IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 3, March 2019

Session Secured Attack Detection Scheme for Network Communication

Mahesh R Khairawadagi[1], Pooja Ganesh[2], Vanitha Raju[3], Nalini MK[4]

Student, BE, Department of ISE, BMSCE, Bangalore, India[1,2,3]

Assistant Professor, Department of ISE, BMSCE, Bangalore, India[4]

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. 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). The later constitutes the inter-body communication system. 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 encrypted by various encryption policies and algorithm. This would avoid the intruders from stealing TOP-SECRET data/information. GNS 3 tool is used for implementing routing and cryptography on the network.

Keywords: Wireless Body Area Network (WBAN), Autonomous System (AS), Autonomous System Number (ASN)

I. INTRODUCTION

There is a need for a separate internetwork in case of military applications. 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.

II. PROBLEM STATEMENT

Any Country consisting of a huge Border or Area would contain a large amount of military, air force and navy personnel. They may be commissioned to operate even at remote areas, away from the national capital or military base communication between these nodes is of top most importance a network. needs to be setup to security exchange information between the nodes these men need to be monitored carefully, to increase these efficiency in serving the nation health monitoring of these mean by embedding various body sensors and encrypting the data between the nodes is of top most priority.[1]

III. REQUIREMENTS SPECIFICATION

A. Functional Requirements

i. A sophisticated network consisting of sensors at nodes designed to operate autonomously and to connect to various other sensors and appliances.
ii. Controlled redundancy in the network and load balancing.
iii. Effective dynamic routing protocols on routers.[2]
iv. Static routing and tunnels configured wherever necessary.

B. Non-functional Requirements

Non-functional requirements play the behavior performance of the system at its critical stages.

i. Provision has to be made to accommodate huge loads of data.
ii. A buffer to enrich processing at critical stages.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 3, March 2019

iii. Provision of adding new links and expanding the network in case of saturation.
iv. Encryption algorithm for secure transfer data.

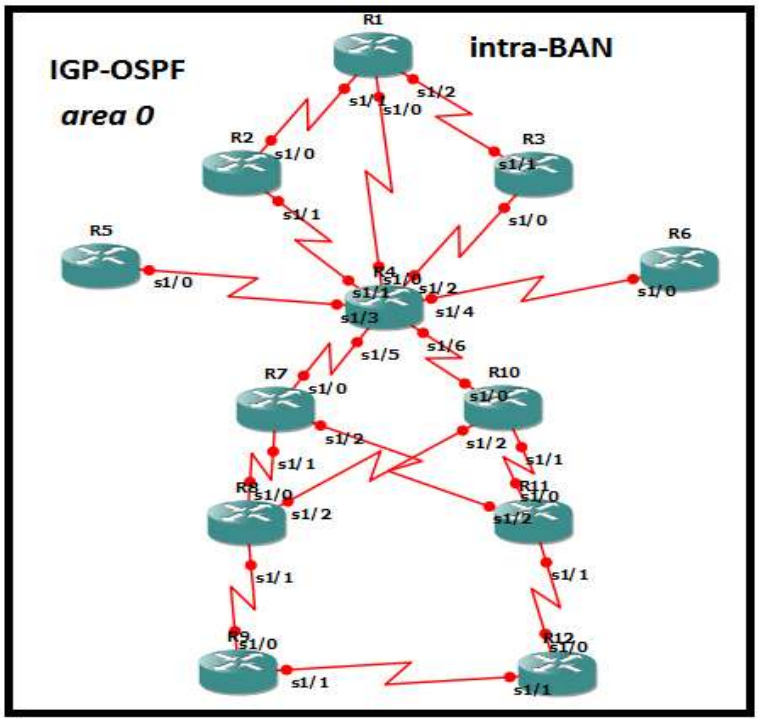

Figure 1 shows an intra-body network

IV. INTRABODY NETWORK

Intra body network consists of sensors and other elements embedded on or inside the human body. [3] These form the nodes of the network and are interconnected by links. A Body Area Network is constructed to interconnect the nodes, thereby exchanging important information and bringing about the real-time concept of sensors inter-dependability. Figure 1 shows an intra-body network.

```
neck#sh ip ospf
 Routing Process "ospf 100" with ID 10.1.12.1
 Start time: 00:10:48.080, Time elapsed: 00:21:44.388
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 --More--
```

Figure 2 shows the configuration commands on selected routers of the Body Area Network.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 3, March 2019

Routers are placed at each node to allow the packets to traverse throughout the network. OSPF is configured on the network to allow routing of packets, best path selected by the protocol. Static routes are configured between the nodes of interest. [4] Figure 2, 3 and 4 shows the configuration commands on selected routers of the Body Area Network. For remote access of the routers, telnet is configured and figure 5 shows an attempt to gain remote access using username and password.

```
Chest#sh ip ospf
 Routing Process "ospf 100" with ID 10.1.23.2
 Start time: 00:12:03.708, Time elapsed: 00:21:50.252
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 --More--
```

Figure 3 shows the configuration commands on selected routers of the Body Area Network.

```
abdomen#sh ip ospf
 Routing Process "ospf 100" with ID 10.1.23.3
 Start time: 00:13:54.628, Time elapsed: 00:20:45.336
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 --More--
```

Figure 4 shows the configuration commands on selected routers of the Body Area Network.

