ISSN 2278-3091
Volume 8, No.6, November – December 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse105862019.pdf
https://doi.org/10.30534/ijatcse/2019/105862019

Analyzing Wireless Local Area Network Traffic Authentication Delay in Different Metrics to Improve Its Performance

Dr. J. Sebastian Nixon[1], Roba Seyoum Tola[2]
[1] School of Informatics, Wolaita Sodo University, Ethiopia, dr.nixon14@gmail.com ,
[2] School of Informatics, Wolaita Sodo University, Ethiopia, robelseyoum348@gmail.com

ABSTRACT

The WLAN Standard 802.11n is the most popular wireless network nowadays. However, the network performance is always important anxiety for users who is ready to migrant from wired to wireless network. In this paper we analyzed the network performance of IEEE 802.11n physical characteristics of wireless network while running different applications on different wireless network personal computer using physical characteristics of HT PHY5.0GHz 802.11n and in different data rate. Applications included Database, HTTP and FTP. For the experiment, a wireless LAN was built that included 10 wireless clients and an Access point [AP].

The experimental test was completed to analyze 802.11n standard wireless local area network performance on the network with different level of security with Database, FTP and HTTP server application. The network device such as router is configuring throughout Open Shortest Path First routing protocol to decrease utilization, create specific load distribution over the network.

In this paper we tested three scenarios that modeled are: 1.No Security Scenario, 2.Limited Security Scenario and 3.Advanced Security Scenario. The level of protection used was 802.11n to filter and block some applications and their performance is analyzed. Twenty workstations are used in the simulation which all accesses the Database, FTP and HTTP server under different scenarios. The relationship between network security and performance are estimated which include the effects of protection such as firewalls on network performance. Various scenarios were evaluated through simulations using Riverbed Modeler Academic Edition 17.5(OPNET17.5) and explained the property of unusual levels of safety on a network using 802.11n wireless network standard then proposed a solution.

Key words: AP, BSS, *IEEE 802.11n*, *SIMULATION*, *WLAN*.

1. INTRODUCTION

1.1 Background of Study

Wireless network has been used in several condition including business enterprise and home. The advantage of wireless network is that the location of devices is flexible, and users do not need to worry about cabling. Without complex cabling, wireless network is simple to setup and apply. Currently, IEEE 802.11 family is the most used wireless LAN. The opening edition of the 802.11 standard was completed in 1997[17].

Wireless networking technologies (Wi-Fi) allow Wi-Fi enabled devices to communicate over a wireless medium. Typical Wi-Fi networks include the following 3 components 1. A wired connection from ISP, 2. An access point and 3. Wi-Fi enabled clients. Wi-Fi offer different broadband speed and operate in different fields [3].

The communication between nodes is done through Access Points (APs). The access points also co-operate a role as a wireless Ethernet adapter. Wi-Fi has gained popularity because of installation simplicity and the increased number of Wi-Fi radio ready laptops. Now, many businesses like airport, café, restaurant, and shopping area offering wireless internet-services to customer. Demand for wireless technologies has gain more significance in business and everyday-life, as population is receiving denser by closely spaced buildings. Wi-Fi network have easy use in markets, offices, airports, and other location provide that costs like flexibility, mobility, simple to use and low cost. Company that hope to enter this market wants brainpower in this area to make suitable business decision based on the property of present and future technologies. Awareness of the technology in conditions of security issues, performance, installation and maintenance cost are interest. IEEE 802.11 structural design defines nine services which could be separated into two groups which are Station (STAs) services and distribution services. STAs services contain Privacy, Authenticity, de-authenticity, and delivery of the data whereas distribution services contain association, re-association, disassociation, integration and distribution. Stations are devices which have IEEE 802.11 specification with PHY and MAC interface to Wi-Fi network. Station may be any Wi-Fi supported devices. The Access Point is a device which acts as an interface between the wired network and wireless clients [9].

A BSS is a set of clients that able to communicate with each other with in 802.11 WLAN then they appearance a BSS. It is also called a cell. A short time, every mobile station may not be in touch because of limitation of coverage area in all mobile stations should be within a range to be in touch. Although a BSS include an access point and one station, the BSS is not an Independent BSS. It is called an infrastructure BSS or simply as BSS. If there are two stations, and all stations are in the BSS are mobile stations and

there is no any connectivity to wired LAN network, the BSS called Independent BSS (IBSS) or ad-hoc network. IBSS stations frankly contact one and another (peer to peer) but they are unable to connect with any BSS. The distribution system (DS) is the fixed wired infrastructure and used to connect a set of BSSs to create an extended service set (ESS). The IEEE 802.11 distribution services allow a wireless terminal to roam without restraint within ESS and also allow an 802.11 WLAN to connect to the wired LAN Infrastructure. Extended service set (ESS) include several IEEE 802.11 standard, BSSs type only subnet work where access point can exchange a few words each other to forward traffic from one BSS to another and provide facility to move mobile station from one BSS to other. The ESS configuration is a set of multiple BSS cells which can be linked by either wired LAN or wireless LAN and used the same channel. The access point performs this communication through the distribution system [12].

The 802.11b set focus on the substructure two layer of the open system Interconnect (OSI) model, the physical layer and data link layer. The 802.11b standard allow for two type of transmission: FHSS and DSSS. Both type of spread spectrum use more bandwidth than a typical narrowband transmission, but enable a strong signal that is easier for the receiver to detect than the narrowband signal. The IEEE 802.11b set work on data link layer, and physical layer. 802.11n define two type of tool: a wireless station which is usually a PC prepared with wireless network interface card (NIC) and an AP. The 802.11b standards define two modes: infrastructure mode and adhoc mode [15].

In the infrastructure mode, the wireless networks include at least one access point associated to the wired network communication and a place of wireless end station. This design is called a basic service set form a single sub network. Since most company WLANs require access to the wired LAN for service (file server, printer, internet link), they activate in infrastructure mode [15].
Adhoc mode is just a set of 802.11b wireless station that switches a few words directly with one another without using an access point or any connection to a wired network. This mode is useful for rapidly and without difficulty setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for service, such as a hotel room, convention center, or airport where access to wired network is barred [15].

The process of animatedly associate and re-associate with AP allow network manager to set up WLANs with very broad coverage by create a series of overlapping 802.11b cells throughput a building or across a campus. To be successful, the information technology (IT) manager ideally will employ channel re-use, taking care to set up each access point on an 802.11b DSSS channel that does not overlap with a channel used by neighboring AP. A hotspot often operates Wi-Fi technology via router, offering internet access. Free hotspot normally suggest free access to menu or buy list also provide payment systems like pay pall, or via credit card, or work public network in which verification and confirmation features are turned off [16]

The term poisoned hotspot or rogue hotspot refers to a malicious individual who sniff the data sent by user on a free hot spot including decipher passwords, and login names. The "User-fairness model" is a bill model can be implementing with the help of EDCF (IEEE 802.11e, which make revision to MAC layer of the current IEEE 802.11 to expand support for LAN application that have QoS requirements [4].

There are some safety tips for using public Wi-Fi in secure way includes, using firewall, turning off wireless network when not in use, hiding important files, and not typing credit card numbers, passwords or sensitive data without proper safety mechanism on browsers [16].

