A solution to Enhance VPN effect on wireless network Performance

Subhi Aswad Muhanad Qasim
subhiaswad@yahoo.com
M. Q. Jabbarmoony_q@yahoo.com
College of Information and Communication Engineering/ Al-Nahrain University

Abstract:
This work presents a design of secured Wireless Network by utilizing Virtual Private Network (VPN) technique and provides a solution to enhance its performance by using Wireless Quality of Service technique (WQoS).A set of parameter are investigated include delay, throughput, jitter round trip time. These parameters are checked for a WLAN without VPN and WQoS, WLAN with VPN, and WLAN with VPN and WQoS.
Keywords:-Wireless LAN, WLAN, Virtual Private Network, VPN,Wireless Quality of Service technique, WQoS, IEEE 802.11n.

1. Introduction
Wirelesscommunications have gained a great part in communications, offering very importantdevelopment perspectives in mobile telephony,wireless Internet and generally in wireless LANs.Wireless LANWLAN is a very flexible structure fordata communications, which might be implementedeither as analternative of a wired LAN or as an extensionproviding some extracoverage area between a wiredbackbone network and a mobile use [1]. 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 [2]. Among proposals to implement security in WLANs is VPNs. VPNs offer security by means of the integration of authentication, encryption, access control, and session management [3]. VPN provides secure communication through the use of public telecommunication infrastructure,maintaining privacy through the use of a tunneling protocol and security procedures. VPN provides authentication, access control, confidentiality, and data integrity to ensure security of the data [4]. VPNs use encryption techniques to prevent the interception and analysis of datagrams while they are in the public network, and this will increase delay, jitter, packet loss, and packet overhead. As a result the performance of the network will degrade. Quality of Service can help to reduce the effect of VPN. QoS refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency and improved loss characteristics [5].

This paper presents a design of secured WLAN over IEEE 802.11n by utilizing Virtual VPN technique and provides a solution to enhance its performance by using QoS technique. Also it implies studying and analyzing the effect of VPN on the performance of the designed WLAN. Furthermore it provides a way to eliminate the effect of VPN and enhances WLAN performance by utilizing QoS tools for wireless environments WQoS.The present work implements three different scenarios used during simulation and simulation: WLAN, WLAN-VPN, and WLAN-VPN-QoS. The type of VPN tunnel used in this work is; Layer Two Tunneling Protocol over Internet Protocol for Security (L2TP/IPSec). LanTraffic V2 network packet generation and monitoring tool is used to test and analyze the proposed wireless network. Distributed Services Code Point (DSCP) value is used to assign priority for network traffics in order to measure QoS effect.

2. VPN
According to the standard definition provided by the *Internet Engineering Task Force* (IETF), a VPN is "*An emulation of* (a) *private Wide Area Network (WAN) using shared or public IP facilities, such as the Internet or private IP backbones*." [6]. VPN designs can be constructed in a variety of scenarios. The most common deployment scenarios are the following [7]:

i. Remote VPN.
ii. Intranet VPN.
iii. Extranet VPN.

Furthermore VPNs are categorized into three types:

i. Trusted VPNs use the following Data Link Layer technologies (Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP)).
ii. Secure VPNs use the following encryption protocols (Internet Protocol Security (IPsec), L2TP/IPsec, Secure Sockets Layer (SSL), and Transport Layer Security Protocol (TLS)).

iii.

iv. Hybrid VPNs combine aspect of trusted and secured VPNs.

3. WQoS

Some high-layer applications such as data,video, and audio have different requirements inbandwidth, delay, jitter, and packet loss.To support applications with QoS over 802.11WLANs, IEEE 802.11 working group developed a standard called IEEE802.11e [8].

The Enhanced Distributed Channel Access (EDCA) protocol provides QoS in IEEE 802.11 networksby establishing four access classes (ACs). This ACs areparameterized by the following: (1) the arbitrationinterframe spacing for the jth AC: AIFS(j); (2) the minimumcontention window (CW) size for the jth AC: CW min (j); (3) themaximum CW size for the jth AC: CW max (j); (4) the maximumnumber of retransmission attempts for the jth AC: m(j).To transmit a MAC protocol data unit (MPDU) a QoS station(QSTA) must defer its transmission until the channel is idle for atime period equal to the AIFS(j):

$$AIFS(AC)=AIFSN(AC).\sigma+SIFS \qquad (1)$$

Where AISFN (AC) is the number to differentiate the AIFS for each AC QSTA, σ isthe slot timefor 802.11standards, which is determined according to the physicalmedium used, and SIFS is the short interframe spacing [9].Table (1) shows the defaultparameter settingsdefined for different ACs in 802.11e draft standard, whereAC1 for voice is assigned the highest priority while AC4 forbackground is given the lowest priority.

