Int. Jrl. of **Computational Learning & Intelligence**
Vol. 02, Issue 03 (July), 2023

RESEARCH ARTICLE

Attack Discernment and Protected Network Communication in Wireless Body Area Network (WBAN)

Smitha B N . Kumari G Gaikwad . Rohith H G . Sammed Patil . Suraj Gudi

Department of Computer Science and Engineering,
Sai Vidya Institute of Technology, Yelahanka, Bengaluru, India.

Received: 21 April 2023 / Revised: 16 May 2023 / Accepted: 27 May 2023

DOI: 10.5281/zenodo.8210362

Abstract – Wireless Body Area Network (WBAN) is the most rapidly growing branch of networking and data communication. With the rapid advancements of wireless communication and semiconductor technology, sensor network designed to operate autonomously to connect various other sensors (medical, position and geography) and appliances has become more robust and efficient. 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). The intra-body network consists of sensors and other elements embedded on or inside the body. These form the nodes of the network and are interconnected by links. A Body Area Network is constructed to interconnect the nodes, thereby exchanging information and bringing about the real-time concepts of sensors inter-dependability. Malicious nodes can construct a dynamic blacklist of Network nodes, which can be used to block nodes whose trust values fall below a pre-defined threshold. This network when connected and tested would enable exchange of confidential and essential data of military personnel. The information in the network to be transmitted is password protected. This would avoid the intruders from stealing TOP-SECRET data/information. GNS 3 tool is used for implementing routing and cryptography on the network.

Index Terms – Autonomous System, EIGRP, RIP, TELNET, AP, Implant Node, QOS, IP, OSPF, Subnet Mask, vty Lines.

I. INTRODUCTION

This work considers the realization of a human body implanted with biomedical sensors, operating wireless protocols of variable frequency, and measuring more than one physiological parameter of the body. As shown in Figure 1, 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. During complex surgical procedures, the captured sensor data from the operating room can be applied for modelling [1]. The use of a routing protocol to advertise routes that are learned by some other means, such as by another routing protocol, static routes or directly connected routers can be referred to as route redistribution.

Enhanced Interior Gateway Protocol which is an Interior Gateway Protocol is the protocol of choice for our project. The use of EIGRP in simulation of the inter-body network is being propounded by us [1]. Body Area Networking (BAN) is a contemporary and special field of networking and wireless communication in which packets are forwarded to a specific destination within the human body [2]. This is possible only when the sensors or computers or other electronic components at the nodes are properly interconnected and every node is reachable [3]. In this project efforts were made to interconnect all the nodes within an autonomous body using a dynamic routing protocol such as the OSPF. Inter body communication was also made possible using Virtual-Links configured between two boundary routers of the two autonomous systems. Inter body communication between two or more autonomous human bodies were also made possible by configuring OSPF on routers and dividing the networks into logical areas (backbone area and other areas called the non-backbone areas).

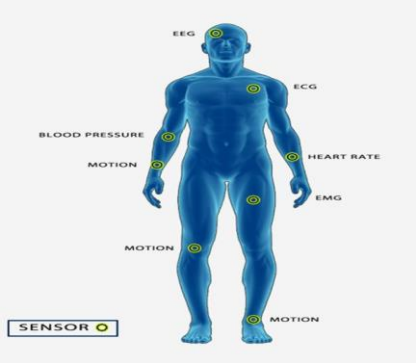


Figure. 1: Wireless Body Area Network

3-WAY HANDSHAKING

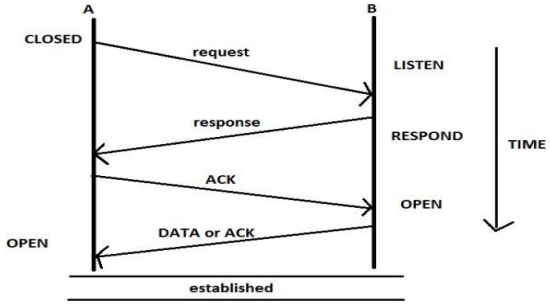


Figure. 2: 3 way hand-shaking flow diagram

Above Figure 2 represents 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).