While using Wi-Fi hotspot you should be sure that sent information should be fully encrypted, and always logout after finishing your work. Always remember that you are not permanently signed into accounts. Pay attention to browser alerts and warnings. HTTP and TLS does not fully protect browsing [11].

The world has become increasingly mobile and wireless networks allows users to work and move freely, therefore wireless technologies, now a days, are more popular that wired or fixed networks. The word “Wi-Fi” stands for wireless fidelity, which means that the device having Wi-Fi can access a Wireless Local Area Network [1].

Wireless LAN is seen as the technology that will enable the most convenient link between existing wired networks and portable computing and communication equipment, such as laptop computers and personnel digital assistants (PDAs), at the office, hotel, company, or campus level. An obvious advantage of the WLAN is that it reduces the need for wiring among several building.
In general, the application of the WLAN system can be simply between two computers or between a computer and a wired network, all the way up to the complete network with many users and a great number of data paths [13].

The supplement standards 802.11e, 802.11f, 802.11h, and 802.11i are defined to enhance the capability of 802.11-based WLANs. The 802.11e is for enhancements of the quality of service (QOS). The 802.11f provides a recommended practice for an inter access-point protocol. The 802.11h extends the spectrum and transmit power management at 5 GHz for European operation. The 802.11i enhances MAC layer security [13].

2. LITERATURE REVIEW

Security methods available today- from older protocols that have vulnerability such as the Temporal Key Integrity Protocol (TKIP), which is a modification on WEP to defend against currently known attacks (it is WEP +four patches for key mixing; message integrity; re-keying and initialization vector protection)[2].

To sustain the fast deployment of IEEE 802.11 technology there is a need for protection against such low-cost, yet very effective attacks. In this work, they describe and evaluate DiscoSec, a solution against the most prominent vulnerabilities within present WLANs. A similar goal was also set within the IEEE 802.11 Task

Group, which is still in proposal stages, and therefore, they implement the concept of DiscoSec as an open-source IEEE 802.11 device driver to serve as a benchmark and prototype for future developments. Various design and implementation decisions were based on measurements using modern equipment [7].

Concerning attacks based on unauthenticated management and data frames, the work demonstrate their devastating effect on IEEE 802.11 networks. Based on the same vulnerabilities, in various attacks are successfully mounted even against the new security standard IEEE 802.11. While the empirical demonstration is a frequently used method to illustrate the problem of link-layer security, protection against such attacks prevalently remains conceptual. The authors employ two protocols, SIAP and SLAP, to establish a secure association utilizing public key infrastructure. While their solution offers encryption, it also modifies the IEEE 802.11 state machine and requires a SIAP server. In commercial products, Cisco offers a feature called Management Frame Protection (MFP), but there is regrettably no detailed information other than white papers. Interestingly, MFP does not seem to be a client-side supported feature, and thus only protects APs, while clients remain vulnerable to management frame attacks. The first solution with a design supporting the IEEE 802.11 state machine, extensively tested on performance limited hardware and available for use on present devices was introduced and it is less effective because access control is not considered [6].

Wireless messaging is now a dynamic ingredient in the communication modes of our life. Many applications over the Internet now use wireless messages to contact with the end user. There is also a growing concern over how much these services are secure and how they can be compromised, which are described briefly in this presentation [10].

The deployment of the Wireless Local Area Network (WLAN) technologies has tremendously grown in the latest two-three years. Many companies and organizations install WLANs in their facilities to improve the efficiency of their co-workers by allowing them to have access to network services most of the time, without any additional cables or high infrastructure cost. So-called hot spots (airports, railway stations, hotels, malls, and conference-centre) allow the occasional traveler and the professional worker to be in constant contact with his/her company without using any expensive dial-in services [8].

Wireless network has more advantages over wired network and different from each other the way how they transmitted data. Taping the media that is used in network communication is the only possible way in wired networks and in wireless networks communication is done with air media or RF [22]. That's why wired is more secure than wireless networks, the transmissions which take place in air with the right equipment can easily intercept those transmissions. To secure the wireless networks more difficult it is not an easy task as wired [14].

2.1 WLAN Components

There are two basic components of WLAN:1.Access points [APs] and 2. Network Interface Cards/client adapters are the main components of WLAN [5]. AP connects all the wireless clients in the WLAN to exchange the data as shown in the following Figure 1.

Figure 1: Components of WLAN

2.2 Common WI-FI IEEE 802.11 Family Standards

According to [1], The WLAN uses either infrared or radio frequency technology to send and receive data. Based on radio technology the IEEE 802.11 was implemented as the first WLAN standard in 1997. The following are some of the WLAN standards.

Table **2.1** IEEE 802.11 Standards

Standard	data rate	Frequency	modulation	Range	date of release
802.11a	54Mbps	5GHz	OFDM	35-120m	Sep 1999
802.11b	11Mpbs	2.4GHz	DSSS	35-140m	Sep 1999
802.11g	54Mbps	2.4GHz	OFDM,DSSS	38-140m	June 2003
802.11n	150Mbps	2.4-5GHz	OFDM	70-250m	Oct 2009
802.11ac	867Mbps	5GHz	OPDM	----------	Dec 2012

2.3 WLAN Performance Evaluation

As all security mechanism adds encryption and decryption process additionally to the traffic, it definitely drops the performance of the wireless transmission. There are two different ways of conduct such experiment: test bed based and simulator based.

One of the previous test bed based researches has found that most wireless encryption protocol will drop the wireless performance from 1% to 19% depending on the protocol itself and the traffic type (UDP/TCP). The experiment has tested several Windows operating system with a two nodes wireless test bed environment [18].

Another group of researchers has expanded this research with additional WPA2 encryption protocol and Linux operating system involved. The test bed is under a two-nod 802.11n draft wireless network environment. The result of this research still shows that the most recent encryption protocol is comparatively the best one [19].

According to these researches, the outcome data of test bed based experiment is quite unstable as the real test bed environment may have various unpredictable elements. Factors such as the quality of the equipment and even the temperature of the air can interfere the experiment. However, simulator based experiment is another phase. Terrain Modeling Module evaluates the wireless network performance by using OPNET. OPNET offers several of modules for different simulation purpose [20].

There is a group of researchers has done a similar wireless network evaluation by using OPNET simulation. They compared the network performance of IEEE802.11g with the previous IEEE802.11b network and give a way of doing such evaluation in OPNET simulation [21].

2.4 FACTORS AFFECTING NETWORK PERFORMANCE

The performance of a network helps to improve and assures the quality of service the operator is providing whiles also guaranteeing optimum network utilization. Computer networks are

becoming complex and maintaining security across such network in multivendor environment is becoming a big challenge. Integration of differentiated services has a great impact on the network source. Operators are also optimizing the network to improve the service quality and meet customers' needs.

Some of the factors are: Congestion, Threshold, Throughput, Bandwidth, Delay and latency, Jitter , Network utilization, Firewall technology and Packet loss

3. METHODOLOGY AND MATERIAL

To measure the performance and the behavior of networks and networking device with varying security strength, simulations and analytical study were used. In this paper, the study of network performance with change in security is solely based on simulation. This section deals with three scenarios which are modeled using Riverbed Academic Edition17.5 as a simulation tool.