Table 1: Default EDCA parameter set

AC	CWmin	CWmax	AIFSN
AC_VO(Voice)	7	15	2
AC_VI(Video)	15	31	2
AC_BE(Best Effort)	31	1023	3
AC_BK(Background)	31	1023	7

To understand the service differentiation introduced byAIFS and CW, see Fig. (1), wherethere are two stations with packets in AC1 and AC4,respectively.

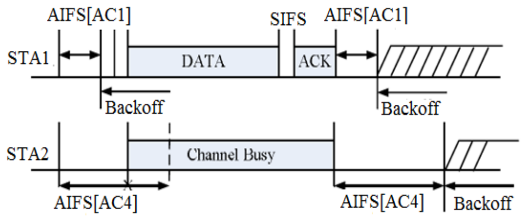

Figure (1): Channel access in EDCA.

The difference of AIFSN is 5, so the AC1 inSTA1 will decrease its back off counter 5 slots earlier thanAC4 in STA2. In addition, the back off counter of high priorityAC may count to zero in this interval and transmit the packet,which results in channel busy due to high priority packettransmission and resynchronization after that.Therefore, the back off counter of low priority AC will bedecreased much slower than that of the high priority AC.

Aninteresting observation from this example is that, since the lowpriority AC cannot access the channel in the intervalintroduced by AIFS difference, different AC experiencesdifferentchannel busy probability, which makes AC with highpriority beneficial.

In a single QoS station supporting EDCA, each AC isimplemented as a separate queue, as shown in Fig.(2).

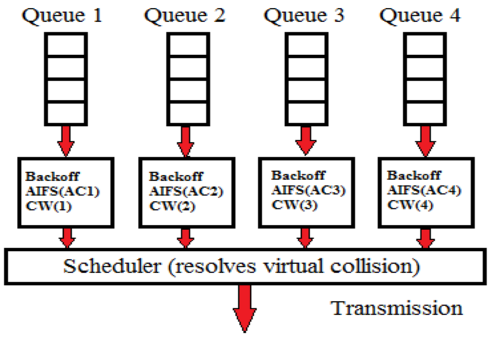

Figure (2): Station with multiple priority queues.

Eachqueue behaves like a virtual station and contends for thechannel access independently. When a collision occurs amongdifferent queues of the same station, i.e., two back off countersof the queues decrease to zero simultaneously, the highestpriority queue always wins the contention, and the lowerpriority queues act as if a collision occurred [10].

4. Simulation

The topology used is an infrastructure wireless LAN in the Client-Server mode using IEEE 802.11n standard. The proposed network consists of four nodes, one server and three clients. These nodes are arranged such that the distance between each Client and the access point is about one meter. A representation for the implemented topology is shown in Fig. (3).

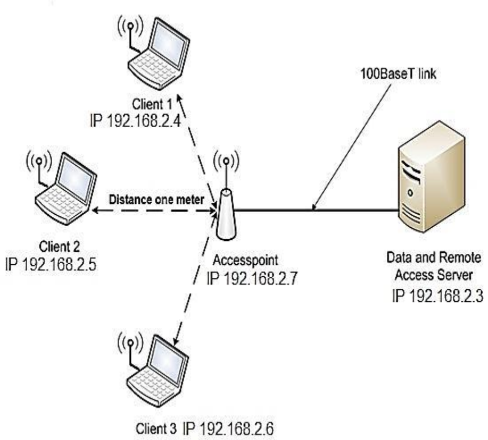

Figure (3): proposednetwork topology.

The server node runs Windows Server 2008. The server node is configured as a domain with Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Remote Access Server (RAS).Client node runs windows server clients operating system and utilizes services provided by server node. The access point type used is (TP-Link Advance Wireless N Router, data rate 300Mbps) with the following configurations as listed in Table (2).

