ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 3, No.15 , May 2015
ISSN : 2322-5157
www.ACSIJ.org

Mitigating Intrusion and Vulnerabilities in Cognitive Radio Networks

I. Ohaeri, O. Ekabua, B. Isong, M. Esiefarienrhe and M. Motojane

North-West University, Computer Science Department
Mafikeng Campus, South Africa
oh.ifeoma, ekabuao {@yahoo.com}, isongb77@gmail.com, micheal.esiefarienrhe, m.motojane{@nwu.ac.za}

Abstract

The deployment of Cognitive Radio Networks has been greatly hindered in spite of its potentials by the rate at which intrusions and vulnerabilities replicate within every domain of the network. Cognitive Radio Network is expected to drive the next generation wireless networks that can optimize the use of spectrum due to its unique and dynamic properties, but the high rate of intrusions has frustrated all the efforts of this promising network. Hence, there is need for a more investigation on better security measures to be employed in the network. Therefore, this paper proposes the design and implementation of an Intrusion Detection and Prevention Framework (IDPF) that monitors and analyses all inbound and outbound traffic in CRN in order to mitigate intrusions and vulnerabilities that increases on daily basis against CRN for a reliable and secured network. This will improve the rate of deployment of Cognitive Radio Networks.

Keywords: *Cognitive Radio Networks, Security, Intrusion Detection, Intrusion Prevention.*

1. Introduction

The growing need to standardize the knowledge, information and data structures relating to the spectrum environment enables mechanism and automated methods for spectrum access. This has led to the innovation of cognitive radio (CRs). Cognitive radios are a new idea that was ushered in by the wireless medium as the beginning of a new modality in wireless networks. They gain awareness of their environment and surroundings and are capable of adapting their behavior accordingly. Also they possess unique and dynamic properties that increase the effectiveness and efficiency of wireless spectrum usage. The properties includes: self-configuration, self-healing, self-optimization, and self-protection. Consequently, several intrusions and vulnerabilities have arisen due to these unique cognitive abilities. The IDPF security mechanism designed in this paper can be used in the cognitive radio network management system in order to provide quality and secured services to end users. The IDPF application can keep records of all network users' processes and operations in real time [1].

Therefore, this paper focuses primarily on the design and implementation of the IDP Framework that is capable of monitoring and analyzing all network packets transmitted in and out of the network. By this measure, all intrusions and vulnerabilities that replicate on daily basis against cognitive radio networks can be mitigated.

2. Related Work

Mechanisms for protecting networks and various infrastructures of devices that must be put in place to achieve an efficient quality of service is the essence of network security. Avenues to protect cognitive radio network cuts across intrusion and vulnerabilities detection and other security infrastructures [2].

The radio (electromagnetic) spectrum is a limited natural resource that grants access to wireless devices, and the increase and efficiency of these wireless devices operating in unlicensed bands has caused overcrowding of spectrum bands. Intelligent cognitive radio devices senses, and identifies "white space" (vacant or unused areas) in the spectrum that can be utilized for communications, whereas, hardware-based wireless and conventional hardware devices has the ability to only access specific area of the radio spectrum [3].
Cognitive radio emerged as a technology that enables effective utilization of a new spectrum. The spectrum utilization scheme is referred to as distributed spectrum sensing and sharing (DSS). Data and information management in cognitive radio network operates in a distributed form. Spectrum resources which are limitless natural resources are shared by both licensed and unlicensed users. DSS helps to identify unused spectrum bands (white spaces) without causing any form of interference to licensed or primary users.

The information gathered from spectrum sensing is used by dynamic spectrum to allocate or distribute the free channels (vacant or unused areas) for the cognitive radio nodes that are demanding or striving for it [4]. CRN is first aware of its environment and capabilities. It is capable of independently changing its physical layer behavior and present environment [5]. It is able to perform the adaptation strategy which is totally based on cognitive spectrum. Having these capabilities, when the spectrum environment alters within the cognitive radio users, it is able to sense these changes and immediately make adjustments. The physical layer settings like transmission power, channel detection and selection changes automatically and independently meet the constraints and quality of assurance (QoS) requirements of other spectrum users [6]. The cognitive radio network management system should be able to provide a security scheme or mechanism that will establish secured communications, and record the operations processed by the users to determine intrusions and check malicious activities, for the purpose of verification, validation and detection of malicious users [7].

The security threats in cognitive radio entail majorly illegal information injection and forging of information transmission. The radio environment map (REM) fetches several characteristic data from a large spectrum sensing cognitive users. Attackers can maliciously falsify local spectrum sensing data to confuse the receiver in other to lunch attacks which can prompt the receiver to make wrong spectrum accessing decision [8]. A secure computer network is a trusted and reliable system that functions appropriately. Normally, information technology security is usually analyzed on the basics of confidentiality, integrity and availability. In the 1980s, computer systems had been equipped already with an audit capability. The operating system can be able to collect system-wide attributes using the audit trace capability. The analysis been done by humans became very tedious as collected events and activities increased. An automated method of collecting and analyzing data to produce vital information to check network intrusions became very necessary. However, the birth of this automated mechanism or tool became the foundation or root of intrusion detection.

This automatically calls for an intrusion detection security mechanism that is capable of; monitoring and examining packet traffic to discover its source and destination IP addresses together with source and destination ports; identifying network sessions and examine dialogs between the systems for multi-packet activity, examining and responding to entire conversations between hosts, using knowledge of protocols and network sessions to analyze traffic to discover malicious activities. This research intends to use intrusion detection and response model to provide those important capabilities for understanding and responding to attacks to ensure security in cognitive radio networks [9].

Apparently, work has been done to achieve network security but much effort is still needed to achieve a reliable security infrastructure which guarantees adequate quality of service (QoS), and maximum security [10].

3. Framework Design

The framework is designed using OPNET tool version 14.5, and also the experiments were performed in OPNET environment. Relevant parameters, statistics and required scenarios that describe the obtained results are also provided to validate the proposed concept. The various scenarios includes: firewall, No Firewall, firewall VPN, IP Ping, and Traffic flow. Each of the scenarios are demonstrated to show the detection and prevention capabilities of the framework.

The IDPF has several capabilities which include: Network monitoring, Attack detection, and prevention. The major framework components includes: Routers, Firewall, Internet Cloud, Sensor, and the Management server which carries the database system. The Management server also provides mechanism such as security policy, CRN attack signature base, decision engine and response mechanism. Figure 1 above clearly presents the overflowing of traffic from different network domains which include: the primary users' network, the secondary users' network, and intruders' network. The different user domain exchange communication with the management server over the CRN.

