International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:3, No:3, 2009

Impact of Implementing VPN to Secure Wireless LAN

H. Bourdoucen, A. Al Naamany and A. Al Kalbani

***Abstract*—**Many corporations are seriously concerned about security of networks and therefore, their network supervisors are still reluctant to install WLANs. In this regards, the IEEE802.11i standard was developed to address the security problems, even though the mistrust of the wireless LAN technology is still existing. The thought was that the best security solutions could be found in open standards based technologies that can be delivered by Virtual Private Networking (VPN) being used for long time without addressing any security holes for the past few years. This work, addresses this issue and presents a simulated wireless LAN of IEEE802.11g protocol, and analyzes impact of integrating Virtual Private Network technology to secure the flow of traffic between the client and the server within the LAN, using OPNET WLAN utility. Two Wireless LAN scenarios have been introduced and simulated. These are based on normal extension to a wired network and VPN over extension to a wired network. The results of the two scenarios are compared and indicate the impact of improving performance, measured by response time and load, of Virtual Private Network over wireless LAN.

***Keywords*—**IEEE802.11, VPN, Networking, Secure Wireless, WLAN, Opnet.

I. Introduction

WIRELESS LAN technologies such as IEEE802.11 provide end users and network professionals with a good degree of flexibility and cost reduction in terms of cost of saving cables [1-3]. However, with the increased reliance on the WLANs, the security issue is becoming of great concern for this technology as it is becoming a subject to numerous attacks. These attacks are often divided into passive attacks such as eavesdropping and traffic analysis, and active attacks such as DoS and Masquerade.

This security weaknesses of WLANs, leads the network vendors and analysts to look for and provide remedies to these attacks and threats [4-5]. Most of them agree that there are two primary levels of securing for a wireless network. The first level is the Frame level which introduces encryption and authentication technologies, and the second level is the radio frequency level which introduces intrusion detection and prevention.

This paper is an attempt to define enhancement of different technologies used to secure and reduce the threats associated with the wireless LAN, and examines the impact of using Virtual Private Network technology to secure the WLAN technology. In addition to these, it will present analysis on its impact on the cost as well as on performance measurements that are mainly related to delay and Load.

After a umber of observed vulnerabilities on WEP, it was suggested to go ahead with deploying WLAN discounted security measures introduced by the IEEE 802.11 standard working groups together with the Wi-Fi alliance. The idea was that the best security solution could be found in open, standard-based technologies delivered by Virtual Private Networking (VPN). IP security (IPSec) is the standard for VPN, which went through a number of revisions that have resulted in a robust security standard that provides good data confidentiality, authentication, and access control regardless of the transmission medium. By integrating wireless LANs into an IPSec infrastructure, allows WLAN infrastructure to focus on simply transmitting wireless traffic, while the VPN would secure it, as shown in Fig. 1 below.

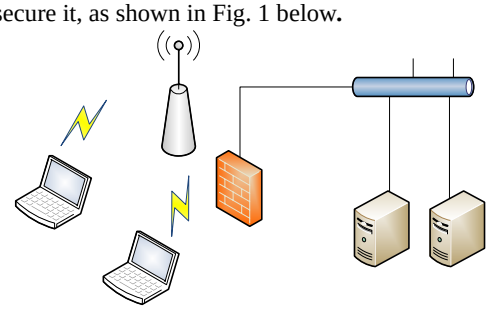

Fig. 1 Integration of WLAN and VPN configuration.

Note that this VPN maintains data privacy through the use of a tunneling protocol and security procedures. There are different ways one can adopt to implement a VPN, but the two most common types are remote access VPN and site-to-site VPN [6]. The Remote Access VPN configuration is used to allow VPN software clients such as mobile users to securely access centralized network resources that reside behind a VPN server. The site-to-site VPN allows to create dedicated, secure connections between locations across the open Internet or public connection. They can be either Intranet-based or Extranet-based. In its simplest form, by encrypting data while it is sent and decrypting it at the receiver, the data is effectively sent through a "tunnel" that cannot be "entered" by data that is not properly encrypted and part of the

H. Bourdoucen, A. Al Naamany and A. Al Kalbani are with the Electrical and Computer Engineering Department, College of Engineering, Sultan Qaboos University, P.O. B;ox 33, Al-Khod, Muscat 123, Sultanate of Oman (authors' e-mails: hadj@squ.edu.om, naamany@squ.edu.om, m051407@squ.edu.om).

communications process. It involves placing a packet within another packet and sending it over a network. The protocol of the outer packet is understood by the network at both points, called tunnel interfaces, where the packet enters and exits the network [6].