Table (2): Access point configurations

Parameter	**Value**
Basic Service Set Identifier (BSSID)	Moony
Operation Band	IEEE 802.11n
Operation Mode	11n only
Channel Number	1
Channel frequency	2.414 GHz
Channel Width	Auto
IP Address	192.168.1.1

The tool used for traffic generation, network monitoring, and Differentiated Services Code Point(DSCP) values assigning is LanTraffic V2, and for CPU monitoring is CPU Cool. These tools are installed on the server node and client nodes.

The creation and administration of the VPN tunnels is facilitated by the use of ***Windows Server 2008 Routing and Remote Access Services (RRAS)*** role.

The VPN type used in the simulation is L2TP/IPSec and security setting is strongest encryption. VPN configurations used for RAS and clients are listed in Tables (3).

Table (3): Implemented VPN tunnel setting

VPN Protocol	L2TP/IPSec
VPN IP address for Server	192.168.2.100
VPN IP address for Client	192.168.2.101
Encryption Type	MPPE 128 bits
IPSec Encryption Algorithm	AES 256 bits
Device Authentication Method	MS-CHAP
	Preshared Key (key value used: 123456)

The Hardware configurations for server and clients are listed in Table (4).

Table (4): Hardware specifications for server and clients

Node Type	**Operating system**	**CPU**	**Memory**	**Adapter**
Client 1	Windows XP Professional	Intel Pentium M 1.4GHz	768 MB	TP-Link High Power Wireless Adapter IEEE 802.11n
Client 2	Windows 7 Ultimate	Intel Core2 Duo 2.1 GHz	4 GB	TP-Link High Power Wireless Adapter IEEE 802.11n
Client 3	Windows 7 Ultimate	Intel Atom 1.6 GHz	2 GB	Atheros IEEE 802.11n
Server	Windows Server 2008	Intel Atom 1.6 GHz	2 GB	TP-Link advanced wireless N router IEEE 802.11n

The network has been tested according to the following three scenarios:

i. **WLAN**: this scenario is used for testing network characteristics without VPN tunnels and QoS configurations according to the following steps:

a) The wireless network is run in client server mode.

b) Four logical connections are implemented between the network clients and server using LanTraffic V2, as listed in Table (5).

Table (5): Implemented connections between client and server				
Connection	**Connection Source**	**Connection Destination**	**VPN Tunnel**	**DSCP Value**
#01	Client 1	Client 3	No	0x00
#02	Client 3	Client 1	No	0x00
#03	Client 3	RSA	No	0x00
#04	Client 2	RSA	Yes	0x22

c) LanTraffic V2 tool is used to generate network traffic and monitoring the network.

d) Obtained results are used for comparison purposes.

ii. **WLAN –VPN:** this scenario is used to test network characteristics under the effect of VPN tunnels and without QoS configurations. Column (4) in Table (3-14) describes the VPN tunnels locations**.**

iii. **WLAN –VPN – QoS:** this scenario is used to test FCWN characteristics under the effect of VPN tunnels and with QoS configurations. LanTraffic V2 is used to assign priority for VPN traffics in the network by setting the LanTraffic V2 parameter value of DSCP. The priority range value for DSCP is between (0-36) Hex. The QoS characteristics are activated by setting (QoS packet Scheduler) parameter from properties of the wireless NIC in each wireless client.

This implementation procedure is repeated for five times for each scenario, and then the average of five repetitions is taken for all the results obtained from the implementation procedure to obtain accurate results.

5. Simulation Results

Hardware implementation results shows the results obtained from simulation for the scenarios: (WLAN, WLAN-VPN, and WLAN-VPN-QoS).

a. Throughput

The measured average throughput for simulation scenarios is shown in Fig. (4). The results show that the throughput for all scenarios is nearly similar. The throughput value for all scenarios starts with relatively small value and increases gradually with the increase in packet size, and reaches a maximum value nearly (14 Mbps). The figure shows the throughput only when packets size increases and the in case when packets size decreases is similar but in reverse decreases from about (14 Mbps) with the decreasing in packet size to about (0.5 Mbps). Note that some of the throughput is compromised by media access mechanism (i.e. Carrier Sense Multiple Access \ Collision Avoidance (CSMA\CA)) for preambles of transmitted frames, MAC header, and ACK frames.