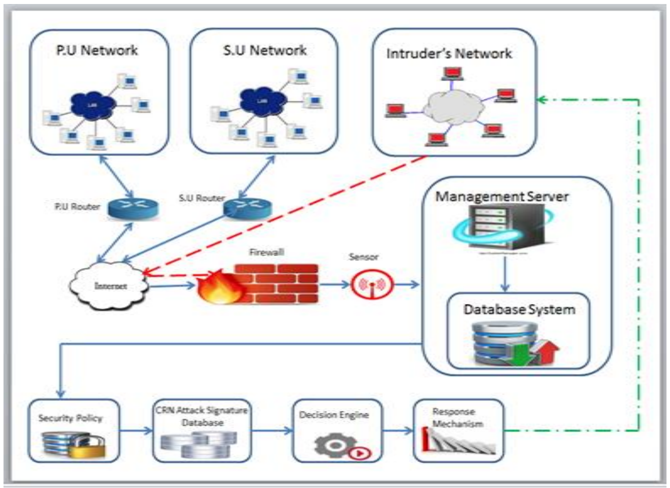


Fig. 1. IDP framework

The exchange of communication between the management server and the PUs and SUs are linked by PU Router and SU Router respectively. The management server is accessed over the internet. Despite the security level provided by any network host, intruders or attackers always look for a means of interrupting the communication and traffic flow. Hence, the dotted line in figure 1indicates the intruders' or attackers' attempts to penetrate the management server. Nevertheless, the firewall interrupts and hinders the intruders' activities. In the IDPF above, the firewall operates as the intrusion prevention system, as it stops and blocks all suspicious activities detected via the firewall, while the sensor acts as the eye of the network, it monitors, and analyses all incoming traffic from the attackers network and blocks all suspicious activities detected via the firewall. The IDPF consists of both the primary users' network, the secondary users' network, and the attackers' network. Each of the networks has its own user domain that is connected to the CRN management server via the router over the internet. Public domain and users can also use applications and services provided by the public cloud – internet cloud. The internet cloud is a public cloud that is accessible publicly. The cloud is used in the framework because it has abilities to run a program on many connected computers and networks at the same time. Also, it helps in the sharing of available resources over a network as well as maximizing the effectiveness of the shared resources. It enables users to access systems using a web browser regardless of their location or the device they use. Users can connect from anywhere due to the position of the infrastructure.

Moreover, the CRN firewall protects the network against intrusions and vulnerabilities. The sensors serves as the "eyes" of the network with the major responsibility of monitoring the traffic flow and the data packets transmitted (routed) to the network. The security policy is consulted whenever there is a request for network access. The user profile is verified with credentials captured in the network database to ensure that a user is who he or she claims to be. All systems and network intrusions are specified in the attack signature database. The decision engine determines whether to grant or deny access and an automated response can be generated to block off the attacker and stop the attacks from escalating.

4. Experimental Setup

We used OPNET 14.5 to build the designed IDPF. OPNET offers several benefits as it provides a GUI for different topologies design which permits a realistic simulation of networks, and has a performance data collection and display module. OPNET has a wide confidence in the validity of the results it produces. The explicitly generated traffic in OPNET simulation enables research on data filtering and intrusion detection strategies. Table 1 summarizes the profiles and scenarios used in the simulation of IDP Framework, while Table 2 presents the parameters used.

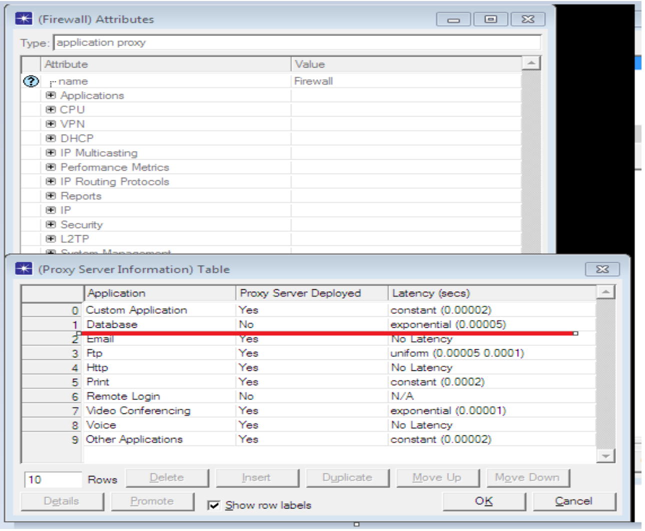
Table 1: Summary of the profiles and scenario

Scenarios	Profile
No Firewall	SABC,CRN web browser
Firewall	SABC, CRN web browser
Firewall_VPN	SABC, CRs
PING	SABC, Researcher
Traffic Flow	SABC, Multiuser

Table 2: Framework parameters

Parameter	Values
Simulator	OPNET Tool
Simulation Area	1500*1000
Simulation time	600 sec
Traffic Type	HTTP, DB Query
Transmission Power	0.005w
Protocol	IPv4

The IDPF is designed in assumption using Figure 1 and 2. It is designed to prevent unsupported applications from having access to the CRN Sever. The aim is to ensure that no client gets access to the network without proper authentication from the database server. Figure 2 indicates application setup for firewall to support no database proxy information. As indicated from the red line, the database responds to 'No proxy' server deployed. By this we employ the monitoring, detection and prevention technique as defined in the IDP framework.



(Firewall) Attributes

Type: application proxy

Attribute	Value
name	Firewall
⊞ Applications	
⊞ CPU	
⊞ VPN	
⊞ DHCP	
⊞ IP Multicasting	
⊞ Performance Metrics	
⊞ IP Routing Protocols	
⊞ Reports	
⊞ IP	
⊞ Security	
⊞ L2TP	

(Proxy Server Information) Table

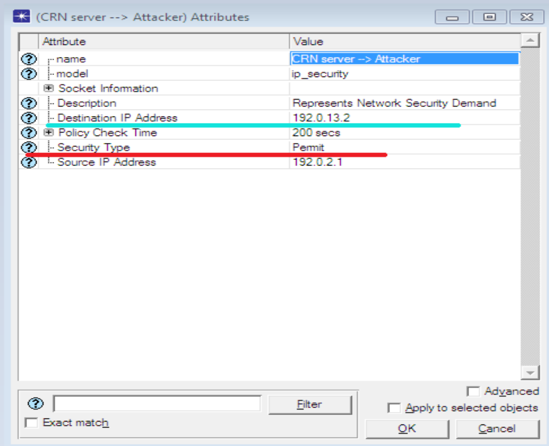
	Application	Proxy Server Deployed	Latency (secs)
0	Custom Application	Yes	constant (0.00002)
1	Database	No	exponential (0.00005)
2	Email	Yes	No Latency
3	Ftp	Yes	uniform (0.00005 0.0001)
4	Http	Yes	No Latency
5	Print	Yes	constant (0.0002)
6	Remote Login	No	N/A
7	Video Conferencing	Yes	exponential (0.00001)
8	Voice	Yes	No Latency
9	Other Applications	Yes	constant (0.00002)

10 Rows

☑ Show row labels

Fig. 2. Firewall attributes

In Figure 3 the parameters for IP Ping traffic are shown. The red line indicates that the security type attribute is set to permit; by this, the traffic flow will be traced and recorded. As every node have its own IP address as shown by blue line.



