IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

Simulation of Wireless BAN using Network Simulation Tool

Vishesh S[1], Manu Srinath[1], Sneha Gopinath[2], Pranava Karanth R[3]

B.E, Department of Telecommunication Engineering, BNM Institute of Technology, Bangalore, India [1]

B.E, Department of Information Science Engineering, JSSATE, Bangalore, India [2]

Student, Department of Telecommunication Engineering, KSIT, Bangalore, India [3]

Abstract: A BAN (Body Area Networking) is a wireless network of wearable computing devices along the body. Advances in wireless communication technologies such as wearable and implantable biosensors, and with recent developments in embedded computation area are making way for design, development and implementation of Body Area Networks. This paper presents to you the simulation of the idea proposed in our previous paper titled "Conceptual Study of Wireless BAN using Bluetooth/IEEE 802.11n"[1] we have successfully simulated the proposal using GNS3 tool and drawn conclusions in this paper. OSPF is used to interconnect the routers/sensors at various parts of the body, either placed at the nodes or as stubs (at the body endings). Heart is the central and the most powerful router and all the nodes are connected to it in a star topology. Many interface loops are created which act as the body endings or information/data/multimedia exchangers. The BAN on a person who is transmitting the data is enclosed under area 0 (backbone of the OSPF). Area 0 is interconnected to various other BAN's enclosed by different areas n, where n=1,2,3,.... and n is not '0' via virtual links. Communication between two BAN's is possible only by handshaking. Also the information/data/multimedia to be exchanged is encrypted, password protected using encryption and network security protocols.

Keywords: OSPF, Area 0, information/data/multimedia exchanges, encrypted, password protected, encryption and network security protocols.

I. INTRODUCTION

The rapid growth in physiological sensors, low power integrated circuits, and wireless communication has enabled a new generation of wireless sensor networks, now used for purposes such as monitoring traffic, infrastructure, gaming and health. [2] The BAN is an interdisciplinary area which could allow inexpensive and continuous health monitoring with real time updates of medical records through the internet. It is strange to see how a BAN system can be analogous with the anatomy of the human circulatory system. Below are the parts of the human circulatory system and their analogous counterparts as proposed in our previous paper titled "Conceptual Study of Wireless BAN using Bluetooth/IEEE 802.11n"

- Heart ||| Central switch/router
- Veins ||| wireless data from nodes or devices to the central router/switch
- Arteries ||| wireless data from central switch/router to nodes or end points
- Regions where veins and arteries end (finger tips/toe tips) ||| end points/stub/end I/O devices
- Regions where branches of circulatory system takes place ||| nodes/ network nodes

Compared with the existing technologies such as WANs, BANs enable wireless communication in and around the human body by means of sophisticated pervasive wireless computing devices.

Several key applications will benefit from the advanced integration of BANs and emerging technologies or update in present wireless technologies.

- Remote health/fitness monitoring: Health and motion information are monitored in real-time, and delivered to nearby diagnosis or storage devices, through which data can be forwarded to off-site doctors for further processing.
- Military and sports training: For example, motion sensors can be worn at both hands and elbows, for accurate feature extraction of athletes' movements.
- Interactive gaming: Body sensors enable gaming freaks to perform actual body movements, such as boxing and shooting, that can be a feedback to the corresponding gaming console, thereby enhancing their entertainment experience.
- Personal information sharing: Private or business information can be stored by body sensors for daily life applications such as shopping and information exchange.
- Secure authentication: This application involves resorting to both physiological and behavioural biometric schemes, such as facial patterns, finger prints and iris recognition. The potential problems such as proneness to forgery and duplicability have motivated the investigations into new physical/behavioural

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

characteristics of the human body, e.g., Electroencephalography, gait, and multimodal biometric systems.

II. NETWORKING TERMINOLOGIES

Before moving into the simulation of BAN, let us shed some limelight on the following networking technologies:

- Network simulation tool [3]
- OSPF [4]
- Areas in OSPF [5]
- Central router, nodes and stubs [6]
- Handshaking [7]
- Encryption [8] and network security [9]

A. Network Simulation Tool (NS tool)

In communication and computer network research, network simulation is a technique where a program models the behaviour of a network either by calculating the interaction between different network entities using mathematical formulae or actually capturing and playing back observations from a production network. The behaviour of the network and its attributes can be monitored and modified in a controlled manner using network simulation tool. In our paper, we are using GNS3 as the network simulation tool. It allows the combination of virtual and real devices, used to simulate complex networks.