Data transmitted over unsecured communication using wireless technology by broadcasting signals which can be received by many hackers, where end users absolutely cannot control unless the data is encrypted then it is extremely vulnerable to be intercepted or interrupted [7]. Besides , security, flexibility is another advantage of VPN's as most of them enable to carry almost all IP protocols according to IPSec standard. Such as Web servers, Email servers, FTP servers, file servers or DNS servers can all be completely accessed from anywhere through VPN networks. This allows rationalizing resources and information to prevent waste. The availability of IPSec VPN can be used by client to connect to the company VPN, even it comes from a dial-connection [7]. However, some disadvantages of VPN need to be indicated, despite of their popularity. They require in fact a deep understanding of public network security issues and need taking proper precautions while deployment. Also, VPN technologies of different vendors may not work well due to non compatibility is their specifications.

Tunneling is the process of encapsulating private IP packets into an IPSec packet, in a way that the private data packet is embedded inside the IPSec packet, as shown in Fig. 2 below.

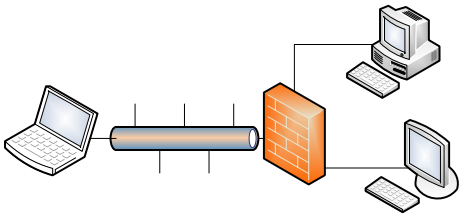

Fig. 2 VPN Virtual tunneling

The authentication between VPN gateways has established the tunnel and the users can send and receive data across it. IPSec tunnels traffic at the packet level, i.e., at the network layer of the Open Systems Interconnect (OSI) seven-layer model, and is indifferent to which higher-level protocol the packets represent. Because an IPSec VPN encapsulates all IP packets regardless of their function, it automatically supports all applications that communicate using IP. IPSec usually requires the use of an installed program on the client machine to handle the encryption [8].

Secure Sockets Layer (SSL) VPNs encapsulate data traffic over an encrypted tunnel to a gateway, by invoking SSL technology when communicating over an "HTTP secure" (https) web link. The receiving SSL gateway decrypts the traffic and passes it to the internal network. SSL VPNs tunnel traffic at the session layer of the OSI model, but not at the network layer, so by default they only support some specific IP applications—typically web access and e-mail, Figure 3 below, shows the implementation of SSL [6].

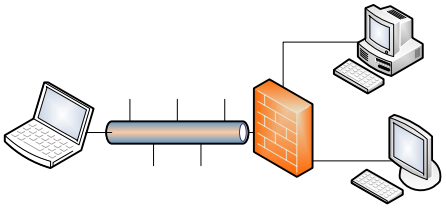

Fig. 3 SSL tunneling in a VPN

Since SSL support is built into web browsers and most e-mail client programs there is no need for a separate program to support these applications [8]. However, wireless LAN (WLAN) technologies such as 802.11g provide end-users and network professionals a tremendous amount of flexibility. However, While full information security may not be attainable, most experts agree that WPA and 802.11i represents an excellent solution, except for one detail. This is related to the fact that 802.11 deals only with security of the airlink, which is the portion of information value chain between a given client and a given access point. This means, only a secure connection between wireless client and WLAN infrastructure [9].

A virtual private network can provide security far beyond the airlink. While there are many forms of VPNs, a popular solution is to use the industry standard IP security (IPSec) protocol, which is specified as part of the overall suite of Internet Protocols. IPSec allows a mobile client or any wired client to establish a secure "tunnel" through all the network elements between client and server [10].

Below is described a framework for securing WLAN traffic using a network-layer virtual private network (VPN). The network architecture for a VPN-secured WLAN implementation is shown below in Fig. 4.

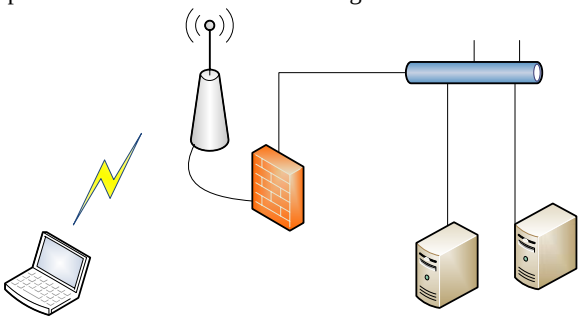

Fig. 4 Network architecture for a VPN-secured WLAN.