(CRN server --> Attacker) Attributes

Attribute	Value
name	CRN server --> Attacker
model	ip_security
⊞ Socket Information	
Description	Represents Network Security Demand
Destination IP Address	192.0.13.2
⊞ Policy Check Time	200 secs
Security Type	Permit
Source IP Address	192.0.2.1

□ Advanced
Filter
□ Apply to selected objects
□ Exact match
OK
Cancel

Fig. 3. Ping Attributes

5. Creating CRN

Creating a CRN domain is required as a platform for IDPF implementation. Figure 4 below shows the CRN, which represents the 'No firewall scenario', it assums that there is no attacks in the network.

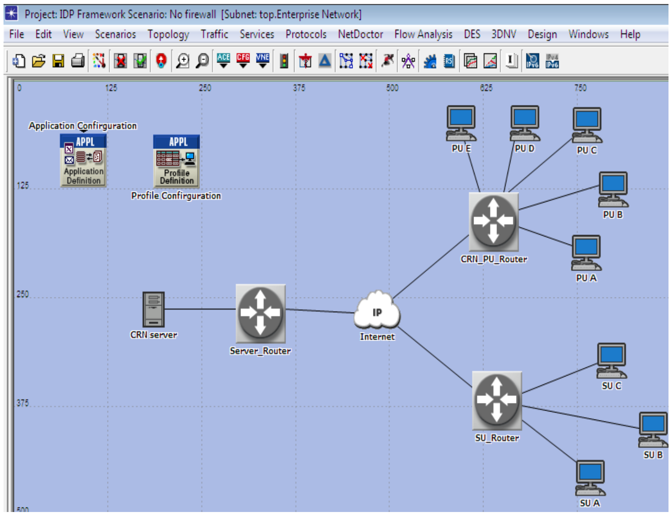
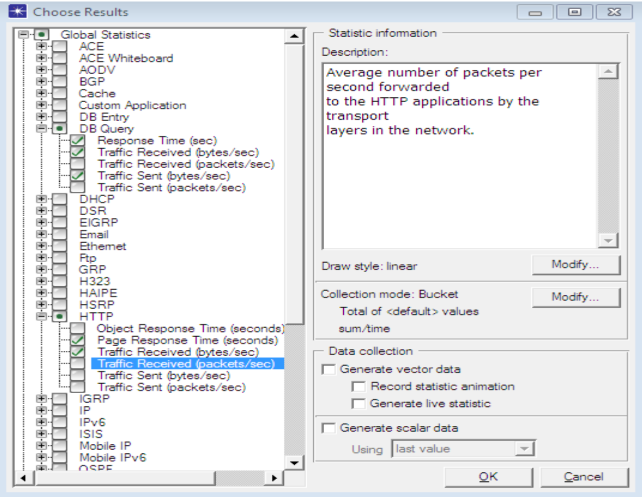

Project: IDP Framework Scenario: No firewall [Subnet: top.Enterprise Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
0
125
250
375
500
625
750
Application Confirguration
APPL
Application Definition
APPL
Profile Definition
Profile Confirguration
PU E
PU D
PU C
PU B
PU A
CRN_PU_Router
CRN server
Server_Router
IP
Internet
SU C
SU B
SU A
SU_Router

Fig.4 CRN general architecture

Above all, there is a building block, called the 'server', which represent the IDP techniques and holds all information regarding the CRN. The server is accessed over the Internet by both the PU and SU who have different priviledges. The 'No_firewall testing scenario' represent the smooth network, where there are no threads around the enviroment. This scenario has some application confirgurations which support all services from one node to another, such as web browsing (Hearvy HTTP 1.1) indicating a web browser application performing hearvy browsing using HTTP

5.1 Choosing Statistics

The following figures show different statistics of simulated CRN. Figure 4.1a shows the 'global statistics' which represents the entire network. It is important to represents results by choosing the 'DB Query', HTTP as it is the applications supported by all nodes found in the network. Figure 4.2b shows the 'client statistics' which indicates the individual nodes statistics. The nodes can be any CRN client, either the PU or the SU. The statistics specify the client traffic sent or received for application HTTP and Client DB.



Choose Results

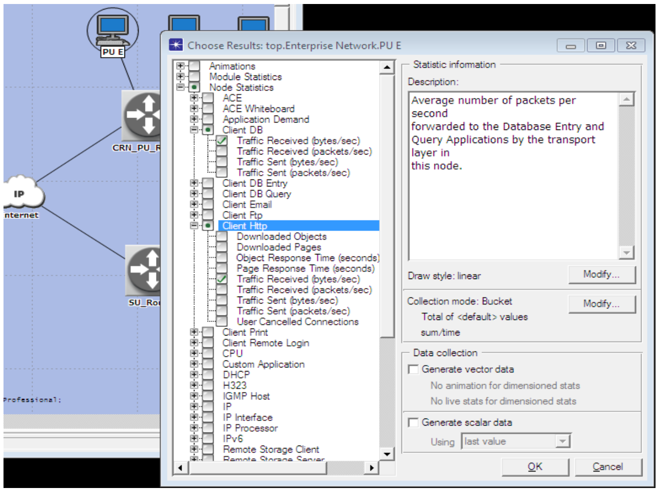
- Global Statistics
  - ACE
  - ACE Whiteboard
  - AODV
  - BGP
  - Cache
  - Custom Application
  - DB Entry
  - DB Query
    - ☑ Response Time (sec)
    - ☑ Traffic Received (bytes/sec)
    - □ Traffic Received (packets/sec)
    - ☑ Traffic Sent (bytes/sec)
    - □ Traffic Sent (packets/sec)
  - DHCP
  - DSR
  - EIGRP
  - Email
  - Ethernet
  - Ftp
  - GRP
  - H323
  - HAIPE
  - HSRP
  - HTTP
    - □ Object Response Time (seconds)
    - ☑ Page Response Time (seconds)
    - ☑ Traffic Received (bytes/sec)
    - □ Traffic Received (packets/sec)
    - □ Traffic Sent (bytes/sec)
    - □ Traffic Sent (packets/sec)
  - IGRP
  - IP
  - IPv6
  - ISIS
  - Mobile IP
  - Mobile IPv6
  - OSPF

Statistic information
Description:
Average number of packets per second forwarded to the HTTP applications by the transport layers in the network.

Draw style: linear
Modify...
Collection mode: Bucket
Total of <default> values
sum/time
Modify...