b. Packet Loss

Figure (5) shows average packet loss for all simulation scenarios. The results show that WLAN has less packet lossthan WLAN-VPN and WLAN-VPN-QoS. Also number of lost packets increases with the increase in packet size. WLAN-VPN has increased packet loss by (15.384%) because the implantation of VPN adds extra header bits to IP packets needed for tunneling operation. WLAN-VPN-QoS has enhanced packet loss but not all the time of simulation. Also WLAN-VPN-QoS shows high packet loss than WLAN-VPN in some period of simulation. Other reasons that increases packet loss is small size packets generated quickly, and this leads to increase collision between wireless nodes and retransmission threshold exceeded eventually packets are dropped. Also small size packets take less time in transmission, (i.e. arrive quickly to destination) and Network Interface Card (NIC) has a limit for the rate for packet processing which leads to buffer over flow and packets to be dropped. For large size packets the transmission delay at interface is increased; also large size packets are spent comparatively long time for decryption than encryption in WLAN-VPN at destination which leads to buffer over flow.

c. Round Trip Time (RTT)

Average RTT is calculated and the results show that RTT for WLAN-VPN, and WLAN-VPN-QoS have RTT greater than that for WLAN, see Fig. (6). This is because of packet encryption and decryption when VPN is implemented. Also Fig. (6) shows that RTT value is affected by packet size (i.e. increases when packet size increases and vice versa). When QoS is implemented, RTT reduces to less than that in WLAN-VPN, and WLAN in some cases. This occurs because VPN traffics assigned high priority (i.e. wireless nodes differ for a short period before transmission or retransmission when congestion occurs). The reasons that cause packet loss mentioned in previous subsection also lead for increasing in RTT for successfully transmitted packets.

d. Jitter

Results for average packet delay variation (jitter) for WLAN, WLAN-VPN, and WLAN-VPN-QoS are shown in Fig. (7). It is clear from the obtained results that encryption and decryption processes used in WLAN-VPN influence jitter about (27.142%) more than increase in packetsize. While implementing QoS in WLAN-VPN-QoS shows less jitter than WLAN and WLAN-VPN.

e. CPU utilization

Thecalculation of average CPU utilization of the three scenarios shows that the same CPU cycles are necessary for all simulation scenarios; see Fig. (8). This is due to the fact that the laptop (Client 2) used in simulation is equipped with 2.1 GHz core 2 duo (i.e. two 2.1 GHz processors) CPU and 4GB of RAM, which can bear such loads and show good response.

6. Conclusions

1. The obtained results show an acceptable network performance under VPN and non VPN in spite of the increase in packet loss, RTT, and jitter.
2. The network shows a small drop in data of (4.2 packet) during WLAN-VPN-QoS scenario as shown in figure (5).
3. The implementation of VPN on the network affects the QoS parameters such that it increases packet loss by 15.384%, jitter by 27.142% and RTT by 32.535% for network.
4. The activation of QoS configurations in simulation shows nearly same results for network.
5. The activation of QoS configurations for (simple, small number of clients, and posse's sufficient bandwidth) network added an extra overhead load on the network traffics that leads to increase QoS parameters.
6. The results of the three scenarios shows that the implementation of VPN and QoS do not affect throughput for all scenarios because of using 802.11n standard which provide transmission rate of300Mbps, and CPU utilization is the same for all scenarios due to the sufficient processing power for the hardware infrastructure even under effect of high traffic and utilizing large packet size in the range of (50-9000) byte.
7. The results prove that an optimal performance level can be achieved if QoS tools are well chosen and configured.

7. References

[1]A. Athanasopoulos, E. Topalis, C. Antonopoulos, and S. Koubias, "Evaluation Analysis of the Performance of IEEE 802.11b and IEEE 802.11gStandards", pp.1, International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06), computer society, IEEE, 2006.

[2] H. Bourdoucen, A. Al Naamany, and A. Al Kalbani, "Impact of implementing VPN to secure wireless LAN", pp. 17, International Journal of Computer, Information, and Systems Science, and Engineering 3:1 2009.

[3] A. Passito, E. Mota, R. Aguiar, L. Carvalho, E. Moura, A. Briglia, and I. Biris, "Using An E-model implementation to evaluate speech quality in voice over 802.11b networks with VPN/IPSec", pp.1124, IEEE, 2005.