The primary component in this wireless LAN security architecture is VPN Concentrator which is the VPN key component. While the non trusted of the WLAN security, the use of VPN technologies such as PPTP, pure IPSec, or L2TP over IPSec provide better encryption levels and dynamic key exchanges that mitigate the weaknesses of WEP. In addition, the authentication required by the VPN adds another layer of control over access to the production LAN by wireless clients.

Depending upon the VPN Concentrator or firewall used, the VPN authentication can be integrated into services available on the Wired LAN (Refer to the Fig. 4).

Once a user is authenticated, all traffic on the wireless network is encrypted and becomes safe from prying eyes, even if a hacker managed to penetrate wireless access point's security and join the network, it would see no clear-text traffic because all legitimate users would be using an encrypted tunnel [11].

II. Simulation Results and Discussion

Two computer tools have been investigated, NS2 and OPNET for simulation of WLAN security using VPN. NS2 is a discrete event simulator targeted at networking research, which provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks [12, 13]. But for this work, Opnet Modeler 11.0 tool has been used. The parameters and configurations needed for the simulated scenarios will be discussed. The aim is to program and simulate wireless LAN of 802.11g protocol, and analyze the impact of integrating Virtual Private Network technology to secure the flow of traffic between the client and the server farm within the Local Area Network, using OPNET WLAN utility.

The Markov model for the distributed coordination function (DCF) protocol has been shown to predict accurately the network throughput of 802.11 networks under realistic traffic load. The performance of 802.11 DCF has been studied in the literature through various models, different simulations, and a number of experiments [15-17]. The throughput model developed by Bianchi provides an accurate and simple analytical model for a finite number of terminals and ideal channel conditions [16].

The probability that a given station transmits is expressed as:

$$\tau = \frac{1-p^{m+1}}{1-p} \times b_{0,0} \quad (1)$$

Where, p is the conditional collision probability and m is maximum backoff stage.

$b_{0,0}$ is expressed as

$$b_{0,0} = \frac{2(1-2p)(1-p)}{(1-2p)(W+1)+pW(1-(2p)^m)} \quad (2)$$

Where W is the contention window.

The derived normalized system throughput S is give by the following ratio

$$S = \frac{P_{tr}P_s E[P]}{(1-P_{tr})\sigma + P_{tr}P_s T_s + P_{tr}(1-P_s)T_c} \quad (3)$$

Where T_s is the average time, T_c the collision time, and σ, slot time and E[P] is the Payload in a slot time. Note that these four parameters are constant. Also in equation (3) above, P_s is the probability that a transmission is successful, P_{tr} the probability that there is at least one transmission in the considered slot time.

There are many statistics that can be determined after simulating and designing VPN in OPNET environment. In this paper, the statistics of interest are mainly:

Ethernet Delay: which represents the end to end delay of all packets received by all the stations. VPN Delay: which gives the End-to-End delay for traffic through a VPN. This delay is measured as time elapsed between traffic entering the network through Ingress and traffic leaving the network through Egress. VPN Load: measures the amount of VPN-traffic entered the Network through Ingress. The statistic is measured in bits per second. VPN throughput: measures the amount of VPN-traffic leaving the Network through Egress. The statistic is measured in bits per second.

WLAN Delay: Represents the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. This delay includes medium access delay at the source MAC, reception of all the fragments individually, and transfers of the frames via AP while Access Point Functionality enabled,

WLAN Throughput: bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network. WLAN Load: Represents the total load (in bits/sec) submitted to wireless LAN layers by all other higher layers in all WLAN nodes of the network.

Database Entry for Traffic Received: represents the average bytes per second forwarded to all Database Entry Applications by the transport layers in the network. Traffic Send: which is the average bytes per second submitted to the transport layers by all Database Entry Applications in the network.

Email Traffic Received Traffic: Average bytes per second forwarded to all email applications by the transport layers in the network. Send Traffic: Average bytes per second traffic submitted to the transport layers by all email applications in the network.