Data collection
□ Generate vector data
□ Record statistic animation
□ Generate live statistic
□ Generate scalar data
Using last value
OK
Cancel

Fig. 4.1a.Global Statistics



Choose Results: top.Enterprise Network.PU E

- Animations
- Module Statistics
- Node Statistics
  - ACE
  - ACE Whiteboard
  - Application Demand
  - Client DB
    - ☑ Traffic Received (bytes/sec)
    - □ Traffic Received (packets/sec)
    - □ Traffic Sent (bytes/sec)
    - □ Traffic Sent (packets/sec)
  - Client DB Entry
  - Client DB Query
  - Client Email
  - Client Ftp
  - Client Http
    - □ Downloaded Objects
    - □ Downloaded Pages
    - □ Object Response Time (seconds)
    - □ Page Response Time (seconds)
    - ☑ Traffic Received (bytes/sec)
    - □ Traffic Received (packets/sec)
    - □ Traffic Sent (bytes/sec)
    - □ Traffic Sent (packets/sec)
    - □ User Cancelled Connections
  - Client Print
  - Client Remote Login
  - CPU
  - Custom Application
  - DHCP
  - H323
  - IGMP Host
  - IP
  - IP Interface
  - IP Processor
  - IPv6
  - Remote Storage Client
  - Remote Storage Server

Statistic information
Description:
Average number of packets per second forwarded to the Database Entry and Query Applications by the transport layer in this node.

Draw style: linear
Modify...
Collection mode: Bucket
Total of <default> values
sum/time
Modify...

Data collection
□ Generate vector data
No animation for dimensioned stats
No live stats for dimensioned stats
□ Generate scalar data
Using last value
OK
Cancel

Fig. 4.1b. Client Statistics

The ‘Client Statistics’ consists of various information for the clients which includes the following: Client AP Association History, Client RSSI (Received Signal Strength Indicator) history as detected by the access point with which the client is associated. Client SNR (signal-to-noise ratio of the client RF session) history as detected by the access point with which the client is associated. Bytes Sent and Received (Kbps) with the associated access point). Packets Sent and Received (per second) with the associated access point.

5.2 Duplicate Scenario from CRN

The following typical usage scenarios are created from the CRN to validate the concept of this paper. This indicates the intrusion detection and prevention capabilities of the framework. This section of the paper includes different scenarios of the framework simulation using OPNET simulator. The OPNET simulator was based on the intrusion detection and prevention parameters which gave the overhead results that were analyzed in section six (6). All the relevant parameters, statistics and features required for the accumulation of the results are further described in this section. Typical usage scenarios prove the concept of understanding this research were demonstrated in this chapter. The scenarios include: Firewall, No Firewall, firewall VPN, IP Ping, and Traffic Plans.

5.2.1 Firewall Testing Scenario: This scenario was duplicated from the ‘No_firewall’ scenario for comparison of smooth network and Secured CRN network as indicated in Figure 6 below.

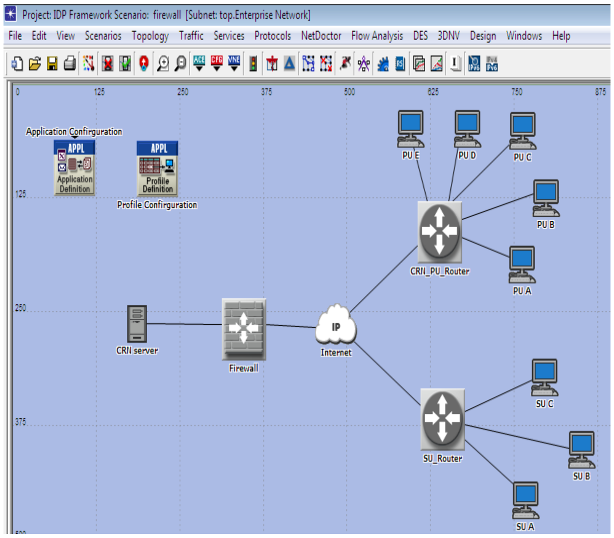

Project: IDP Framework Scenario: firewall [Subnet: top.Enterprise Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
Application Configruration
APPL
Application Definition
APPL
Profile Definition
Profile Configruration
PU E
PU D
PU C
PU B
PU A
CRN_PU_Router
CRN server
Firewall
Internet
SU C
SU B
SU A
SU_Router

Fig. 5. Firewall Scenario

Therefore, the above scenario in figure 5 above, which has different profiles created to allow both PU and SU to access applications such as DB Access, E-mail, web brousing etc. from the server. It is needed to protect database in the server from extrenal access, including both PU and SU. The only way is to add or replace the Server_Router with the firewall, and set the proxy server information of the firewall to NO. which therefore results in blocking all packets such that the firewall confirguration does not allow databased related traffic to pass through the firewall. In this way the database in the server is protected from external access.

5.2.2. Firewall_VPN Testing Scenario: Figure 6 shows the duplicated scenario from the firewall scenario, only now that the diference is that there is the external server router and the firewall.

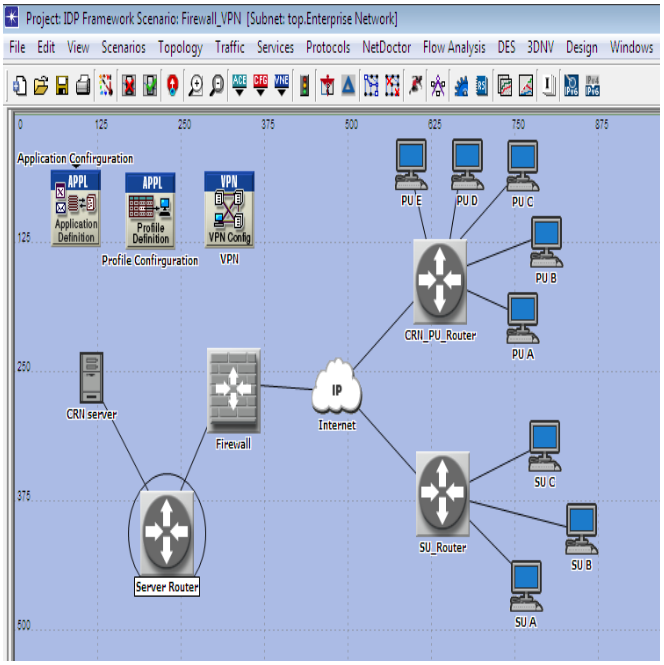

Project: IDP Framework Scenario: Firewall_VPN [Subnet: top.Enterprise Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows
Application Configruration
APPL
Application Definition
APPL
Profile Definition
Profile Configruration
VPN
VPN Config
VPN
PU E
PU D
PU C
PU B
PU A
CRN_PU_Router
CRN server
Firewall
Internet
SU C
SU B
SU A
SU_Router
Server Router

Fig. 6.Firewall VPN Scenario

From the firewall scenario, we secured the database in the server from any external access using the firewall router. Assuming that the PU needed to be active to the database that is in the server, sinse the firewall block or filters all database related traffic regardless of the source traffic. It is needed to consider Vitual Private Network(VPN) Solution. The firewall-VPN scenario was created . A virtual tunnel is used by PU to send database request to the server. As the firewall itself will not filter the traffic created by PU because the IP Packets in the tunnel will be encapsulated inside IP Datagram.