[4] A. A. Jaha, F. B. Shatwan, and M. Ashibani, "Proper Virtual Private Network (VPN) Solution", pp. 309, The Second International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST), Computer society, IEEE, 2008.

[5]Cisco Systems, "Internetworking Technologies Handbook", pp. 1055, 1058, 1059, 1063, and 1067, Fourth edition, ISBN: 1-58705-119-7, CISCO press, 2003.

[6] P. Venkateswari, T. Purusothaman, "Comparative study of protocols used for establishing VPN", pp. 160, international journal of engineering science and technology, Vol. 1(3), 2009.

[7] W. B. Diab, S. Tohme, C. Bassil, "Critical VPN security analysis and new approach for securing VoIP communications over VPN networks", pp. 92, 93, and 94, ACM, Chania, Crete Island, Greece, 2007.

[8]D. Gu, and J. Zhang, " QoS enhancement in IEEE802.11wireless local areanetworks", pp. 122, IEEE Communications Magazine, 2003.

[9]R. Pierre, F. Hoefel, " IEEE WLANS: 802.11, 802.11e MAC and 802.11a, 802.11b, 802.11g phy crosslayer link budget model for cell coverageestimation", pp. 0011877, CCECE/CCGEI, IEEE, Niagara Falls, Canada, 2008.

[10]H. Wu, X. Wang, Q. Zhang, and X. (Sherman) Shen, " IEEE 802.11e Enhanced DistributedChannel Access(EDCA) throughput analysis", pp. 224, ICC, IEEE, 2006.

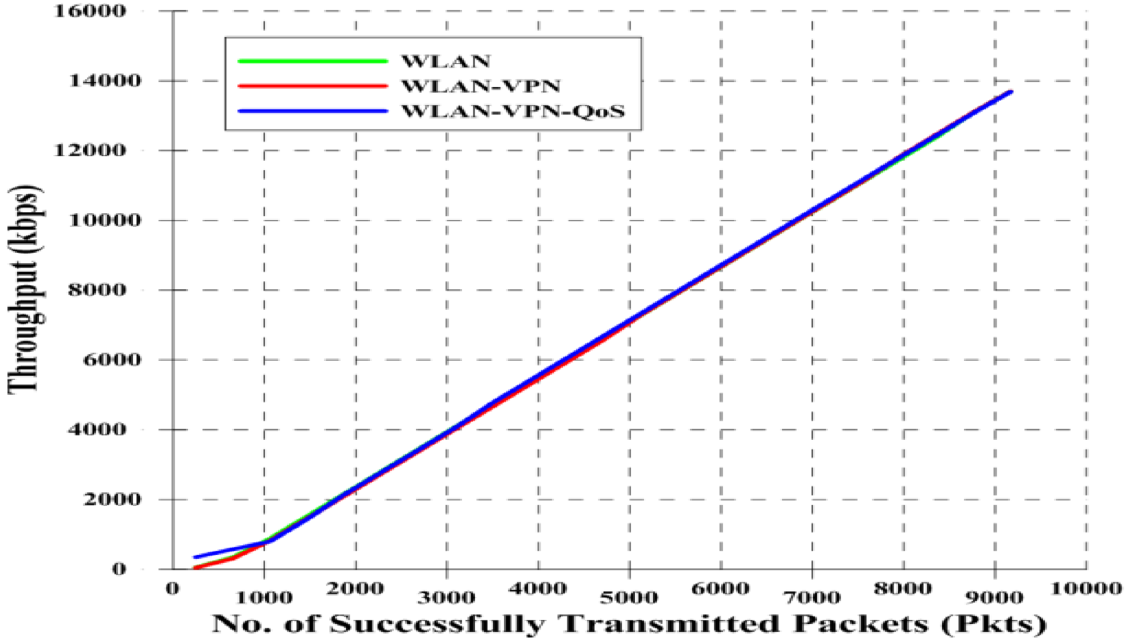

Figure (4): Average simulation Throughput.