Two scenarios been simulated for seven hours duration, (about 12 hours real time) are:

- Scenario (1): Normal Wireless LAN
- Scenario (2): Wireless LAN with Virtual Private Network Technology

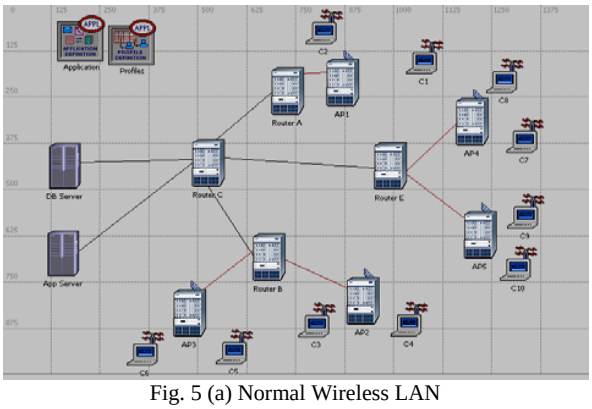

Fig. 5 (a) Normal Wireless LAN

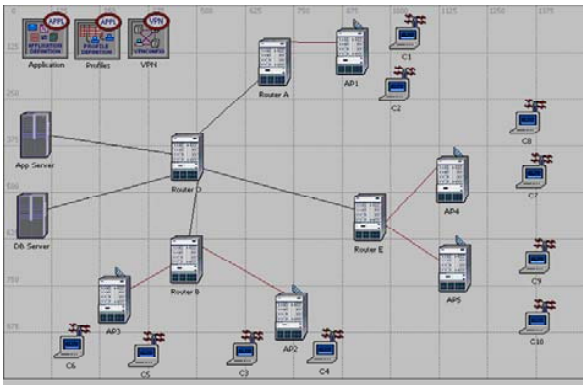

Fig. 5 (b) VPN over Wireless LAN

The obtained results from different scenarios are analyzed to measure the performance implication of deploying VPN over Wireless LAN, in which are divided into three categories: Global Results, Link Results, and Object Results.

Wireless local area with and without VPN have been simulated and results analyzed for both networks. The diagrams considered are shown Figures 5 (a), (b).

Parts of the simulated scenarios consist of Ethernet connectivity (refer to figure 5 (a)), as a global result of the Ethernet delay shown in figure 6 below.

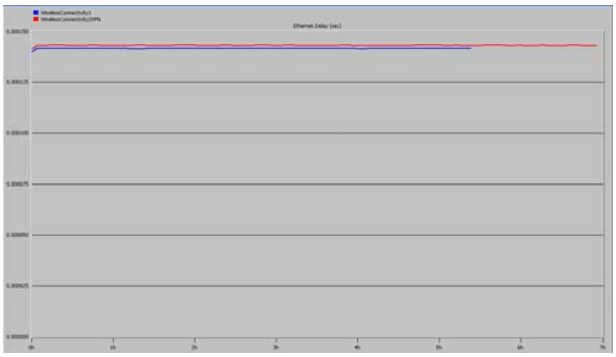

Fig. 6 Ethernet Delay

The results indicate that there is no important impact of Virtual Private Network (VPN) over the response of Ethernet delay. The results show rather stable delay for both normal and VPN scenarios, at approximately 0.14 msec.

The considerations of data dropped results indicate the overflow traffic over the wireless object. The graph of the results are shown in Fig. 7.

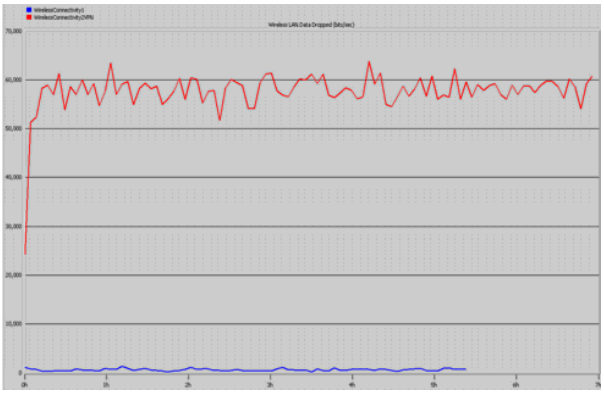

Fig. 7 Ethernet Delay

Unfortunately, the impact of the VPN over wireless traffic indicates a high data drop, which is mainly due to the overflow of traffic. The observed data dropped differences show an average of more than 95%. For a simulation of 4 hours run time, the data dropped at VPN is about 57.5 Kbits/sec, and the normal network with no VPN shows about 858 bits/sec. The results also indicate that the data drop continues almost at a stable average rate of 55 Kbits/sec when a VPN is used.