*5.2.3. IP_Ping Testing Scenario:*This scenario was duplicated from the CRN, which refer to the NO Firewall

Scenario to comapare the results from when we introduce the attacker and trace the IP adressses as indicated Figure 7 below.

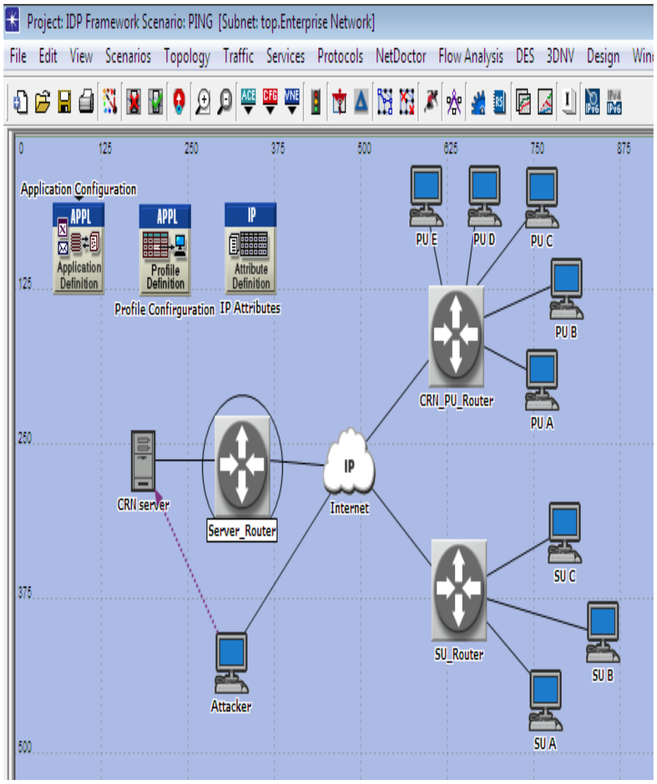


Fig. 7.IP Ping Scenario

The IP_PING scenario was created from the smooth network which is the No_Firewall scenario (CRN). Where the individual attacker attempted to intrude the server, in order to disrupt network flow, thereby coursing delays for packets transmitted in and out of the workstations. In this scenario the attacker managed to bypass authentication through the cloud so as to have access to the server, the IP PING will be traced and recoreded as the server contain the database regarding all information about known attacks, the IP address of the attcker or intruder will be recorded from the simulation log. Immediately the attack is suspected or detected the particular device or network will be blocked in order to prevent the attack and secure the CR Network.

*5.2.4. IP Traffic Flow Scenario:*The scenario was created from the 'IP Ping scenario' but with the IP security which represents the traffic flow from the server to the destination attacker as shown in Figure 8 by the red dotted line.

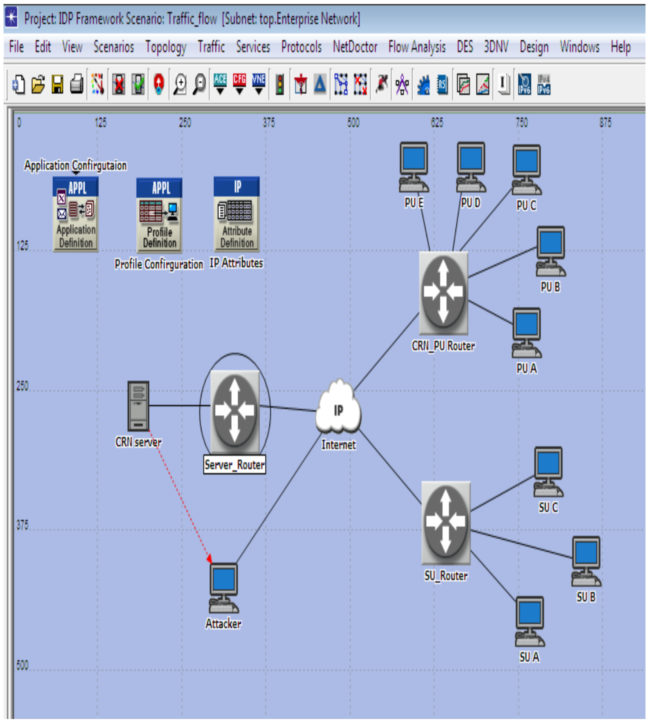


Fig. 8.Traffic Flow Scenario

This is basically the IP Security demand between the source and destination nodes. This is where the server demands authentication details from the attacker. Apparently. this measures ensures that only the right users have access to the CRN resources. However, it is only when the credentials of client are validated will they be granted network access. The security demands allow prevention mechanism to point directly to the destination node preventing it from altering, and disrupting communication flow.

6. Simulation Results

This section mainly focuses on the simulation results discussion. The goal of this chapter is to show how the detection and prevention capability can be applied to mitigate intrusions and vulnerabilities in CRN to provide security for adequate Data and Information Management. This section also provides graphics representations of the differences between several scenarios in relation to securing data and information within CRNs. More so, it presents OPNET specifically, in relation to the IDP frameworkbased on each parameter per each scenario.

6.1 Results Analysis

Within the IDP Framework there are four described scenarios, which are: No firewall, firewall, firewall_VPN, Ping and IP_Traffic Flow scenarios. Each scenario is part of the IDP Framework and it is basicaly the division modules of the IDPF which has a specific role, which is to provide segment of the global security simulations.Results were built from the simulated IDPF. And as the network was simulated, five scenario was built and all combined together to form the designed IDPF shown in Figure 1. The following result figures are built based on different statistics. The first statistics was the global statistics. In the global statistics we compared the applications for the SABC profile, from one scenario to another. Later on the results was based on the built nodes of PUs and SUs different applications, and on the database query and HTTP.