3.1 Methodology of the Study

In this research we designed an experimental method for analyzing WLAN authentication delay by using OPNET modeler 17.5 simulation tools on some of the common application and used quantitative approach to compare the effect of the experimental result to improve the performance.

3.2 Modeling of WLAN Scenario

The complete modeling procedure in OPNET basically has four sections- 1. Design of network model, 2. Selection of individual statistics, 3. Collection of simulation results and 4. Analysis of the results obtained, as it can be seen in Figure 2

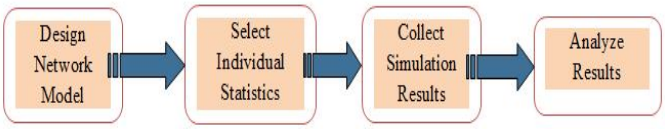

Figure 2: Complete Overview of Designing a Project in OPNET Modeler

The purpose of the experiment is to collect enough data to analyze the network performance of 802.11n. The main idea of the experiment is to build an 802.11n, and use both real application and network traffic generator to create data flow in the network. Another important thing for this experiment is to minimize the effect of uncontrollable factors.

The 802.11n network performance is influenced by several controllable and uncontrollable factors. The controllable factors include distance between nodes and AP, operating system, wireless protocol, IP version, other network configuration parameters and settings, and data stream in the network.

The uncontrollable factors include hardware performance, software error and other random factor. An easy and practical solution for the issues is that repeat the tests and takes the mean value. The tests will repeat in different time to make sure the uncontrollable factors do not stay the same while repeating. In this part of experiment, both real application and network traffic generator are used.

.3.3 Network Design and Simulation

This section presents the actual network design and simulation of the thesis work. The three scenarios which include: no security scenario, limited security scenario, advanced security scenario are modeled here.

3.3.1 No Security Scenario

In this scenario no security is forced on the entire network. An IP based cloud acts as the internet and connects two or more subnets being the three servers and the company's LAN. Two routers are connected across network simulation. Three different applications are set up on this scenario; these are Database application, HTTP application and FTP applications. The needed traffic is generated by configuring both the Application and Profile configuration objects. After the required configurations are done the performance of the cloud in terms of Database applications, HTTP application and FTP application is evaluated. A new project is created by clicking "File" menu and selecting "New project" as in Figure 3.

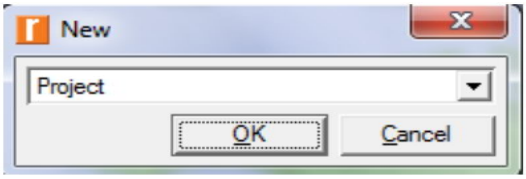

Figure 3: New Projects

The internet used in this experiment incorporates 20 workstations. The simulation is done such that for No Security Scenario, all the 20 workstations gain access to the Database application, HTTP application and use FTP to download and upload file onto the file server.

3.3.2 Limited Security Scenarios

With limited security scenario, a firewall is installed on the network to filter packets. A duplicate of the first scenario is created with a configured firewall filtering capabilities. Here, a packet latency of 0.1 seconds is set on the network to filter packets. The same performance metrics for the No security scenario are used to analyze the network performance.

3.3.3 Advance Security Scenarios

This scenario is designed by making a duplicate of the second scenario. The need for this is to filter packets and prevent illegal HTTP access. After all the scenarios are designed, the simulation is run for a period of one hour. The network performance is hence, analyze.

3.3.4 Performance Metrics

- DB Query Response Time
- DB Query Traffic Sent
- DB Query Traffic Received
- FTP Download Response Time
- FTP Upload Response Time
- HTTP Page Response Time

The same performance metrics is used to measure the performances of the other scenarios. Packet sizes of 50MB (low),

100MB (medium) and 1500MB (high) are imposed on the network and a switching speed of 5Mbps, 1Gbps and 5Gbps are set between the router and the cloud.

3.4 Simulation Procedure

Since the goal of this thesis is to find the outcome of maximizing security with varying controls and analyzing the performance of a network and also to evaluate the relationship between network security and performance and the effect of security for three different scenarios like No security, Limited security and Advanced security. Riverbed Modeler Academic Edition is the simulator for this experiment. The following sections explain the experiment.

3.4.1 Simulation of No Security Scenario

In this section, the procedure to simulate a network with no security case is presented. Firewall is a device that imposes some limitations and restrictions on transfer of data over a network. Firewalls monitors and controls the traffic that traverses a network. Firewall of this kind is used for this experiment. In this simulation an office LAN is used as the endpoint and all transmissions are done via the cloud and firewall devices. A new project is created and project name and scenario are given as Master Thesis and No Security scenario as shown in Figure 4.

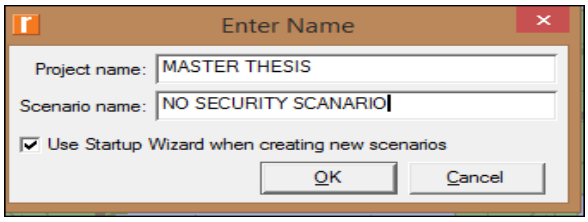

Figure 4: No Security Scenario

On the menu bar perform the following actions to create a basic topology

- Click on file
- Click on new
- A new project dialog box appears
- Click on ok

In the new window, type the project name and scenario name in the project name text box and scenario text box respectively and click ok

After setting up the required project and scenario name, these steps are followed to design the simulation.

- Select Create Empty scenario and click on next
- Choose office and click next
- Select default city on the map
- Click twice on “next”
- The workspace is then displayed

The following objects are dragged onto the workspace:

- The Application configuration object is used to set up the required applications.
- Database, FTP and HTTP applications are used on the network.
- The Profile configuration object is used to configure the profiles
- Ip32_cloud object is used to perform the function of the internet
- Two Ethernet4_slip8_gtwy‘s are used to perform the function of two routers
- 10BaseT_LAN object is used perform the function of the office network which supports 20 workstations
- Three server namely HTTP, FTP and Database are used to support the applications
- Ethernet 10BaseT link is used to connect the LAN and the router

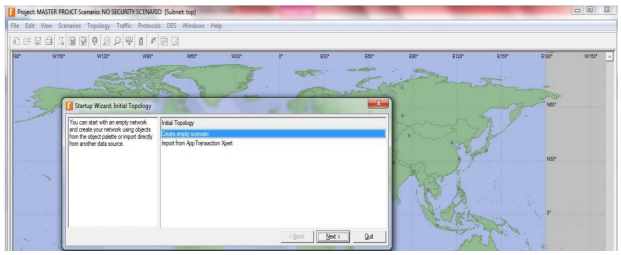

Figure 5: Empty Scenario

3.4.2 Application Configuration

Three applications are established which generate the requisite traffic over the internet or cloud. Riverbed Modeler Academic Edition makes available an object called Application Configuration which is used to create the needed applications on the network. The following procedures explain the configuration of the applications.