V. INTERBODY NETWORK

Inter body network constitutes a huge network of many intra-body networks connected to share information in a secured way. Inter-body network is realized and configured as shown in figure 6. A tunnel is configured between routers using loopback addresses and encryption algorithm is used. As of October 2015 recommended cryptographic algorithm that satisfy minimum security requirements for technology.

i. Encryption: AES-128-CBC mode

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 3, March 2019

ii. Authentication: RSA-3072, DSA-3072
iii. Integrity: SHA-256
iv. Key exchange: DH group 15 (3072bits)

```
Chest#ping 10.1.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/40 ms
Chest#telnet 10.1.23.2
Trying 10.1.23.2 ... Open


User Access Verification

Username: dry
Password:
Abdomen>en
Password:
Password:
Abdomen#
```

Figure 5 shows an attempt to gain remote access using username and password.

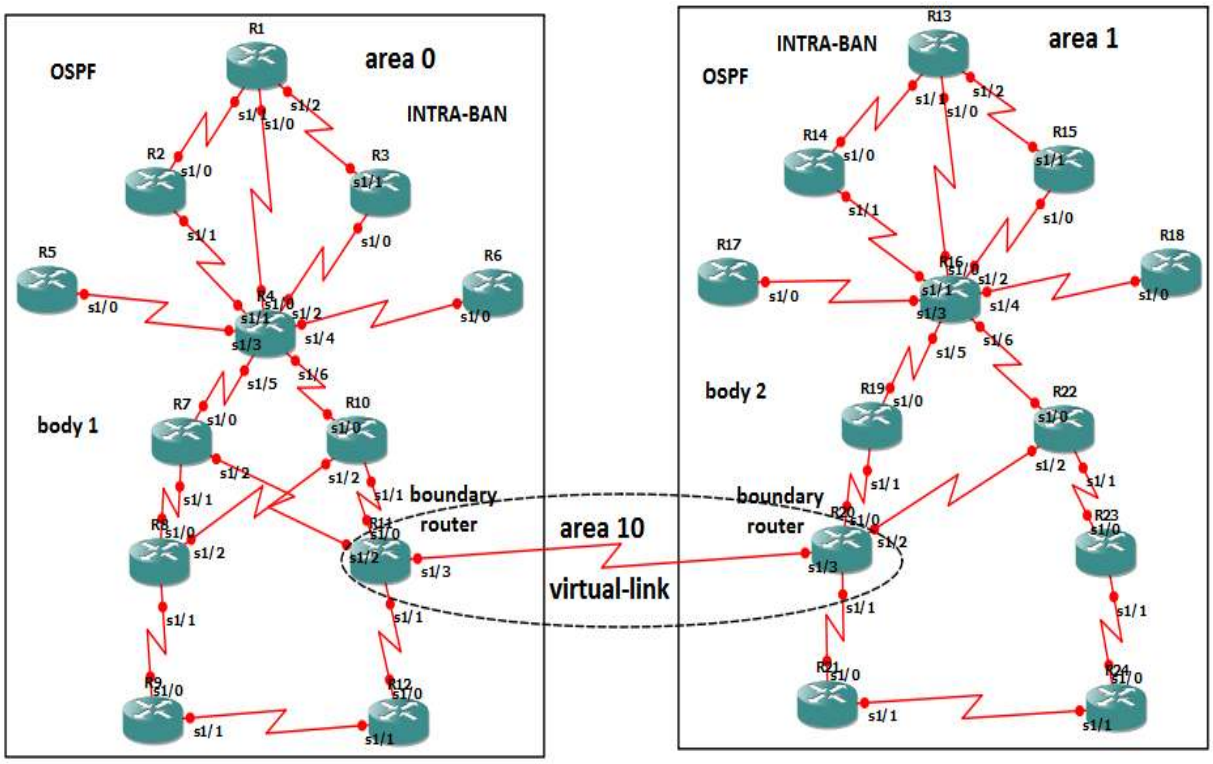

Figure 6 Inter-body network realization using GNS3

VI. CONCLUSION

The mechanism can inspect Network traffic in real time and effectively identify malicious nodes. Our mechanism can construct a dynamic blacklist of Network nodes, which can be used to block nodes whose trust values fall below a pre-defined threshold. A central server responsible for computing trust values of nodes and detecting malicious nodes is deployed. The mechanism can work with other security solutions such as database activity monitoring, white listing, and data loss prevention to strengthen the security of the network and infrastructure. Session based encrypt is used to secure the node from the compromised attacker. Attacker request will be accepted by unique key of individual node validation process. This would avoid the intruders from stealing TOP-SECRET data/information.

REFERENCES

[1]. 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.
[2]. D. Boyle, T. Newe, "Security protocols for use with wireless sensor networks: A survey of security architectures," in Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on, pp. 54-54, 2007.
[3]. E. Jovanov, A. Milenkovic, C. Otto, P. De Groen, B. Johnson, S. Warren, G. Taibi, "A WBAN system for ambulatory monitoring of physical activity and health status: applications and challenges," in 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference, pp. 3810-3813, 2006.
[4]. WBAN- An Experimental Approach Vishesh S1 , Arjuna C Reddy2 , Nagapragathi SV3 , Pooja Manjunath3 , Kavya P Hathwar4 , Anusha U5- International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 8, August 2017, DOI10.17148/IJARCCE.2017.6851

BIOGRAPHIES

Mahesh R Khairawadagi- Student, BE, Department of ISE, BMSCE, Bangalore, India

Vanitha Raju- Student, BE, Department of ISE, BMSCE, Bangalore, India

Nalini MK- Assistant Professor, Department of ISE, BMSCE, Bangalore, India

Pooja Ganesh- Student, BE, Department of ISE, BMSCE, Bangalore, India