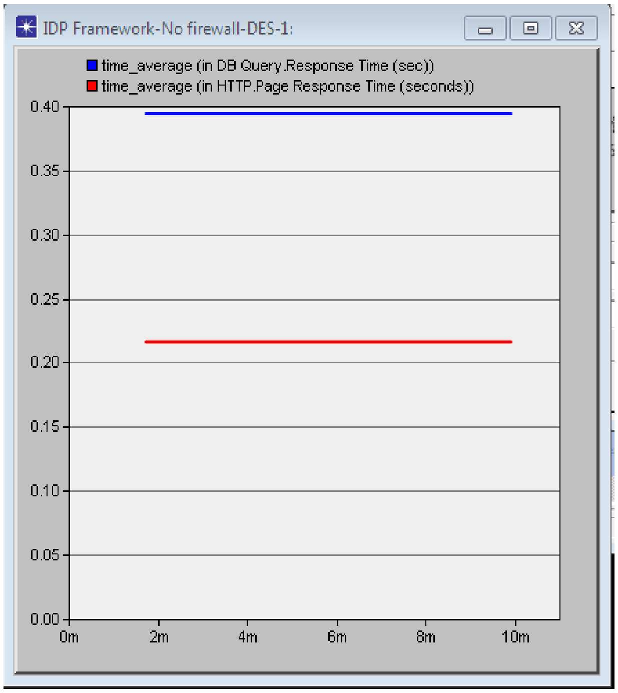


Fig.9. Smooth Network

Figure 9 displays the rate at which database query responds, and HTTP page response time, where there is no firewall. Both graphs are constant and they clearly represents the smooth network. This results are are generated from the global statistics , meaning that all networks including those that are near the CRN are represented. However the smooth network need to be secured to be able to detect intrusions and vulnerabilities in CRN.

The respective figures below displays the results representing the comparison of the four scenarios mentioned earlier which includes the: Firewall, Firewall-VPN, PING, and traffic flow. Therefore, in the smooth network in Figure 10, the traffic can be from any licensed or registered client of CRNs.

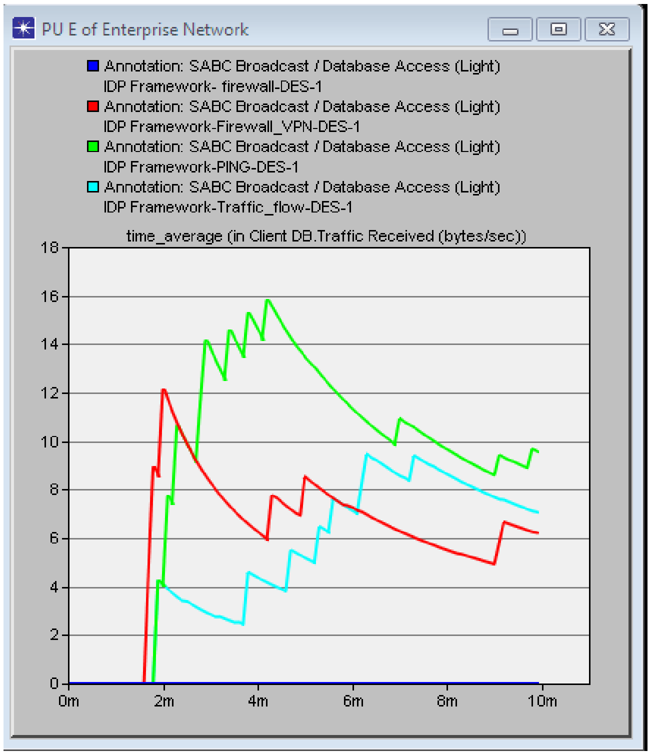


Fig. 10. PU Client DB Traffic Received

From the system parameters, we created the service profile, which is the SABC Broadcast. The profile was chosen because it has several departments which will need to use the network. The results were captured from one of the workstations of CRN, the firewall did not allow any request for the database access to pass to CRN server, whether from a device or from any other networks but in other scenarios such as firewall VPN shown in Figure 6 which allows only the PUs to have database access to the server. However, the remaining scenarios were built on the basis of the firewall-VPN in Figure6. Therefore, the results reacted based on the parameters chosen and hence the firewall allows no database access because it supports no proxy of database access for the entire client DB (PUs). The firewall actually exhibited the prevention capability as it filters all the packets and blocks the suspicious ones.

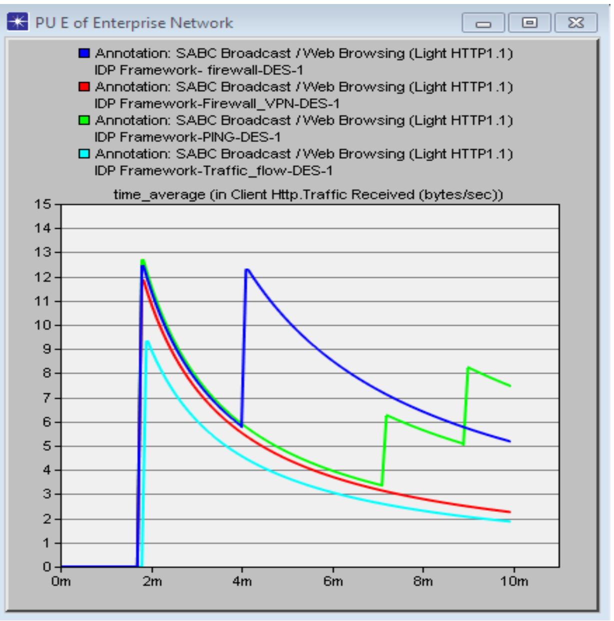


Figure 11. PU Client HTTP Traffic Received

Figure 11 and 12 shows the results derived from the PU within the CRN. They form part of the client for 'client HTTP statistics' shown in figure 4.1a and 4.2b above. It represents the traffic received in relation to supported service which is the HTTP for web browsing across the entire CRN. From the result shown in the figure 13 and 14 graphs, the traffic flow scenario in figure 10 has the least bytes of all the scenarios in simulation time, which indicates that clients acts as either source or destination, and because of the IDPF high security measure. The server connects and communicates to all the nodes within the CRN. Consequently, this causes the traffic to be slow and the rate at which the client (PUs) receives the traffic is also slow. But in the higher statistics, ranging from the simulation time at 2m to 4m, the ping scenario is the highest statistics, but which has no distanced difference between the firewall as shown in the firewall scenario in Figure 5, and firewall-VPN scenario in figure 6. This is because they are all designed based on the IDPF concept. However, in the firewall scenario in Figure 6, the client received much traffic at simulation time "4m to approximately 9m". This is because the IDPF in relation to the firewall ensured that the CRN is adequately secured from all forms of threats, attacks and vulnerabilities. Hence, there was no network disruption.