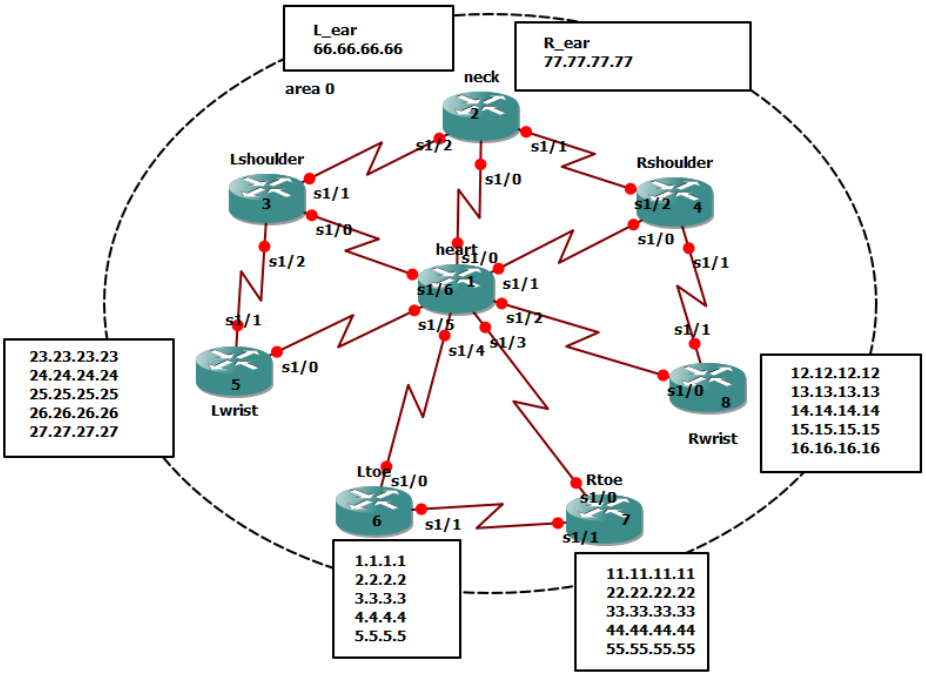

Figure 1 Network architecture of a BAN network

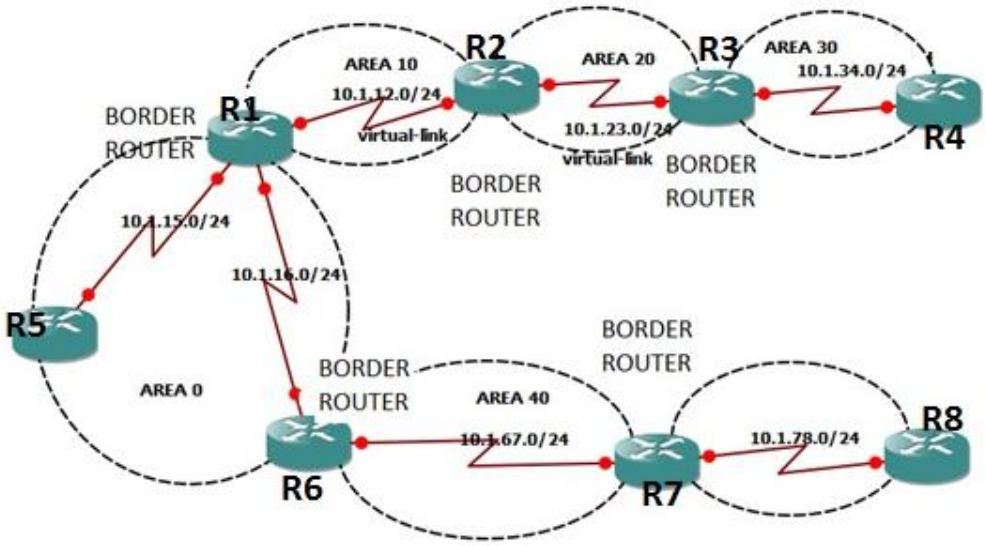

Figure 2 Inter-body communication

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

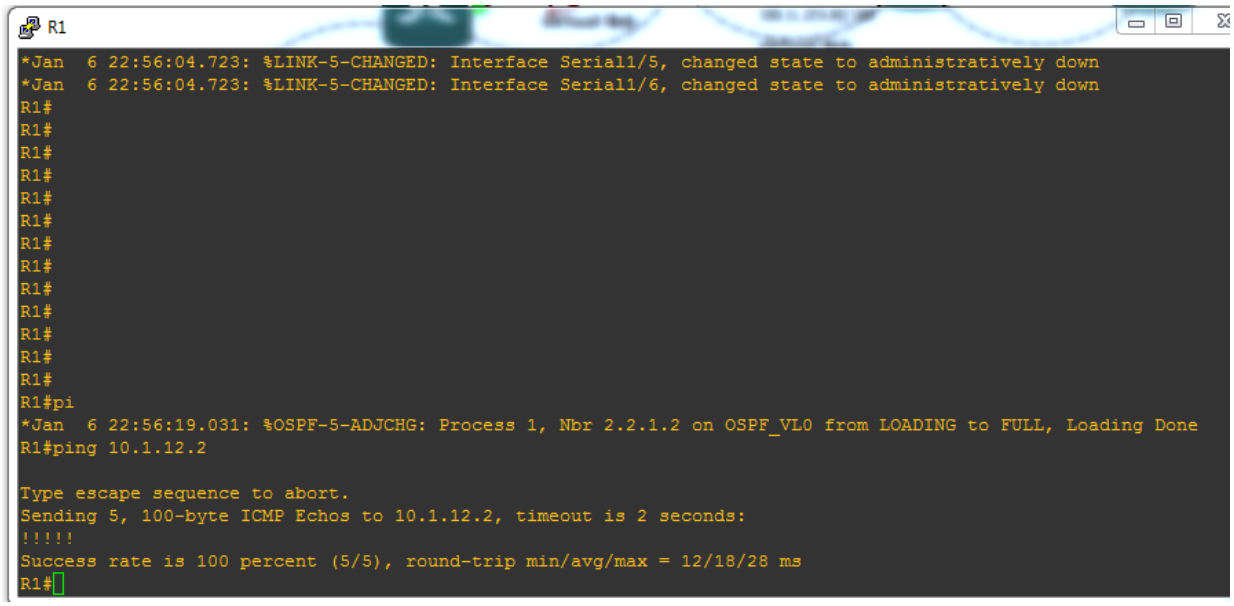

