IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10606

Body Area Routing Network Using Telnet and Two-Way Authentication

Mrs Keerthi P[1], Nischitha G N[2], Spoorthy V Ambati[3] , Aarnavi N[4]

Assistant Professor, Department of Information Science and Engineering, Atria Institute of Technology, Bangalore, India[1]

Student, Department of Information Science and Engineering, Atria Institute of Technology, Bangalore, India[2,3,4]

Abstract: WBAN (Wireless Body Area Network) is the newest branch of networking and data communication. Sensor networks meant to run autonomously to connect different additional sensors (medical, position, and geographic) and appliances have grown more resilient and efficient thanks to rapid improvements in wireless communication and semiconductor technology. We create a network that includes intra-body and inter-body communication. Every body is regarded as an autonomous system (AS) capable of mobility and communication with other autonomous systems (AS) with distinct Autonomous System Numbers (ASN). Sensors and other items installed on or inside the body make up the intra-body network. These are the network's nodes, which are linked together by links. A Body Area Network is built to connect the nodes, allowing them to communicate with one another. As a result, information is exchanged and real-time sensor interdependability ideas are realised. The latter is what the inter-body communication system is made up of. This network is made up of a large number of intra-body networks that are linked together to share information in a secure manner. When connected and tested, this network will allow military personnel to share private and critical information. The information that will be transmitted across the network is password secured. This would prevent intruders from gaining access to TOP-SECRET data or information.

Keywords: Body Area Network, EIGRP, RIP, WBAN.

I. INTRODUCTION

Given the current situation, the goal of this project is to identify and select existing technologies and protocols that meet the major needs of WBANs for healthcare applications in terms of patient mobility, secure and reliable data, power consumption, and the requirements for large numbers of sensor nodes to cohabit in a small space. The protocol stack, as well as a comprehension of each protocol layer, is required to comprehend the unique requirements of a medical network. This paper provides an overview of the current state of WBAN research. It focuses on WBAN-based healthcare network topologies and communication protocols. The most recent implementation options for this type of network, as well as the protocols utilized at each protocol layer, are discussed. Each implementation has its own set of traits, benefits, and drawbacks, which are detailed and assessed in a series of comparative tables. In addition, we present a comparison of emerging and existing radio technologies and protocols for nonproprietary WBANs operating on unlicensed radio frequency bands.

A significant number of military, air force, and navy troops would be present in any country with a big border or area. They may be tasked with operating in remote places far from the national capital or military base, and communication between these nodes is critical to the network's success. These men must be properly monitored in order to maximize their efficiency in serving the nation. Health monitoring of these means by embedding various body sensors and encrypting the data between the nodes is of the utmost importance.

II. LITERATURE SURVEY

The technique can inspect network traffic in real time and detect rogue nodes effectively. Our system can create a dynamic blacklist of Network nodes, which may be used to ban nodes whose trust values fall below a certain threshold. A central server is installed, which is responsible for determining node trust values and detecting rogue nodes. To increase the security of the network and infrastructure, the method can be used in conjunction with other security solutions such as database activity monitoring, white listing, and data loss prevention. To protect the node from the compromised attacker, session-based encryption is employed. A unique key of the individual node validation process will accept the attacker's request. This would prevent intruders from gaining access to TOP-SECRET data or information. [1]

DOI: 10.17148/IJIREEICE.2022.10606

A significant breakthrough in Body Area Networking is required. Physical connections like wires or foils running all over the body would be a failure on the side of researchers. In circumstances where electrons move through the body and carry information/data, a high impedance shoe is required. Because the human body is an excellent conductor of electricity, it acts as a short in the flow of charges throughout the body. The wireless Body Area Network is a great alternative to the aforementioned. Within the circle of a body (an AS) or between two or more AS, data is transmitted and received. Intra-AS communication is one type of communication, while Inter-AS communication is another. We've implemented a wireless data routing and sharing system that uses a variety of protocols and is compatible with today's technical environment. [2]

In the field of electronics and communication, Wireless Body Area Networking (WBAN) is a new technology. The fast development of physiological sensors, low-power integrated circuits, and wireless communication has resulted in the emergence of a new generation of wireless sensor networks, which are being employed for traffic, infrastructure, gaming, and health monitoring. The BAN is a multidisciplinary field that could provide low-cost, continuous health monitoring via the internet, including real-time updates to medical data. WBAN sensors would need to be simple, tiny in form factor, light in weight, power efficient, simple to operate, and customizable. Additionally, the storage devices must allow for remote storage and viewing of patient data, as well as Internet access to external processing and analytic tools.[3]

Body Area Networking (BAN) is a new and unique type of networking and wireless communication in which packets are routed to a specific location within the human body. Only when the sensors, computers, and other electrical components at the nodes are correctly integrated and each node can be reached is this possible. The goal of this research was to use a dynamic routing system like OSPF to connect all of the nodes within an autonomous body. Virtual-Links were configured between two border routers of the two autonomous systems to allow inter-body communication. Configuring OSPF on routers and partitioning the networks into logical areas (backbone area and other) enabled inter-body communication between two or more independent human bodies.[4]

Wireless Body Area Networks for healthcare applications are still in the early stages of development, but they promise major benefits in terms of monitoring, diagnostics, and therapeutics. Because WBAN sensor devices are used to collect sensitive data and may encounter hostile scenarios, they require a complex and highly secure security medium or structure to prevent hostile communications within the system. These gadgets offer various levels of security and privacy protection for sensitive and confidential patient medical information. [5]