- Right-click on Application Definition object and select Edit attributes
- Add three rows to the Applications definitions table, to enable the creation of three application
- Rename the first row as HTTP and select heavy browsing against HTTP application
- Rename the other row as FTP and choose High load against FTP application
- Finally rename the last row as Database and select High load against the Database application

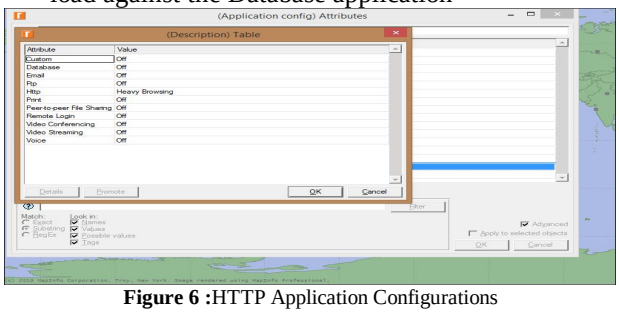

Figure 6 :HTTP Application Configurations

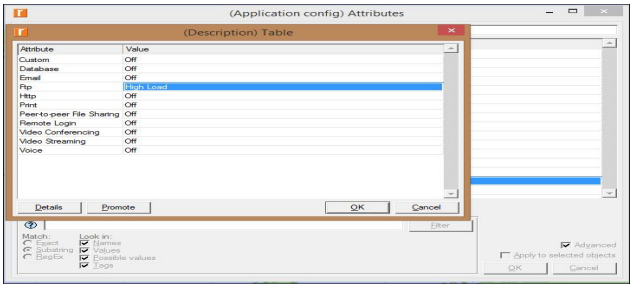

Figure 7: FTP Application Configurations

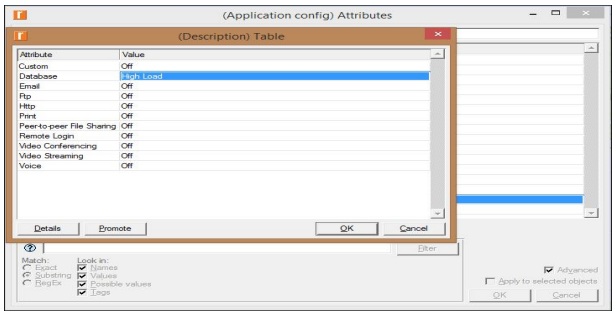

Figure 8: Database Application Configurations

3.4.3. Profile Configuration

An application needs to generate traffic over the internet. Riverbed Modeler offers a Profile Configuration object which is used to generate the necessary traffic. The steps below detail how to configure the profile definition:

- Right-click on Profile configuration object and choose Edit attributes
- Add three rows for configuration
- Name the first row "ADMIN" and select HTTP as its equivalent application
- Name the second row as "TECHNICIAN" and select FTP as its equivalent application
- Name the last row as "RESEARCHER" and select Database as its equivalent application as shown in Figure 9.

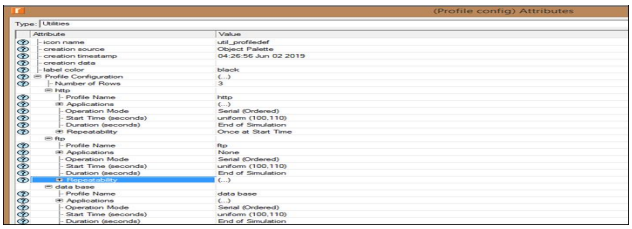

Figure 9: Profile Configuration

3.4.4. Internet Configuration

Riverbed Modeler makes available an IP32 cloud which performs the function of a simple public internet based cloud. In this thesis the cloud is used to support the three applications. The steps show how to configure the cloud or internet.

- Right click on the cloud and select Edit attributes
- Change the Packet latency by setting its value to 0.1 seconds

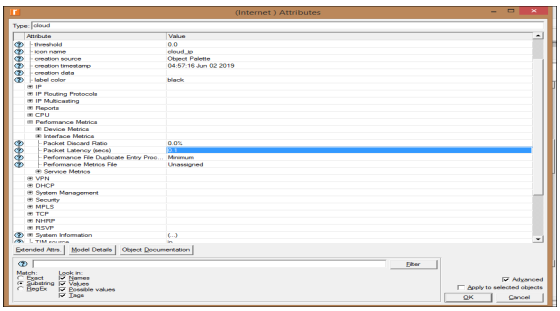

Figure 10 : Internet Configuration

Setting packet latency to 0.1 it implies that, the maximum packet delay across the internet as a result of HTTP, FTP and Database Applications is 0.1seconds.

Every packet travels over the cloud with a limited delay of 0.1seconds.

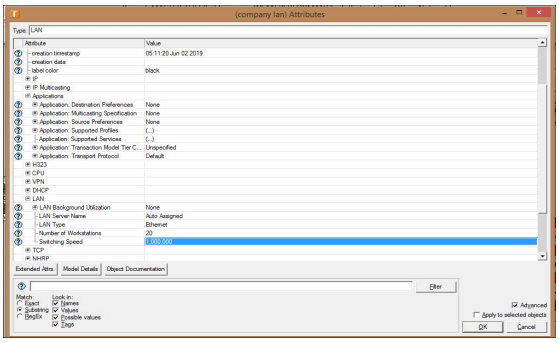

Figure 11: Company LAN Configurations

3.4.5. Company LAN Configuration

The company's network is built with a 10BaseT_Switch_LAN and the following steps show how the LAN is configured:

- Right click on Company LAN and click on edit attributes
- Set number of workstations to 20
- Expand Application supported profiles and add three rows
- Add Database profile to the applications and set the number of users to Entire LAN
- Add HTTP profile to the applications and set the number of user to Entire LAN as depicted by the figure below
- The FTP profile are also added and the number of users are each set to Entire LAN

The Company's network is connected to the Router 1 using 10BaseT links which is in turn connected to Router 2

3.4.6. Server Configuration

Three Ethernet servers 'are dragged unto the project and configured to support Database, HTTP and FTP applications respectively in the following steps.

- Right click on the database server and select edit attributes
- Edit the application supported profiles and set Database application as supported
- A similar approach is used to configure the HTTP server, where the HTTP application is set as supported
- Same steps are configured for the file server, where FTP application are supported

3.4.7. Router Configuration

Router used in the simulation is the Ethernet4_slip8_gtwy object. The link between them is Discrete Simulation 1 and Test1 which are connected to IP32 cloud and the remote servers. Router 1 and Router 2 were used for load balancing purposes the following step shows how it was configured.

- Click on the Discrete Event Simulation
- Click on the configuring/Run DES
- Click on IP and expand its attributes
- Change the IP Dynamic Routing Protocol from default to OSPF

3.5 Performance Metrics Configuration

To measure the performance of cloud against the all three applications few parameters are required. Riverbed Modeler provides three levels to analyze performance of a network. These are the global level, node level and link level. In this thesis the Global level is used to analyze the performance of applications on the network. Global level is configured as:

- Click on DES menu and select Individual statistics
- A new window opens with the options to global statistics, node statistics and link level statistics shown in Figure 12.