II. METHODOLOGY AND IMPLENTATION

A. ROUTERS

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet [5]. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node. A router is connected to two or more data lines from different IP networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet header to determine the ultimate destination [5]. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. A router has two types of network element components organized onto separate processing Planes.

1) Control plane: A router maintains a routing table that lists which route should be used to forward a data packet, and through which physical interface connection. It does these using internal preconfigured directives, called static routes, or by learning routes dynamically using a routing protocol. Static and dynamic routes are stored in the routing table. The control-plane logic then strips non-essential directives from the table and builds a forwarding information base (FIB) to be used by the forwarding plane.

2) Forwarding plane: The router forwards data packets between incoming and outgoing interface connections. It forwards them to the correct network type using information that the packet header contains matched to entries in the FIB supplied by the control plane.

B. PROTOCOLS

a) Open Shortest Path First (OSPF): It is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). OSPF supports the Classless Inter-Domain Routing (CIDR) addressing

model [10]. OSPF is a widely used IGP in large enterprise networks. IS-IS, another LSR-based protocol, is more common in large service provider networks.

b) Enhanced Interior Gateway Routing Protocol (EIGRP): It is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration [4]. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers. Functionality of EIGRP was converted to an open standard in 2013 and was published with informational status as RFC 7868 in 2016.

c) Routing Information Protocol (RIP): It is one of the oldest distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination [10]. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. RIP implements the split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated.

Existing System

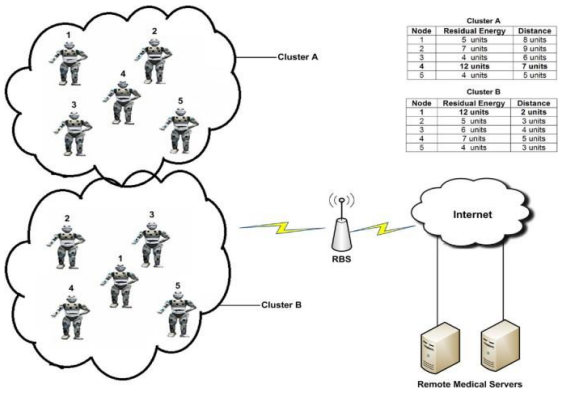
"Survey of main challenges (security and privacy) in wireless body area networks for healthcare applicationS" by SamaherAl-Janabi, brahim-Al Mohammad Shojafar c, Shahaboddin Shamshirband [9]. Wireless Body Area Network (WBAN) is a new trend in the technology that provides remote mechanism to monitor and collect patient's health record data using wearable sensors. It is widely recognized that a high level of system security and privacy play a key role in protecting these data when being used by the healthcare professionals and during storage to ensure that patient's records are kept safe from intruder's danger. It is therefore of great interest to discuss security and privacy issues in WBANs. In this paper, we reviewed WBAN communication architecture, security and privacy requirements and security threats and the primary challenges in WBANs to these systems based on the latest standards and publications. This paper also covers the state-of-art security measures and research in WBAN. Finally, open areas for future research and enhancements are explored.

Proposed System

The aim of this work is to identify and select existing technologies and protocols that satisfy the main requisites of WBANs for the application of healthcare with regard to patient mobility, secured and reliable data, power consumption, and the requirements needed for large amounts of sensor nodes to coexist in a relatively small space. To understand the special needs in a medical network, both the protocol stack and understanding of each protocol layer are essential.

This paper presents an overview of the state of the art in WBAN. As shown in Figure 4, It is mainly focused on architectures and communication protocols for healthcare networks based on

WBANs.[2] We analyze the most recent implementation solutions for this type of network, as well as the protocols used at each protocol layer. Each implementation has its own characteristics, advantages, and disadvantages, which are comprehensively described and analyzed in several comparative tables. Moreover, we also provide a comparative study of emerging and existing radio technologies and protocols for nonproprietary WBANs on unlicensed radio frequency bands.