The wireless delay presents the delay of packets received and forwarded by the wireless nodes across the network, the graph obtained represent the delay difference with and without VPN, refer to Fig. 8.

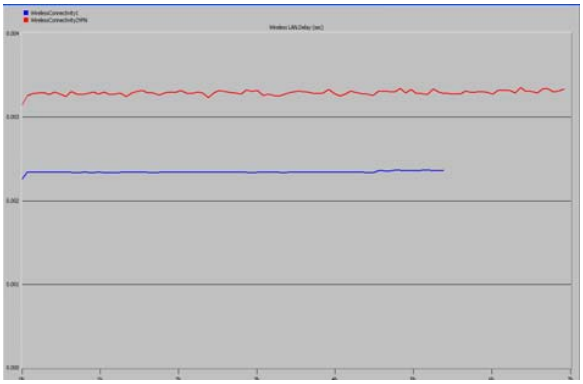

Fig. 8 Wireless Delay

The results indicate that the delay response on either receiving or forwarding packets by the wireless nodes using VPN and without VPN as having almost the same impact, the average difference is about 40% between the sampled delay indicates that at the fourth hour of the run simulation gives a delay of 3.28 msec with VPN and 2.34 msec without VPN with a difference of 0.94 msec.

The load indicates the total traffic received and utilized across the wireless nodes. The graph shows the average variation of the Wireless load with and without VPN across these nodes. Fig. 9 shows these variations.

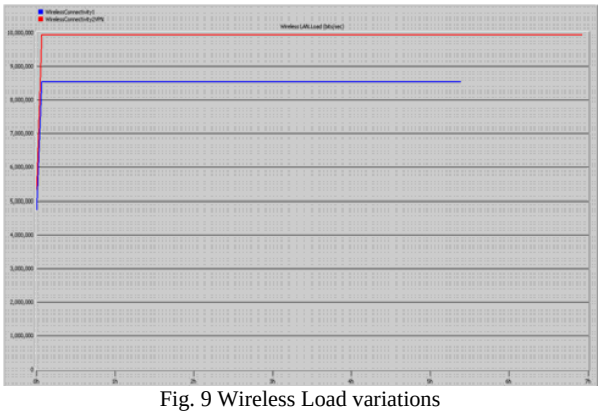

Fig. 9 Wireless Load variations

The obtained graph indicates an average difference between the two simulated scenarios of about 16%, given a difference of 174 KB at the third minute of the run time simulation. Based on the sampled data retrieved, at the third minute of simulation run indicates a VPN load of 9,953 Kbits/sec, and without VPN it gives 8,558 Kbits/sec, and it remains stable for the rest of the simulation time.

Another analysis of VPN impact is the object which presents any node in the simulated scenario, as an object Access Point (1) has been analyzed to show the impact of VPN over a Wireless Object or nodes, especially at the Media Access Delay, which indicates the Total time (in seconds) that the packet is transmission. The graph shown in Fig. 10 indicates the results obtained.

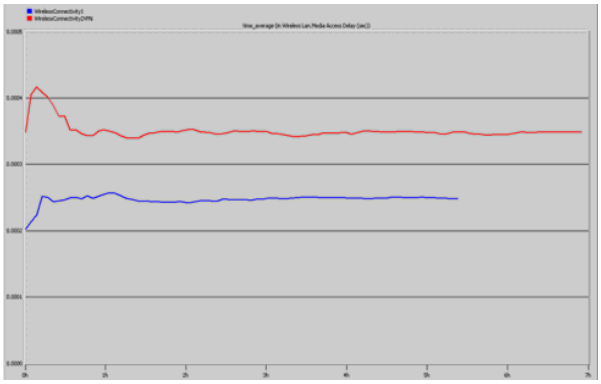

Fig. 10 Wireless node Media Access Delay

The graph shows that, the object delay difference reached an average of about 39%, with a difference of 0.097 msec. At third hour and fifty minutes of the simulated run with VPN gives a delay of 0.34 msec and without VPN, it gives a delay of: 0.25 msec, which indicates a very low delay difference over the AP object with VPN.