Following metrics are chosen for performance evaluation. From the Global level statistics,

- Expand the DB query option and choose response time
- Expand the HTTP option and choose the page response time
- Expand FTP options the download and upload response time.
- Expand and select the Ethernet delay

From the link level statistics the following metrics are selected
Expand point to point and select inbound and outbound utilization

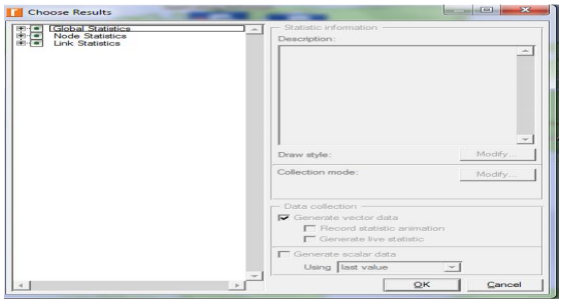

Figure 12: Performance Metrics

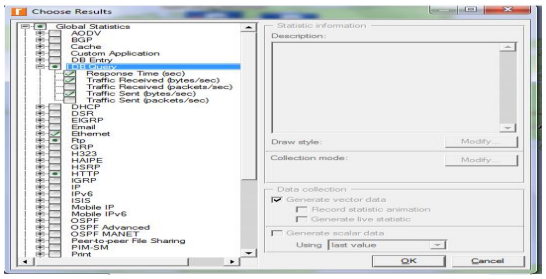

Figure 13: Global Statistics Performance Metrics

3.6 Simulation of Limited Security Scenario

Duplication of the no security scenario to create the new scenario for this section is done. In this scenario the Ethernet2_slip_8 firewall replaces Router 2 over the internet. The firewall will permit needed traffic to travel through the network and also perform packet filtering. The duplicate procedure is shown in Figure 15

The steps below is used to configure the firewall.

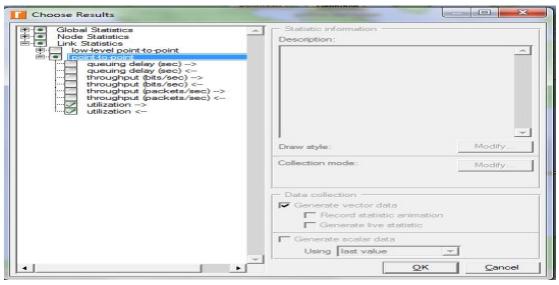

Figure 14: Link Level

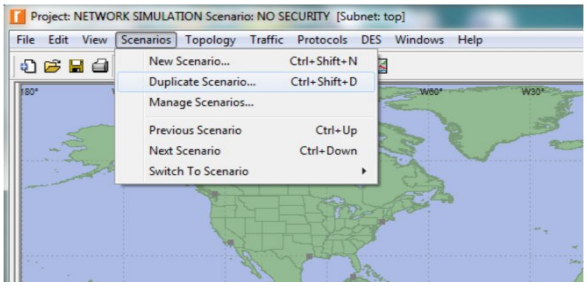

Figure 15: Duplicate Scenario

- Remove Router 1 and replace with ethernet2_slip8_firewall
- Right click on the firewall and set its name to Limited Security setup and choose Edit attributes
- Expand Proxy server information and modify the row and set its latency value to a constant of 0.5
- Expand the row1, row3 and row 4 and set a constant of 0.1 as their latency. A constant value of 0.1 is set for latency on database, file and web application which is an indication that, the firewall is performing packet filtering and thus a delay of 0.1 seconds is imposed over the router.

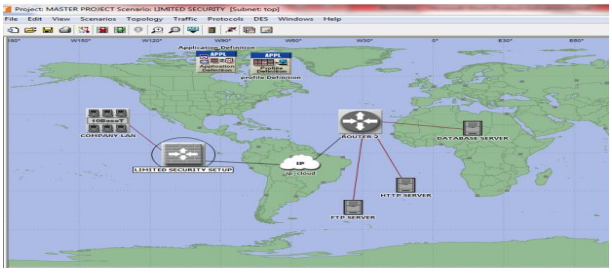

Figure 16: Limited Security Scenarios

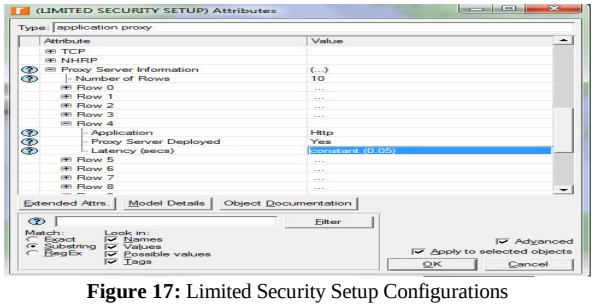

Figure 17: Limited Security Setup Configurations

In the simulation, Limited security scenario is configured and the same performance metrics as the first scenario are used across this scenario.

3.7 Simulation of Advance Security Scenario

In this scenario web traffic that travels through the network is foiled. The scenario is designed by duplicating the second scenario. The following steps describe the changes are made to this network scenario:

- Right click on ethernet2_slip8_firewall and set its name to Advance security setup and edit the attributes
- Expand the Proxy server information and select the row 4 which is HTTP application
- Change "proxy server deployed" to "No" as shown in Figure 19.

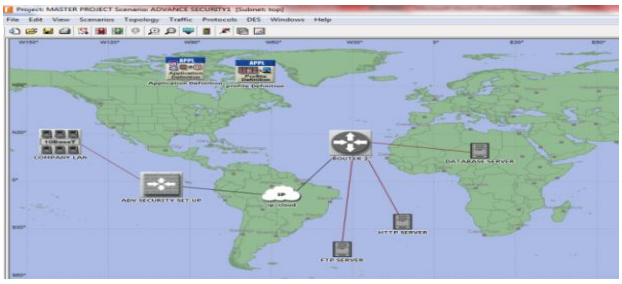

Figure 18: Advance Security Scenarios

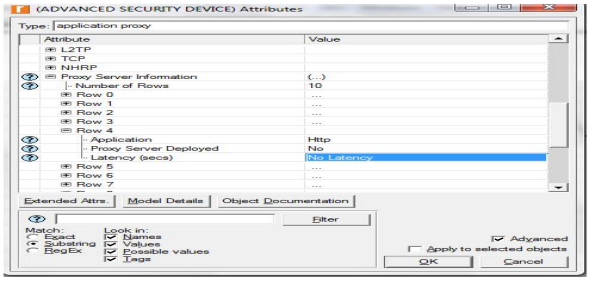

Figure 19: Advanced Security Configurations

With this all the HTTP traffic across the cloud is blocked for some users and enhances the simulation of advanced security scenario.

3.8 WLAN Configuration

In this scenario, we have a server connected to a switch and the switch split into 2 links and connected to 2 access points. For each access point, 10 stations are connected to its closet access point by assigning the correct BSSID. Each of these stations runs the FTP heavy application which will be requesting a burst of 50000 bytes of data for a mean period of 360 seconds from the server. The network setup is shown in figure 20.