Cluster A

Node	Residual Energy	Distance
1	5 units	8 units
2	7 units	9 units
3	4 units	6 units
4	12 units	7 units
5	4 units	5 units

Cluster B

Node	Residual Energy	Distance
1	12 units	2 units
2	5 units	3 units
3	6 units	4 units
4	7 units	5 units
5	4 units	3 units

Figure 3: Shows Inter-Body Connection and Intra-Body Connection.

III. EXPERIMENT AND RESULTS

Establishing connection by configuring the Routers and by applying the routing protocols like EIGRP, RIP, OSPF, TELNET. Creating a simple topology, and establishing the connection with the help of routing protocols. For these, we'll be using GNS-3 tool. We are using 13 Routers in total as shown in figure 5. 5 Routers in 1 Autonomous System and 6 Routers in another Autonomous System. Two Extra Routers for Back-up. In the middle of the two autonomous Systems there will be a Router that is used for connection of two autonomous System. First, we'll be placing c7200 Cisco Routers and configure it. We'll Choose PA-8T slot because c7200 routers consists of 8 ports. Then we'll be assigning IP Address for the Routers. After assigning IP Addresses, we'll implement Routing protocols, for communication. To see the result, we have typed a command "ping IP Address". If the packets are sent successfully, the it will be indicated with "!" mark, if it fails "." mark will be indicated.

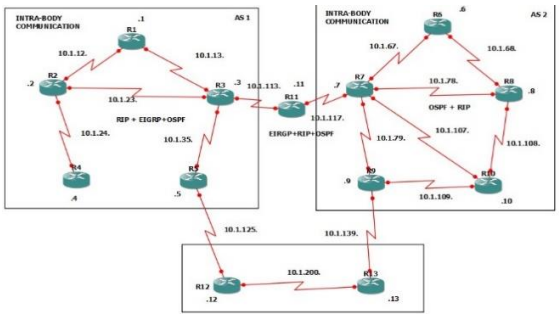


Figure 4: Representation of the Topology

After implementation of TELNET protocol [4], we'll be able to set up password and useful feature about this is that, once we open the terminal, it asks for password, to login. This acts as a security for avoiding attacks from the third party. This basically acts as user access verification. As shown in figure 5, once you login by entering the password, you can ping the routers established by giving their IP Addresses. TELNET protocol is used to login to another router, inside other router console. For Example, in figure 6, the console opened here is 4th Router's, but we have logged in to 3rd Router. We can come back from this by typing "exit" command.

IV. RESULT AND ANALYSIS

In this section, the proposed cluster-based WBAN technique is analyzed with respect to security, cost, energy consumption, reliability of nodes. Both intra-WBAN and inter-WBAN communications involve routing, below are the few points mentioned to overcome the limitations [9].

1. Resource constraints: To address the limited resources of WBANs, we have proposed various techniques such as energy-efficient routing protocols, router re-distribution and adaptive transmission power control.

```
head(config)#username person4 password 5678
head(config)#line vty 0 4
head(config-line)#login local
head(config-line)#^Z
head#
*May 15 22:51:24.011: %SYS-5-CONFIG_I: Configured from console by console
head#telnet 10.1.12.1
Trying 10.1.12.1 ...
% Destination unreachable; gateway or host down

head#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
head(config)#router ospf 100
head(config-router)#network 10.1.13.3 0.0.0.0 area 0
head(config-router)#^Z
head#
*May 15 23:29:49.467: %SYS-5-CONFIG_I: Configured from console by console
head#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
head(config)#router rip
head(config-router)#version 2
head(config-router)#network 10.0.0.0
head(config-router)#no auto-summary
head(config-router)#^Z
head#
*May 15 23:30:27.827: %SYS-5-CONFIG_I: Configured from console by console
head#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
head(config)#router rip
head(config-router)#redistribute ospf 100 metric 1
head(config-router)#^Z
```

Figure 5: Router re-distribution.