The link throughputs is the third area to be analyzed after the global and object, which indicates the receiving and sending of data packets. The utilized point to point link at the simulated scenarios between the AP1 and Router A (Refer to Fig. 11), which shows the results of the utilized link.

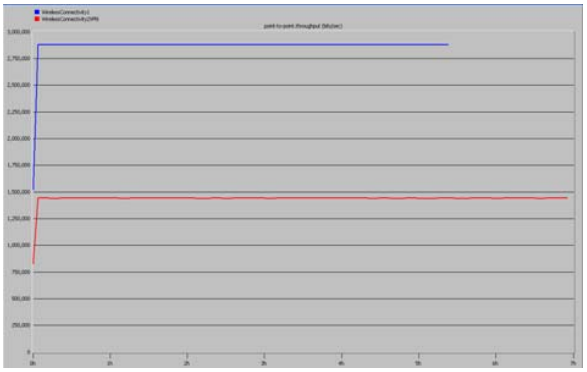

Fig. 11 Inbound Throughput

The results show that the inbound throughput utilization of VPN over the link presents an overall average difference of about 50%, at the 3rd minute throughput over the link with VPN of 2,889Kbits/sec and Normal (No VPN) of 1,449Kbits/s. The results show a high throughput at normal scenario with VPN because of the delay time with VPN and high data drop.

Using the same link, Fig. 12 shows the results of the outbound of throughput with and without VPN, which depicts the difference and impact of VPN when introduced over the selected point to point link.

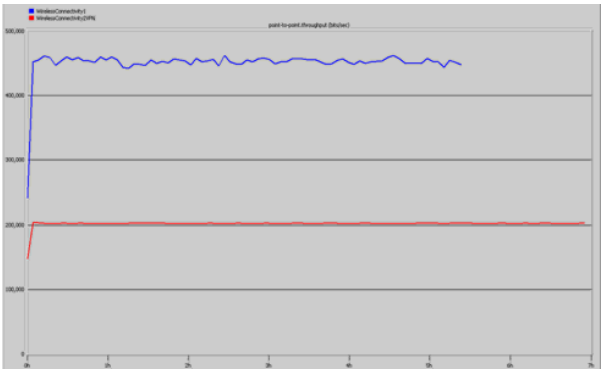

Fig. 12 Outbound Throughput

The results clearly show that the outbound throughput utilization of VPN over the link presents an average difference of about 55%. The impact of VPN shows a value lower than that of the normal WLAN scenario. This is because of the high delay time with VPN and High data Drop, which is almost similar to the inbound case.

Table I, shows a summary of the obtained results collected from the outcomes of the two scenarios. The results show a comparison to indicates the impact of performance (Response Time, Load) of Virtual Private Network over wireless LAN.

The performance impact has been analyzed from two different parameters, the response time and the traffic load differences and the results are summarized below.

With regard to Response Time, given a Database server response time difference of 2.37 seconds which is almost 50% of the normal response time, and the response time difference

of the wireless nodes which reaches about 0.9 milliseconds, given an average of 40% difference of response time delay. Concluding an expected overall response time delay differences between the two scenarios, due to the additional VPN Processes, which been caused by the encryption processes and the extra headers added on every packets.

TABLE I
SUMMARY OF THE OBTAINED RESULTS FOR THE TWO SCENARIOS EXPLAINED IN TEXT

	Time (hr)	Normal	VPN	Diff.	%
Global Results					
Database Server - Response Time (Sec)	3:08	4.98	7.35	2.37	47.5%
Wireless - Data Dropped (bits)	3:08	800	57710	56910	97%
Wireless - Delay (Sec) - VPN	3:08	2.34×10^{-3}	3.25×10^{-3}	0.91×10^{-3}	39%
Wireless – Load (bits) – VPN	3:08	8537180	9932390	1395210	16%
Object Results (Access Point 1)					
Media Access Delay (Sec)	3:08	2.49×10^{-4}	3.46×10^{-4}	9.7×10^{-5}	39%
Link Results (AP1 – Router A)					
Throughput Inbound (bits)	3:08	2879920	1440170	1439760	50%
Throughput outbound (bits)	3:08	448660	202010	246650	55%

With regard to Traffic Load, the traffic load over the Wireless LAN which has been produced by the VPN, shows that there is a high traffic load difference indicated by the collected results. The traffic load at the wireless nodes gives a difference of 174 Kbytes traffic and the link inbound gives a traffic of 180 kbytes, and the outbound of 31 kbytes. This indicates a high traffic load which has a high impact on the data drop over the wireless nods. The data drop indicates an overflow traffic over wireless nodes which need to be resolved by using the IEEE802.11n protocol instead of IEEE802.11g, which has a high bandwidth rate and increases the Ethernet bandwidth to a Gigabit. This results of VPN generating a high traffic load over the wireless LAN nodes, which impacts the flow of data over the wireless nodes. This is because of the encryption processes and the added authentication headers for each packet sent.