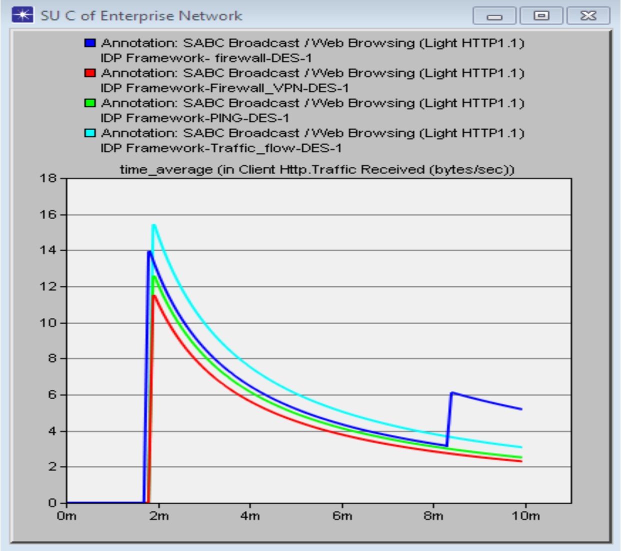


Figure 12.SU Client HTTP Traffic Received

In Figure 12, the results for the web browsing application shows that from the traffic flow scenario the SUs clients which support the HTTP applications, received traffic at higher rate compared to the firewall-VPN scenario.it received lower traffic at bytes per second as shown from Figure 17. This is caused by the role of the firewall as it filters packets passing through it. Therefore, some packets are filtered from the firewall and the procedure favours the firewall scenario. The VPN is created for PUs to access applications from the server. This private network is necessary technique that helps in preventing users from outside the CRN to have direct access to all the available resources in the CRN server.

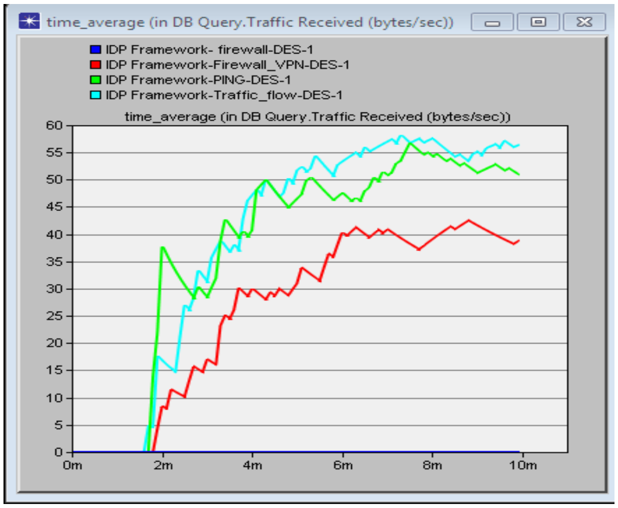


Fig. 13.Global DB Query Traffic Received

The global statistics for the entire different networks found in the IDP Framework is represented in Figure 13. We assumed that the firewall proxy to database query is deactivated by the administrators of CRN, the lower statistics shows that there is no response to database query, meaning that database in the server cannot be accessed by any of the user from CRN or even the attackers' network. The statistics for scenario firewall-VPN in figure 6are the second least from the rated bytes/sec received database traffic, because the VPN was created to allow only certain users to go and access the database in the server. For the PING and traffic flow shown in Figure 7 and 8 respectively, there is a competence of database query to be accessed as it can be received globally, the statistics is higher because of the high security requirements.

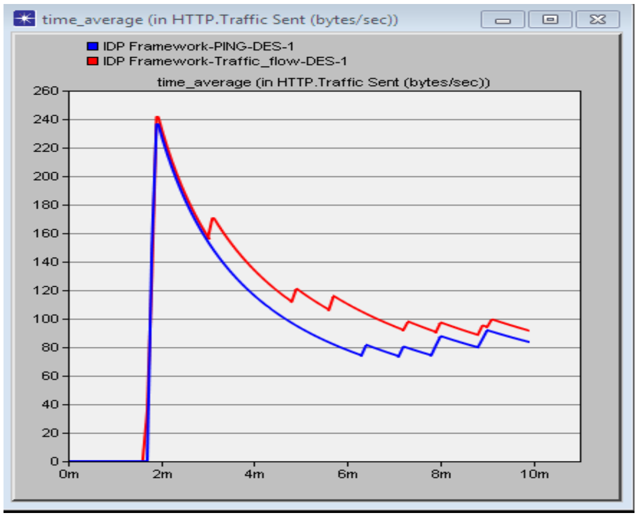
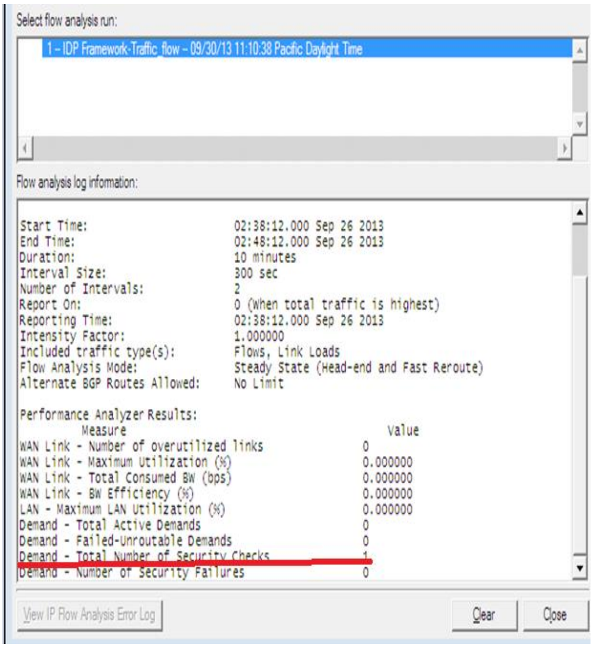


Fig. 14. Global HTTP Traffic Sent

The PING scenario and the Traffic scenario reported in figure 14 are more or less similar because they all represent the CRN basic security requirements. However the only difference is that when the network has ping attack, every route will be traced, recorded and reported so that the server will store the information about monitored nodes found suspicious. Moreover, in the case of the traffic flow which is basically the IP security, the security is high within all routes and attacks can be prevented from entering the important source nodes like the CRN server. At time average 2m to approximately 3m statistics is the same but in the traffic flow scenario the traffic sent in supported application HTTP from the server has higher statistics due to the fact that IP security focuses to the destination workstation as shown from Figure 13. This prevents attackers from accessing the source nodes or the host network. Therefore, PING only monitors and traces the entire routes in order to detect all forms of as shown in Figure 15.