Figure 3When Border Router R1tried to ping R2

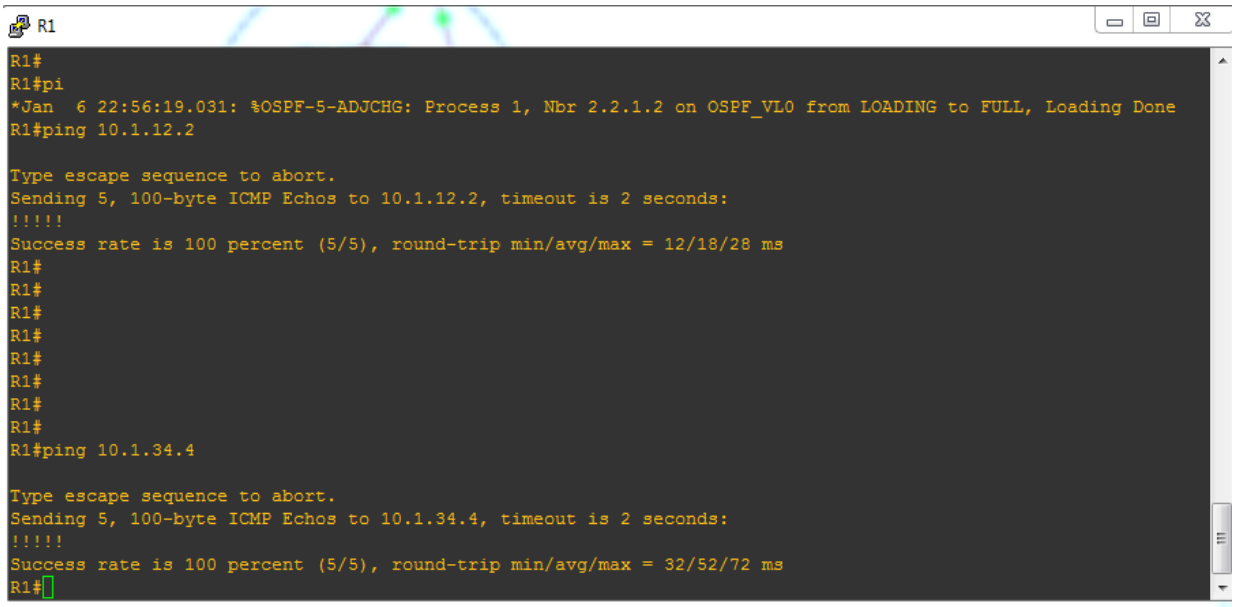

Figure 4 Area 0 was able to establish communication with the stub router R4 in area 30 by using virtual link; by 100% transfer of packets when pinged