Table II gives a bandwidth requirement of various applications [13], which will help organizations to decide how much bandwidth required to use for VPN over their Wireless LAN based on the above outcomes.

TABLE II
BANDWIDTH REQUIREMENTS FOR VARIOUS APPLICATIONS

Application	Rate
E-mail	2.4 to 9.6 Kbits/sec
Database	Up to 1MBits/sec
Document Imaging	10 to 100 MBits/sec
Compressed Video	2 to 10 MBits/sec

III. CONCLUSION

In this paper, simulation of wireless LAN for IEEE802.11g protocol has been done, and analyzes impact of integrating Virtual Private Network technology to secure the flow of traffic between the client and the server farm using OPNET WLAN utility has been carried out. Two Wireless LAN scenarios have been considered and the results compared. These are Normal Extension to a wired network and VPN over Extension to a wired network. The results collected from the two scenarios, indicate the impact of performance, mainly Response Time and Load, of Virtual Private Network over wireless LAN. Roaming and handover, which are closely related, were not considered in the current work. In order to implement roaming, the station should be continually scanning for the best signal of the available access points. Moreover, handover requires the knowledge of handshaking process. However, in order to realize an actual performance impact of WLAN, it is important to consider roaming and handover aspects in a future work.

REFERENCES

[1] The Centre for Internet security, Networking Bench Mark, Thesis Title: Wireless Networking Benchmark, version 1.0, April 2005.
[2] P. K. Neelakantham, Villanova University, Thesis Title: Wireless Networking Study of IEEE 802.11 Specification Communication Networks, Summer 2002.
[3] Self Study Report on Personal Area Network, Submitted by: H. Srikanth, Guid.
[4] National Institute Standards and Technology (NIST), Thesis Title: Wireless Network Security 802.11, Bluetooth and Handheld Devices, By: Tom Karygiannis and Les Owens, 2002.
[5] DISA Field Security Operations, Final Draft Wireless Security Technical Implementation Guide, Version 4, Release 0.3, 18th August 2005.
[6] N. Edde, Security Complete, Second Edition, 2002.
[7] Stockholm's University, Master Thesis: Security Centre for an Enterprise, By Huxiodong, Feb 2005.
[8] Schlumberger Information Solutions, Houston, white Paper of: Virtual Network Solutions for Remote Access, Comparison between SSL and IPSec, 2004.
[9] R. Myers, Technology Industry, in Communication News, Article Title: Combine VPN and Encryption – Wireless Security, 2003.
[10] Mercurion System Inc, Information Technology Consulting and Support Services, White paper: Using VPN to Secure WLAN Traffic, 2004, http://www.mercurionsystems.com.
[11] B. Lewis and P. T.Davis, Electronic Book, Wiley Publishing, Inc, 2004.
[12] NS Simulator for beginners, University De Los Andes, Sophia-Antipolis, 2003.
[13] OPNET Modeler Accelerating Network R&D, Opnet 11.0 product documentation, www.opnet.com/support.
[14] Cisco System Inc, Cisco Wireless Security, Chapter:8, www.searchnetworking.techtarget.com/ searchnetworking /downloads /chapter08.pdf.
[15] G. Bianchi, L. Fratta, M. Oliveri, "Performance Evaluation and Enhancement of the CSMA/CA MAC Protocol for 802.11 Wireless LANs", Proc. PIMRC 1996, October 1996, Taipei, Taiwan, pp. 392-396.
[16] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," IEEE Journal on Selected Areas in Communications, Vol. 18, No. 3, pp. 535–547, Mar. 2000.
[17] N.T. Dao and R.A. Malaney, "A New Markov Model for Non-Saturated 802.11 Networks", 5th IEEE Consumer Communications and Networking Conference, 2008.