WBANs and remote healthcare monitoring systems: existing and future research trends. To begin, divide a WBAN into four categories based on medical device communication, including in-vivo nano communications. Following that, a taxonomy of entities involved in remote healthcare monitoring systems was established. Then, at each tier of communication, we looked at the security requirements and issues that medical equipment confront. The issues of ensuring confidentiality, integrity, and availability at all tiers of communication in WBANs were highlighted in particular. The difficult issue of nano-networks with extremely restricted resources and capacities was identified. Finally, various areas of research to assure end-to-end security were emphasised, as well as certain flaws in present WBANs. [6]

WBASN is a relatively new technology that has the potential to transform healthcare applications in the near future. We summarised different characteristics and issues of WBASN in this paper. We attempted to cover the most recent developments in this field while also providing some general debate for the topic's general readers. WBASN will be stronger in its practical applications and will immediately touch the public health sector, bringing ease to our daily lives, once the expected results of different ongoing initiatives (and more that may come in the future) are ready. An interesting area for future research would be to look into edge computing-based/assisted BSN systems. These new advancements would have an impact on the BSN and WBASN, as more and more papers on edge computing are released. [7]

Continuously monitoring patient parameters is critical, and when the number of patients in the hospital is large, this process will be laborious, time-consuming, and effort-consuming for the physicians, so: One of its advantages is that it reduces the stress and workload experienced by medical personnel. Healthcare practitioners can constantly monitor, diagnose, and advise their patients utilising the system. System that used a microcontroller to measure a patient's heartbeat and temperature and delivered it to a remote end with great effect at a low cost. The system is dependable, cost-effective, and simple to use. It's simple to use, quick, efficient, and secure. The results gained are supported by the execution of the proposed system, which demonstrates that this system is effective. The results gained from the implementation of the suggested system show that this system is the best for monitoring patients in hospitals. In contrast to other types of medical equipment, the system includes the ability to preserve data for later use. The findings reveal that this technology continuously checks patient health in real time and under various settings. This approach provides clinicians with valuable

DOI: 10.17148/IJIREEICE.2022.10606

information regarding the patient's health situation. It cuts down on time spent travelling to follow up on patients' cases and collect patient data. As a result, give the doctor more time to follow up on more critical cases in the hospital. [8]

III. COMMUNICATION NETWORKS IN MILITARY SYSTEMS

A. Intra-Body Network

In this project, we employed IGPs – RIP on each node to dynamically route packets between each router, as each BAN on a human body is considered an autonomous/independent network. RIP version 2 (RIPv2) was developed in 1993, published in 1994 as RFC 1723, and ratified as Internet Standard 56 in 1998. It included the ability to transfer subnet information, which facilitated Classless Inter-Domain Routing (CIDR). To ensure backward compatibility, the hop count limit of 15 was maintained. RIPv2 can fully interoperate with the earlier standard if all Must Be Zero protocol fields in RIPv1 messages are appropriately provided. Fine-grained interoperability changes are also possible thanks to a compatibility switch feature.

B. Inter-Body Network

Inter-BAN, also known as inter body communication, is a networking model in which communication occurs between two autonomous bodies that run their own internal dynamic routing protocols and are connected to each other by means of Virtual-Links. This is in contrast to intra body area networks, which function as autonomous systems. Three-way handshaking is the only method that allows for this communication.

C. Security in Topology

We provide security within topology by providing a password. A CISCO router's access is restricted via passwords. Virtual terminal lines and console lines can both be given passwords. On a network where numerous persons need access to the router, a console password is useful. The router is inaccessible to anyone who is not authorized. As a result, it prohibits unauthorized users from gaining access to the router. CISCO router uses console password configuration to protect the console line.

Telnet password is known as virtual terminal password. You may access the router and alter anything using telnet. As a result, it's critical to secure telnet access using a strong password. Vty lines are specified differently on different devices. Cisco has a vty line range of 0 to 4. It has a total of 5 vty lines. Vty line is protected from intruders by providing password to vty line. Telnet is a protocol for connecting to remote computers (referred to as hosts) across a TCP/IP network (such as the internet). You can connect to a telnet server using telnet client software on your computer (that is, the remote host). When your telnet client connects to the remote host, it transforms into a virtual terminal, allowing you to communicate with the remote host from your computer. Most of the time, you'll need to log into the remote host, which needs you to have an account on that system. You can occasionally log in as a guest or public user without creating an account.

D. Backup Network

The RIP protocol is used to implement the backup network in the topology. Data is transferred to the intended destination over this backup network if any topological connection is lost or broken. The routing protocol EIGRP is used to construct an intra-body network in the topology. A redistribution router is used to establish the inter-body communication, importing and exporting RIP to EIGRP. Telnet protocol is used for remote access to the nodes, and each console line and virtual terminal is password-protected.

IV. CONCLUSION

We gave a brief summary of the existing WBAN suggestions and potential applications in this project. Network architecture, security, packet tracing, and connection are the four design issues that have been resolved. Researchers would have failed if they had discovered tangible connections throughout the body, such as cables or foils. When information or data is transported by electrons through the body, a high impedance shoe is crucial. The human body functions as a short to the flow of charges inside the body since it is a very good conductor of electricity. The wireless Body Area Network is an excellent substitute for the aforementioned. A body's perimeter is where data transmission and reception occur (an AS)

DOI: 10.17148/IJIREEICE.2022.10606

ACKNOWLEDGMENT

We would like to take this opportunity to thank our guide **Mrs. Keerthi P**, for giving us all the help and guidance needed, we are grateful for her kind support and valuable suggestions.

REFERENCES

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