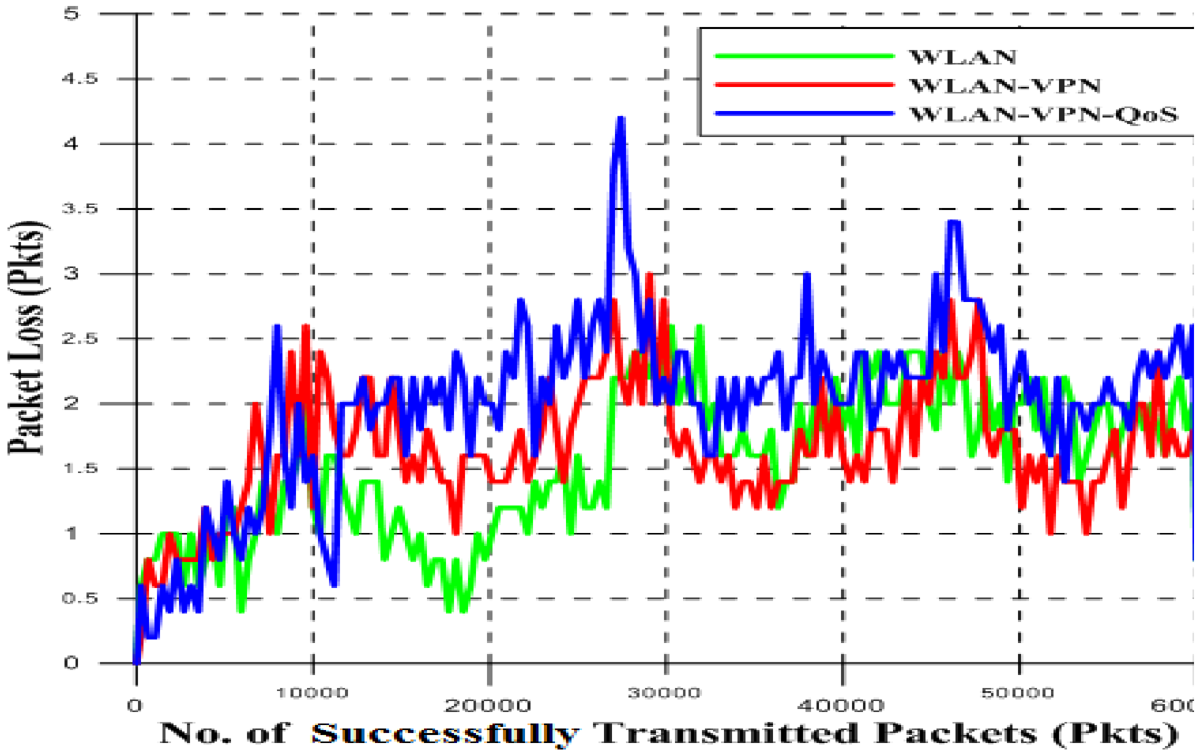

Figure (5): Average simulation packet loss

.