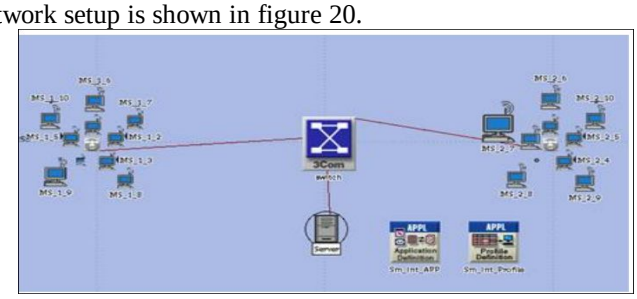

Figure 20: WLan configuration

3.9 Running the Simulation

After configuring the scenarios, the simulation is run for one hour. This is done by selecting the "manage scenarios" option from the scenario menu as displayed in figure 21.

By selecting the manage scenario, a new window opens which allows the simulation to run for one hour or more as depicted in Figure21.

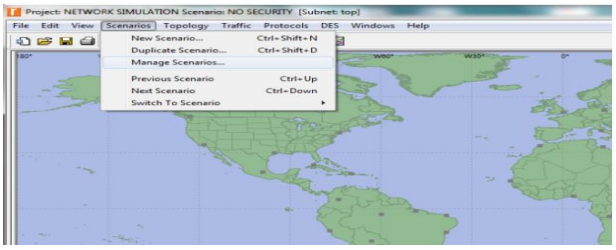

Figure 21: Manage Scenarios

4. RESULT AND DISCUSSION

In this section we analyze and discuss the output of the simulation from section 3. The analysis and discussions are evaluated after running the simulation for one hour. The three simulations in this thesis work are:

- No Security scenario where there is no protection on the network.
- Limited Security scenario where a firewall is installed on the network to filter packets of the three applications.
- The Advance Security scenario where firewall is imposed with blocking capabilities to block one application. Traffic from HTTP application is blocked for some users in the company whiles that of Database and FTP applications are $_{\text{allowed}}$ to pass through.

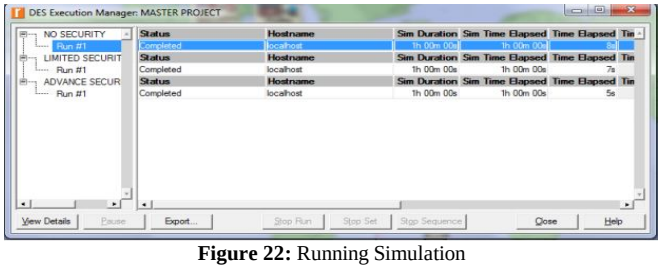

Figure 22: Running Simulation

4.1Wireless Local Area Network Simulation Result

$$\text{THROUGHPUT} = \frac{\textit{TOTAL NUMBEROF DATAPACKET RECEIVED BY EACH NODE} * \textit{PACKET SIZE OF NETWORRK} * 8}{\textit{SIMULATION TIME}} \quad \text{------ (1)}$$

$$\text{PDR} = \frac{\textit{TOTAL NUMBEROF DATAPACKET SUCCESSFULLY RECEIVED BY EACH DESTINATION}}{\textit{TOTAL NUMBEROF DATAPACKET SUCCESSFULLY RECEIVED BY EACH SENDER}} * 100 \text{--(2)}$$

$$\text{E2ED} = \frac{1}{S} \sum_{i=1}^{S} (\text{ri} - \text{si}) \text{ ---------- (3)}$$

Where S is the sum of data packet successfully received by each destination, r_i is the time taken at which the data packet sent, s_i is the time taken at which the data packet sent and i is unique packet identified.

4.2 Database Query Response Time

The Tables below show the database query response time, taking after the first 15 and 60 minutes of the simulation time with different switching speed and varying load.

Table 4.1 Database query response time with packet size 50MB (low load)

DATABASE QUERY RESPONSE TIME 50MB (LOW LOAD)						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	0.021	0.113	0.0234	0.0256	0.0266	0.034
LIMITED SECURITY	0.105	0.0566	0.117	0.128	0.133	0.17
ADVANCED SECURITY	0.525	0.2825	0.585	0.64	0.665	0.85

Table 4.2 Database query response time with packet size of 100MB (medium load)

DATABASE QUERY RESPONSE TIME WITH MEDIUM LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	1.0546	1.0503	0.8844	0.8790	0.8630	0.8777
LIMITED SECURITY	0.008	0.024	0.048	0.080	0.099	0.103
ADVANCED SECURITY	0.133	0.146	0.148	0.156	0.175	0.65

Table 4.3 Database query response time with packet size of 150MB (high load)

DATABASE QUERY RESPONSE TIME HIGH LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	0.1613	0.224	0.260	0.2986	0.3400	0.319
LIMITED SECURITY	0.06	0.084	0.112	0.162	0.2	0.21
ADVANCED SECURITY	0.3	0.42	0.6	0.008	0.006	0.007

4.3 Database Traffic Received

The Tables below shows the database query traffic received, taking after the first 15 and 60 minutes of the simulation time with different switching speed.

Table 4.4 Database traffic received with packet size 50MB (low load)

DATABASE TRAFFIC RECEIVED 50MB (LOW LOAD)						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	5345.6	6732.01	3214.6	8908.3	5123.89	7567.90
LIMITED SECURITY	2672.8	2244.00	1071.533	2969.33	1707.96	2522.63
ADVANCED SECURITY	1336.4	1122.00	535,46	1439.90	845.8	1261.8

Table 4.5 Database traffic received with packet size off 100MB (medium load)

DATABASE TRAFFIC RECEIVED WITH MEDIUM LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	5345.6	6732.01	3214.6	8908.3	5123.89	7567.90
LIMITED SECURITY	2672.8	2244.00	1071.533	2969.33	1707.96	2522.63
ADVANCED SECURITY	1336.4	1122.00	535,46	1439.90	845.8	1261.8

Table 4.6 Database traffic received with packet size off 150MB (high load)

DATABASE TRAFFIC RECEIVED WITH HIGH LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	5345.6	6732.01	3214.6	8908.3	5123.89	7567.90
LIMITED SECURITY	2672.8	2244.00	1071.533	2969.33	1707.96	2522.63
ADVANCED SECURITY	1336.4	1122.00	535,46	1439.90	845.8	1261.8

4.4 Database Query Traffic Sent

The Tables below show the database query traffic sent, taking after the first 15 and 60 minutes of the simulation time with different switching speed.

Table 4.7 Database query traffic sent with packet size of 50MB (low load)

DATABASE TRAFFIC SENT 50MB(LOW LOAD)						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY						
LIMITED SECURITY						
ADVANCED SECURITY						

Table 4.8 Database query traffic sent with packet size of 100MB (medium load)

DATABASE TRAFFIC SENT 100MB(MEDIUM LOAD)						
SWITCHING SPEED	5MB		1GB		5GB	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	2078.718	2192.667	2039.761	2144.228	2020.615	2161.965
LIMITED SECURITY	2050.513	2156.579	2062.906	2155.035	2031.316	2133.228
ADVANCED SECURITY	2035.932	2192.304	2035.932	2192.304	1999.744	2159.673

Table 4.9 Database query traffic sent with packet size of 150MB (high load)

DATABASE TRAFFIC SENT WITH HIGH LOAD						
SWITCHING SPEED	5MB		1GB		5GB	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	9582.50	10338.62	9637.20	10350.41	9582.50	10338.62
LIMITED SECURITY	9579.21	10356.77	9489.50	10283.42	9587.97	10425.26
ADVANCED SECURITY	9511.38	10303.63	9516.85	10294.27	9490.60	10244.12

The performance of the Database, HTTP and FTP application are discussed in graphical representation based on the performance metrics chosen at the global level statistics. All the obtained graphs are compared against the performance metrics and a detailed analysis is given.