Select flow analysis run:

1 – IDP Framework-Traffic_flow – 09/30/13 11:10:38 Pacific Daylight Time

Flow analysis log information:

```
Start Time:                       02:38:12.000 Sep 26 2013
End Time:                         02:48:12.000 Sep 26 2013
Duration:                         10 minutes
Interval Size:                    300 sec
Number of Intervals:              2
Report On:                        0 (When total traffic is highest)
Reporting Time:                   02:38:12.000 Sep 26 2013
Intensity Factor:                 1.000000
Included traffic type(s):         Flows, Link Loads
Flow Analysis Mode:               Steady State (Head-end and Fast Reroute)
Alternate BGP Routes Allowed:     No Limit

Performance Analyzer Results:
        Measure                                         Value
WAN Link - Number of overutilized links             0
WAN Link - Maximum Utilization (%)                  0.000000
WAN Link - Total Consumed BW (bps)                  0.000000
WAN Link - BW Efficiency (%)                        0.000000
LAN - Maximum LAN Utilization (%)                   0.000000
Demand - Total Active Demands                       0
Demand - Failed-Unroutable Demands                  0
Demand - Total Number of Security Checks            1
Demand - Number of Security Failures                0
```

Fig. 15. Flow Analysis Log

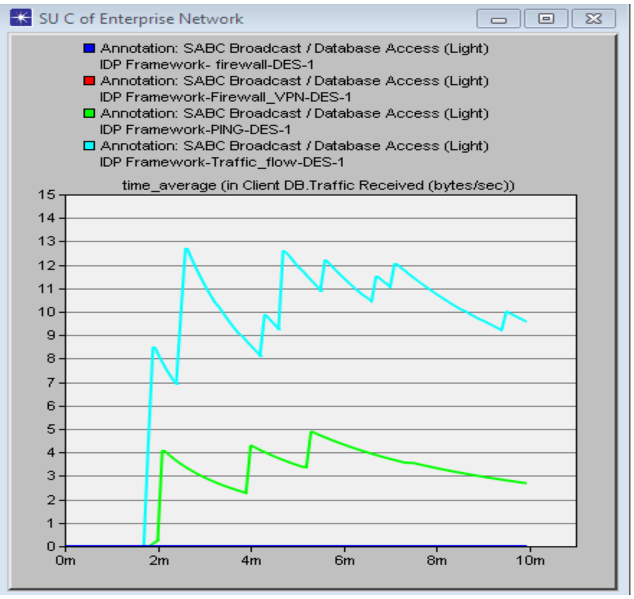


Fig. 16. SU Client DB Traffic Received

The results in Figure 16 above shows the global statistics based on the communication between all the nodes of the CRN (PUs) and the registered secondary users (SUs) with the server. As showed in the firewall scenario the SUs cannot at all access the database in the server. And only the PUs will access the database resources. The firewall supports no proxy for database. Therefore, the database is supported only when the scenario is in ping traffic and traffic flow. This implies that much traffic is received for client DB in traffic flow because attackers are prevented from intruding the network. Thus, the security demand is higher as compared to IP Ping scenario shown in Figure 7.

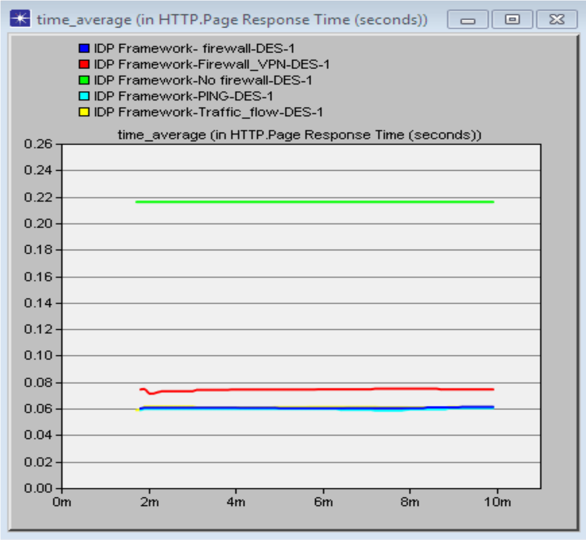


Fig. 17. Global HTTP Page Response Time

Figure 17 indicates that when the network is smooth, the HTTP response time rate increases. This is because no form of attack was identified or detected within the CRN flow. The second higest HTTP response time was within the firewall VPN scenario in Figure 6. This is also because only PUs were allowed to access the database server and no other clients were restricted. The remaining scenarios has lower HTTP page response because of the IDPF sensor monitoring measures which strictly monitors and filters all the traffic in order to detect and block off the attacks. Consequently, this causes heavy load of traffic in the network.

7. Conclusion

There is a high rate of threats, attacks and vulnerability in CRN which has become a global concern. Therefore, in this paper we designed an intrusion detection and prevention framework (IDPF) as a solution to mitigate this security challenge. This consistence framework can be used in securing all data and information in CRN to provide quality of service. The framework allows easy integration of detection and prevention components to form a security infrastructure capable for providing a secured communication in CRNs. Consequently, reported in this paper are the experimental results of the different statistics, based on different nodes and global statistics. These results were generated using OPNET simulator version 16.5. All the graphical representations showing the differences between several scenarios were also provided. Basically, this is to justify the effectiveness of IDPF in providing a secured communication and quality of service in CRNs.

Summarily, security in CRNs cannot be overemphasized as attacks replicates on daily basics and attackers have their hands on all the sophisticated attack tools which are developed rapidly. Hence, maximum security cannot be achieved as attacks and intrusions remain a permanent challenge, because innovations in information technology are endless.

References

[1] B.O Pages, I. Foster, F. Siebenlist, and A. Rachans. " A Multipolicy Authorization Framework for Grid Security," in *Proceedings of the Fifth IEEE Symposium on Network Computing and Application*, 2006, pp.269-272.

[2] S. Frankel, B. Eydt, L. Owens, K. Scarfone. "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," NIST Special Publication, 2007, pp. 119-105.

[3] T. Xiaoyong; L. Kenli; Z. Zeng; B. Veeravalli. "A Novel Security Driven Scheduling Algorithm for Procedure Constrained Tasks in Heterogenous Distributed Systems." *IEEE Journal*, Vol. 60, pp. 1017-1029, July, 2011.

[4] H. Fuping, S. Wang, Z, Cheng. "Secure Coperative Spectrum Sencing for Cognitive Radio Networks, "*in Proceedings of IEEE Military Communication Conference*," 2009, pp. 1-7.

[5] P. An K et al. "Cognitive Radio Defying Spectrum Management," *in proc. CRNI conference*, 2008, pp.2-6.

[6] P. Steenkiste, D. Sicker, G. Minder, R. Dipankar. "Future Directions In Cognitive Radio Network Research," *in proceedings of NSF Workshop Report*, March 9-10, 2009, pp. 1-37.

[7] B.O Pages, I. Foster, F. Siebenlist, A.Rachans. "A Multipolicy Authorization Framework for Grid Security," *in Proceedings of the Fifth IEEE Symposium on Network Computing and Application*, 2006, pp.269-272.

[8] J Hwang; Y. Hyenyoung Y. "Dynamic Spectrum Management Policy for Cognitive Radio: An Analysis of Implementation Feasibiliy Issues, "*in Proceedings of IEEE DySPAN Symposium*," 2008, pp.115-126.

[9] D. Denning, E. Dorothy., "An Intrusion Detection Model,"*in Proceedings of the Seventh IEEE Symposium on Security and Privacy*, 1986, pages 119–131.

[10] G. Radhaman, G.S.V. Radha, K. Rao. Web Service Security and E-business. 701 E. Chocolate Avenue, Hershey USA: Idea group publishing, 2oo7, pp. 129-131.