B. OSPF

Open Shortest Path First (OSPF) is a dynamic routing protocol. The main job of a routing protocol is:

- Advertise networks
- Learn networks
- Verify whether the routing protocol is still valid.

OSPF uses a link state routing (LSR) algorithm and falls into a group of Interior Gateway Protocols (IGPs) operating within a single autonomous system (AS). An OSPF is divided into areas that are logical grouping of hosts and networks. Area 0 is called the backbone area and forms the core of the OSPF network.

C. Areas in OSPF

- Backbone area – Backbone area (also known as area 0) forms the core of an OSPF network. All other areas are connected to it. The backbone area is responsible for distributing routing information between non backbone areas. The backbone must be contiguous but need not be physically contiguous. Backbone can be established and maintained through the configuration of virtual links.
- Stub area – it is the area which does not receive any route advertisements external to the Autonomous System (AS). It is categorised into:
  i. Not-so-stubby-area
  ii. Totally stubby area

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

iii. NSSA totally stubby area

- Transit area – it is an area with two or more OSPF border routers and is used to pass network traffic from one adjacent area to another. This transit area does not originate this traffic and is not the destination of such traffic.

D. Central router network, nodes and stubs

A central router has the following features:

- It is placed centrally so that all nodes or end points are approximately equidistant from it (for better performance)
- It is the most powerful router
- High memory and computing capability
- Always placed in the centre of a star topology

A network node is either a connection point, redistribution point or a communication end point. Many I/O devices can be connected to a node.

A stub network is a computer network or a part of an internetwork, with no knowledge of other networks, which will typically send much or all of its non-local traffic out via a single path, with the network aware of only a default route to non-local destinations.

E. Handshaking

In information technology, telecommunications and related fields, handshaking is an automated or semi-automated process of negotiation that dynamically sets parameters of a communication channel established between two entities before normal communication over the channel begins.

F. Encryption and Network Security

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can access it.

Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their task without intrusion.

III. SIMULATION AND RESULTS

Figure 1 shows the network architecture of a BAN network, with each router configured with OSPF routing protocol and enclosed within an area ‘n’; where n=0 for backbone area and n=1,2,3.... (for other areas). Region of the heart is considered to be the central router with other routers connected to it in star topology.

Certain names and router number is assigned to each router to make simulation and execution more systematic as shown in table 1.

These routers are interconnected using serial ports ‘Sx/y’ where x=0,1,2,....,n and y=0,1,2,....,m.

Certain end points are created as interface loopbacks as shown in figure 1. They are:

- 1.1.1.1
- 2.2.2.2
- 3.3.3.3
- 4.4.4.4
- 5.5.5.5
- 11.11.11.11
- 22.22.22.22
- 33.33.33.33
- 44.44.44.44
- 55.55.55.55
- 12.12.12.12
- 13.13.13.13
- 14.14.14.14
- 15.15.15.15
- 16.16.16.16
- 23.23.23.23
- 24.24.24.24
- 25.25.25.25
- 26.26.26.26
- 27.27.27.27
- 66.66.66.66
- 77.77.77.77

Where, 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4 and 5.5.5.5 represent 32-bit addresses of 5 toes (left).

11.11.11.11, 22.22.22.22, 33.33.33.33, 44.44.44.44 and 55.55.55.55 of 5 toes (right).

66.66.66.66 Represents the 32-bit address of left ear lobe.

77.77.77.77 represents the 32-bit address of right ear lobe.

23.23.23.23, 24.24.24.24, 25.25.25.25, 26.26.26.26 and 27.27.27.27 represent 32-bit addresses of left hand fingers.

12.12.12.12, 13.13.13.13, 14.14.14.14, 15.15.15.15 and 16.16.16.16 represent the 32-bit addresses of right hand fingers.