4.5 FTP Downloads Response Time

The Tables below shows the FTP download and upload results, taking after the first 15 and 60minutes of the simulation time with different switching speed

Table 4.10 FTP downloads response time with packet size 50MB (low load)

FTP DOWNLOAD RESPONSE TIME 50MB (LOW LOAD)						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	0.183463	0.130961	0.07721	0.144607	0.194266	0.220272
LIMITED SECURITY	0.388105	0.432882	0.25342	0.347535	0.441276	0.393998
ADVANCED SECURITY	0.264058	0.28095	0.264053	0.280945	0.342098	0.417238

Table 4.11 FTP downloads response time with packet size 100MB (medium load)

FTP DOWNLOAD RESPONSE TIME MEDIUM LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	45MINS	15MINS	45MINS	15MINS	45MINS
NO SECURITY	0.183463	0.130961	0.07721	0.144607	0.194266	0.220272
LIMITED SECURITY	0.388105	0.432882	0.25342	0.347535	0.441276	0.393998
ADVANCED SECURITY	0.264058	0.28095	0.264053	0.280945	0.342098	0.417238

Table 4.12 FTP downloads response time with packet size 150MB (high load)

FTP DOWNLOAD RESPONSE TIME HIGH LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	45MINS	15MINS	45MINS	15MINS	45MINS
NO SECURITY	5.594	4.654	6.327	5.202	7.262	5.324
LIMITED SECURITY	26.259	35.761	31.214	35.679	11.064	8.064
ADVANCED SECURITY	1.187	1.093	1.216	1.084	1.087	1.086

4.6 FTP Uploads Response Time

The Tables below show the FTP upload response time, taking after the first 15 and 60minutes of the simulation time with different switching speed.

Table 4.13 FTP upload response time with packet size 50MB (low load)

FTP UPLOAD RESPONSE TIME 50MB(LOW LOAD)						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	0.11026	0.224611	0.162853	0.219477	0.090653	0.165794
LIMITED SECURITY	0.262592	0.309749	0.48156	0.471822	0.315871	0.327106
ADVANCED SECURITY	0.340902	0.337859	0.340897	0.337854	0.267664	0.315456

Table 4.14 FTP upload response time with packet size 100MB (medium load)

FTP UPLOAD RESPONSE TIME MEDIUM LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	0.320	0.323	0.320	0.328	0.320	0.323
LIMITED SECURITY	0.689	0.728	0.731	0.760	0.722	0.733
ADVANCED SECURITY	0.730	0.777	0.655	0.731	0.820	0.728

Table 4.15 FTP upload response time with packet size 150MB (high load)

FTP UPLOAD RESPONSE TIME HIGH LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	3.774	4.636	6.365	4.087	1.243	2.535
LIMITED SECURITY	30.854	34.466	28.806	34.492	11.067	9.238
ADVANCED SECURITY	1.378	1.361	1.417	1.398	1.359	1.357

4.7 HTTP Page Response Time

The Tables below show the HTTP page response time, taking after the first 15 and 60 minutes of the simulation time with different switching speed.

Table 4.16 HTTP page response time with packet size of 50MB (low load)

HTTP PAGE RESPONSE WITH 50MB(LOW LOAD)						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	0.75108	0.753608	0.72876	0.74088	0.750731	0.724027
LIMITED SECURITY	0.50845	0.496347	0.504508	0.50819	0.496803	0.504206
ADVANCED SECURITY	0.15239	0.149915	0.152308	0.14994	0.109388	0.125983

Table 4.17 HTTP page response time with packet size of 100MB (medium load)

HTTP PAGE RESPONSE WITH MEDIUM LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	0.503788	0.50579	0.470836	0.495626	0.499494	0.499539
LIMITED SECURITY	0.477433	0.50588	0.490998	0.497054	0.489484	0.502342
ADVANCED SECURITY	0.128929	0.133095	0.1402	0.128689	0.130938	0..140456

Table 4.18 HTTP page response time with packet size of 150MB (high load)

HTTP PAGE RESPONSE WITH HIGH LOAD						
SWITCHING SPEED	5Mbps		1Gbps		5Gps	
SIMULATION TIME	15MINS	60MINS	15MINS	60MINS	15MINS	60MINS
NO SECURITY	14.4188	15.16266	13.15442	14.56281	14.16418	15.58603
LIMITED SECURITY	9.971854	11.15779	9.82973	11.05133	4.339151	3.503513
ADVANCED SECURITY	0.123074	0.13841	0.1317	0.123679	0.150175	0.146801

4.8 Analysis on Database Applications

The database application is one of the applications that was used to generated traffic in this experiment and the performance of the database application is estimated against the database query response time, database traffic received and database traffic sent. A packet size of 50MB (low), 100MB (medium) and 150MB (high) are imposed across the network and a switching speed of 5Mbps, 1Gbps and 5Gbps are set between the router and the cloud. The database query response, database traffic sent and received times are evaluated with each packet sizes and data rate to investigate applications performance.

This section discusses the performance evaluation of the database application under the three scenarios. Database Query Response Time is the elapsed time between the end of an inquiry, query or demand on a computer system and the beginning of a response; for example, the length of the time between an indication of the end of an inquiry and the display of the first result of the response at a user terminal. Lower the query response time indicates higher performance of the database application.

4.8.1 Database Query Response Time

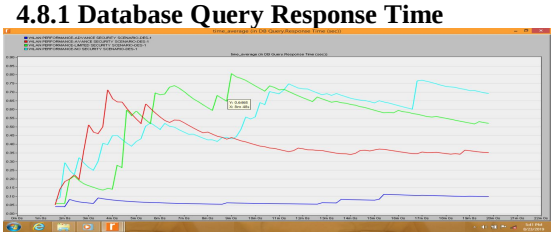

Figure 23 : Database Query Response Time

4.8.2 Database Traffic Received

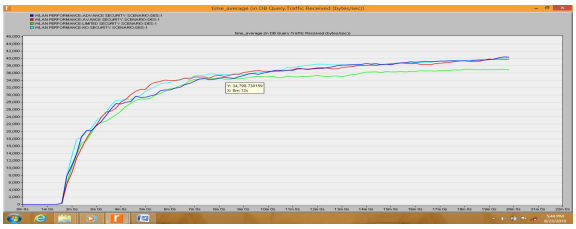

Figure 24: Database Traffic Received

4.8.3Database Query Traffic Sent

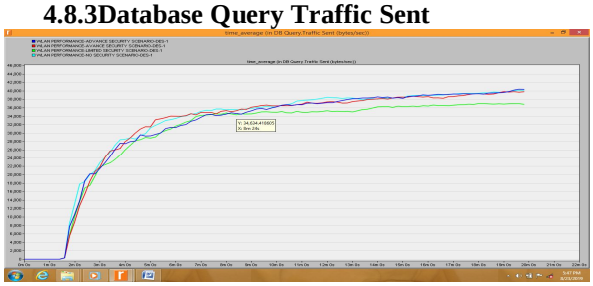

Figure 25: Database Query Traffic Sent

4.9 Analysis of FTP Application

File transfer protocol is an application that generates lots of traffic and it also been assessed against the download and upload response time which is one key indicator in accessing network performance. It is defined as the time beyond between sending application and receiving the response packet. It is calculated from the time a user application sends a request to the server to the time it receives a response packet.