2. Security and privacy: To enhance the security and privacy of WBANs, we have proposed various encryption and authentication schemes, we have used telnet protocol for user authentication.
3. Interference: To mitigate interference issues, researchers have proposed frequency hopping techniques, channel allocation algorithms, and interference avoidance mechanisms.
4. Reliability: To ensure high reliability of WBANs, researchers have proposed redundancy mechanisms such as backup nodes or multiple paths for data transmission.

5. Compatibility: To address interoperability issues, researchers have proposed standardization efforts such as Continua Health Alliance guidelines.
6. Cost: To reduce the cost of implementing and maintaining a WBAN, this can be done by the proposal of using low-cost sensors or leveraging existing infrastructure such as smartphones or cloud computing.

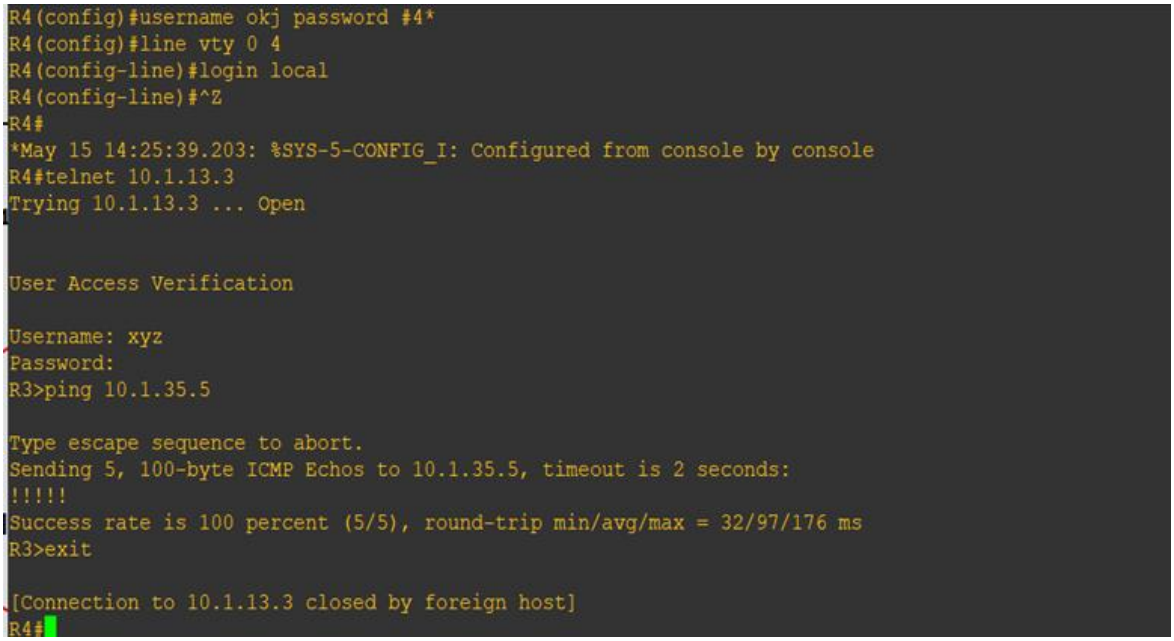


Figure 6: Representation of security and privacy and also secured connection established.

V. CONCLUSION

In conclusion, wireless body area networks (WBANs) have the potential to revolutionize healthcare by providing remote monitoring and collection of patient health data using wearable sensors. However, WBANs face several limitations such as resource constraints, security and privacy issues, interference, reliability concerns, compatibility issues, and cost. To overcome these limitations, researchers have proposed various solutions such as energy-efficient routing protocols, encryption and authentication schemes, frequency hopping techniques, redundancy mechanisms, standardization efforts, and low-cost sensors. By implementing these solutions effectively in real-world healthcare settings, WBANs can provide high-quality and cost-effective healthcare services while ensuring patient safety and privacy. Further research is needed to address the remaining challenges and to explore new opportunities for WBANs in healthcare.