Table 1Router names and numbers assigned to each router according their location

Router name	Router region on the body	Router number
Heart	Near the heart	1
Neck	Neck	2
Lshoulder	Left shoulder	3
Rshoulder	Right shoulder	4
Lwrist	Left wrist	5
Rwrist	Right wrist	8
Ltoe	Left toe	6
Rtoe	Right toe	7

Figure 2 shows inter-body communication whereas figure 1 shows intra-body area network. Here the host acts as area 0 or backbone area and the other areas are configured with area n, n=!0. Virtual links are created to connect area 0 with other areas. This can be done by configuring Border

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

Routers of each area with virtual links and these have the capability to act as a bridge in case of inter-body communication. The data packets are encrypted using encryption algorithms for secure and intrusion free exchange of packets. A particular security password is set for inter-body communication and it happens only through handshaking.

Figure 3 shows the simulation result when the Border Router R1, which can be a node or any end point of area 0 tried to ping R2 (Border Router of area 10), there was 100% packet transfer rate thereby successfully establishing interbody communication.

Figure 4 shows how area 0 was able to establish communication with the stub router R4 in area 30 by using virtual link; by 100% transfer of packets when pinged.

IV. CONCLUSION

In our previous paper titled "Concepts and study of wireless BAN using Bluetooth/IEEE 802.11n", we had proposed a Body Area Network system analogous to the human circulatory system. The major challenge regarding the proposal was its simulation and implementation. In this paper, have successfully simulated the BAN architecture using OSPF routing protocol, virtual links and security passwords. This successful simulation has opened the doors for implementation of BAN which will be done by Konigtronics (OPC) Pvt. Ltd. It will be mainly restricted to bio-medical sensors; which is the need of the day.

REFERENCES

[1] Conceptual study of wireless BAN using Bluetooth/IEEE 802.11n - http://www.ijarcce.com/upload/2016/november-16/IJARCCE%2084.pdf
[2] A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation - E Jovanov, A Milenkovic, C Otto… - Journal of …, 2005 - jneuroengrehab.biomedcentral.com
[3] GNS3 | The software that empowers network professionalshttps://www.gns3.com/
[4] Open Shortest Path First (OSPF) - Ciscowww.cisco.com › ... › Cisco IOS Technologies › IP Routing and Services › IP Routing
[5] What Are OSPF Areas and Virtual Links? - Cisco-www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html
[6] What is a stub network? - 29435 – The Cisco Learning Network-https:/learningnetwork.cisco.com/thread/29435
[7] TCP 3-Way Handshake (SYN,SYN-ACK,ACK) - InetDaemon's IT ...www.inetdaemon.com › TUTORIALS › INTERNET › TCP
[8] What is encryption? - Definition from WhatIs.com - SearchSecuritysearchsecurity.techtarget.com › ... › Network security
[9] SANS Institute Network Security Resources-https://www.sans.org/network-security/

BIOGRAPHIES

Vishesh S born on 13th June 1992, hails from Bangalore (Karnataka) and has completed B.E in Telecommunication Engineering from VTU, Belgaum, Karnataka in 2015. He also worked as an intern under Dr Shivananju BN, Department of Instrumentation, IISc, Bangalore. His research interests include Embedded Systems, Wireless Communication and Medical Electronics. He is also the Founder and Managing Director of the company Konigtronics Private Limited. He has guided over a hundred students/lecturers/interns/ professionals in their research works and projects. He is also the co-author of many International Research Papers. Presently Konigtronics Private Limited has extended its services in the field of Real Estate, Webpage Designing and Entrepreneurship.

Manu Srinath hails from Bangalore (Karnataka); he has completed B.E in Telecommunication Engineering from VTU, Belgaum, Karnataka. His research interests include networking, image processing and cryptography. He is the Executive Officer at the company Konigtronics (OPC) Pvt. Ltd.

Sneha Gopinath hails from Bangalore (Karnataka); she has completed B.E in Information Science Engineering from VTU, Belgaum, Karnataka. Her research interests include Computer Networks, Database Management Systems and Management of Information Systems. She is currently working as a Programmer Analyst at Cognizant Technologies Solutions.

Pranava Karanth R hails from Kundapura, Karnataka. He is currently pursuing B.E in Telecommunication Engineering at K.S Institute of Technology. His research interests include embedded systems and networking.