4.9.1 FTP Upload Response Time

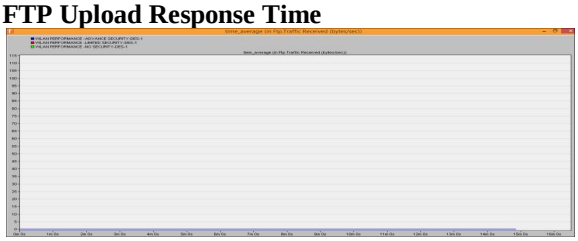

Figure 26:FTP Upload Response Time

4.9.2 FTP Downloads Response Time

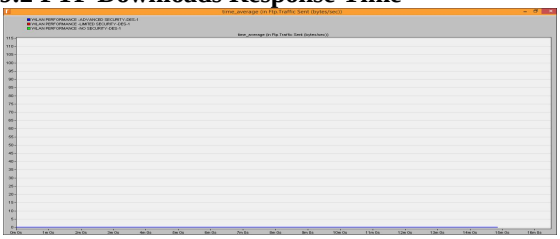

Figure 27: FTP Downloads Response Time

4.10 Analysis on HTTP Application

HTTP application is one of the applications which generate a lot of traffic on the network. HTTP application is evaluated against the HTTP page response time. The lower the value of the response time, the faster the page opens.

4.10.1 HTTP Page Response Time

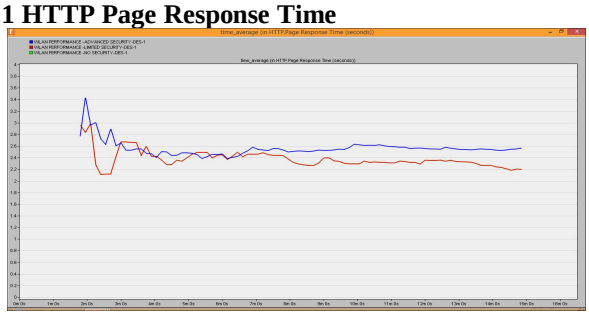

Figure 28: HTTP Page Response Time

5. CONCLUSIONS

In today's computing, companies are striving to optimize their level of protection day in and out by installing firewall systems onto their network. As load increases the performance of the network degrades. But user experience must not be affected when there is change in security. Customer service must be a key factor in every organization and must be appreciated in that customers do not wait hours before being served. Security methods like the use of firewall may cause poor performance in a network based on the application individual used. By configuring the firewall with only necessary settings will not affect the performance of the WLAN.

REFERENCES

[1] Ahmedur Rahman, C. I.Ezeife and A.K. Aggarwal., Abdel-Majid Mourad, Loic Brunel, Akihiro Okazaki, and Umer Salim., "LTE Artichecture", Mitsubishi Electric-Information Technology Centre Europe, 2010.

[2] Atheros Communication. (2004). How Atheros define wireless Network security today and in the feature. White Paper Building a secure wireless Network.

[3] Bhaskaran Raman, Kameswari Chebrolu. (2007, January). Experiences with Wi-Fi for RuralInternetinIndia. [Online]:Available :\https//www.google.com/url?

[4] Houda Labiod, Hossam Afifi, Costantino De Santis..Wi-Fi Bluetooth and Zigbee and WiMax, "Wi-Fi Bluetooth and Zigbee and Wi-Max", 2007, Page 65.
https://doi.org/10.1007/978-1-4020-5397-9

[5] D. Dhiman, "WLAN Security Issues and Solutions," *IOSR J. Comput. Eng.*, vol. 16, no. 1, pp. 67–75, 2014.
https://doi.org/10.9790/0661-16146775

[6] Ivan M. Glen Z., Joe S., and Hao G., (2007). Introduction of IEEE 802.11i and Measuring its Security versus Performance Tradeoff. In Proceedings of the 13th European Wireless Conference, April 2007.

[7] Ivan M., Glen Z., Joe S., and Hao G. (2008). Design, Implementation, and Performance Analysis of DiscoSec – Service Pack for Securing WLANs. University of Kaiserslautern, Germany.

[8] M. Casole, "{WLAN} Security -- Status, Problems and Perspective," *Proc. Eur. Wirel.*, 2002.

[9] Matthew S. Gast."802.11 wireless networks:", 802.11 wireless networks the definitive guide. ISBN 0-596-10052-3, 2011, Page #12-16.

[10] Mishra, M., Vinter, R., and John L. (2004). Pro-active Key Distribution using Neighbor Graphs. IEEE Wireless Communications Magazine.
https://doi.org/10.1109/MWC.2004.1269714

[11] Onguardonline.gov (2011, September), Tips for Using Public Wi-Fi
Networks[Online].Available:http://onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks.

[12] Plamen Nedeltchev, Felicia Brych. "Wireless Local Area Networks and the 802.11Standard", Wireless Local Area Networks and the 802.11Standard, 2001.

[13] Qizheng Gu.. Wireless Local Area Network (WLAN). "RF System Design Of Transceivers for Wireless Communication".2004.

[14] I.- Introduction, "Investigation Of The Impact Of Ddos Attack On Network," vol. 3, no. 2, pp. 275–280, 2015.
https://doi.org/10.25271/2015.3.2.49

[15] Vijay K.Garg. Wireless network evolution 2G to 3G, "Wireless network evolution 2G to 3G", 2002.

[16] Wikipedia, the free encyclopedia (2012, October 10), Hotspot (Wi-Fi),[Online].Available:http://en.wikipedia.org/wiki/Hotspot_%28Wi-Fi%29

[17] Perahia & Stacey, 2008, Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n.
https://doi.org/10.1017/CBO9780511541032

[18] Narayan, Kolahi, Sunarto, Nguyen and Mani, 2008, Generic factors influencing optimal.

[19] Narayan, Tao, Xiangle and Ardham, Impact of Wireless IEEE802.11n Encryption Methods on Network Performance of Operating Systems, 2009.

[20] Hetal Jasani and Yu CAI, May, 2008, Performance evaluation of wireless networks.
https://doi.org/10.1109/SECON.2008.4494276

[21] Victor Kulgachev, Hetal Jasani, 2010, 802.11 networks performance evaluation using OPNET.
https://doi.org/10.1145/1867651.1867690

[22] A. Ifeyinwa Angela, "Evaluation of Enhanced Security Solutions in 802.11-Based Networks," *Int. J. Netw. Secur. Its Appl.*, vol. 6, no. 4, 2014
https://doi.org/10.5121/ijnsa.2014.6403