computer Systems, Elsevier, DOI: 10.1016/j.future.2018.12.001.

[20]. S. J. Marinkovic, C. Spagnol, “Energy-efficient WBANs for Medical Applications”, IEEE Journal on Selected Areas in Communications, 2011, DOI: 10.1109/JSAC.2011.110208.