REFERENCES

1. Qi, W., Su, H., Chen, F., Zhou, X., Shi, Y., Ferrigno, G., & De Momi, E. (2020, December). Depth vision guided human activity recognition in surgical procedure using wearable multisensor. In *2020 5th International Conference on Advanced Robotics and Mechatronics (ICARM)* (pp. 431-436). IEEE.

2. Yang, Y. (2019). Focus on the four core sensor technologies and tap the new growth pole of wearable devices. *High Tech. Ind*, *2*, 36-47.
3. Shajin, F. H., & Rajesh, P. (2022). Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol. *International Journal of Pervasive Computing and Communications*, *18*(5), 603-621.
4. Liu, B., Peng, Y., Xu, J., Mao, C., Wang, D., & Duan, Q. (2021). Design and implementation of multiport energy routers toward future energy Internet. *IEEE Transactions on Industry Applications*, *57*(3), 1945-1957.
5. Al Mahmud, A., Wickramarathne, T. I., & Kuys, B. (2020). Effects of smart garments on the well-being of athletes: a scoping review protocol. *BMJ open*, *10*(11), e042127.
6. Sreedhar Kumar, S., Ahmed, S. T., Mercy Flora, P., Hemanth, L. S., Aishwarya, J., GopalNaik, R., & Fathima, A. (2021, January). An Improved Approach of Unstructured Text Document Classification Using Predetermined Text Model and Probability Technique. In *ICASISET 2020: Proceedings of the First International Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISET 2020, 16-17 May 2020, Chennai, India* (p. 378). European Alliance for Innovation.
7. Wu, H., & Li, Y. (2020). Application of flexible sensor in textile and garment. *Wool Technol*, *48*(09), 94-98.
8. Qi, W., Su, H., & Aliverti, A. (2020). A smartphone-based adaptive recognition and real-time monitoring system for human activities. *IEEE Transactions on Human-Machine Systems*, *50*(5), 414-423.
9. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian informatics journal*, *18*(2), 113-122.
10. Ahmed, S. T., Priyanka, H. K., Attar, S., & Patted, A. (2017, June). Cataract density ratio analysis under color image processing approach. In *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 178-180). IEEE.
11. Luo, J., Chen, Y., Wu, M., & Yang, Y. (2021). A survey of routing protocols for underwater wireless sensor networks. *IEEE Communications Surveys & Tutorials*, *23*(1), 137-160.
12. Sankar, R., Le, X. H., Lee, S., & Wang, D. (2013). Protection of data confidentiality and patient privacy in medical sensor networks. In *Implantable Sensor Systems for Medical Applications* (pp. 279-298). Woodhead Publishing.
13. Patil, K. K., & Ahmed, S. T. (2014, October). Digital telemammography services for rural India, software components and design protocol. In *2014 International Conference on Advances in Electronics Computers and Communications* (pp. 1-5). IEEE.
14. Gao, T., Massey, T., Selavo, L., Crawford, D., Chen, B. R., Lorincz, K., ... & Welsh, M. (2007). The advanced health and disaster aid network: A light-weight wireless medical system for triage. *IEEE Transactions on biomedical circuits and systems*, *1*(3), 203-216.
15. Nagashree, N., Chitralekha, M., Harsha, S. M., Sree, S. S. U., Chinmayee, M., & Basavaraj, S. H. (2023, March). A Modified UNet based Framework towards Early Detection of Autism using EEG Waves. In *2023 2nd International Conference for Innovation in Technology (INOCON)* (pp. 1-4). IEEE.
16. Redondi, A., Chirico, M., Borsani, L., Cesana, M., & Tagliasacchi, M. (2013). An integrated system based on wireless sensor networks for patient monitoring, localization and tracking. *Ad Hoc Networks*, *11*(1), 39-53.