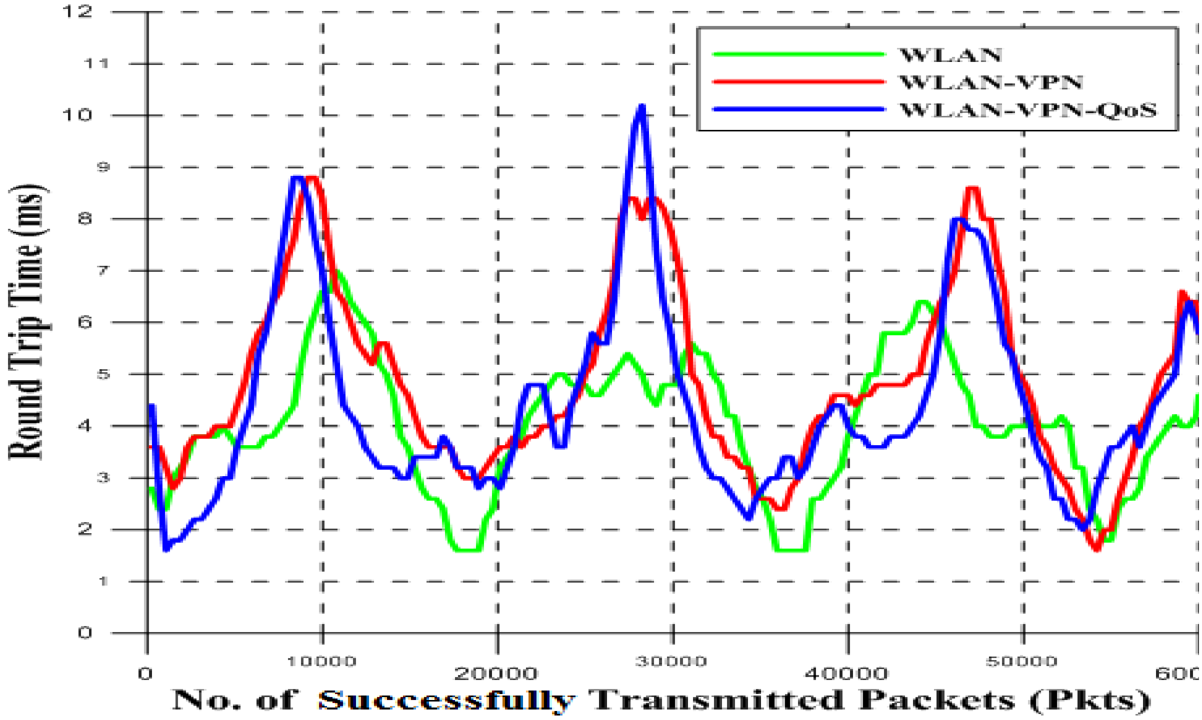

Figure (6): Average simulation Round Trip Time

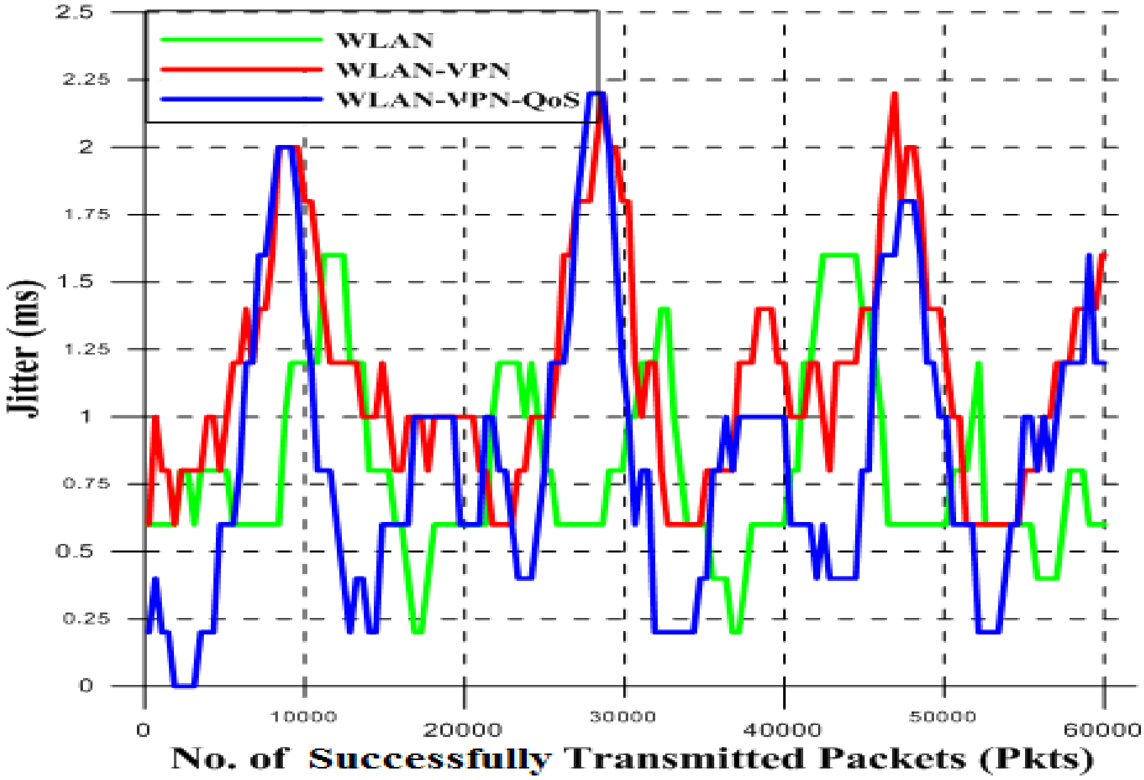

Figure (7): Average simulation jitter.

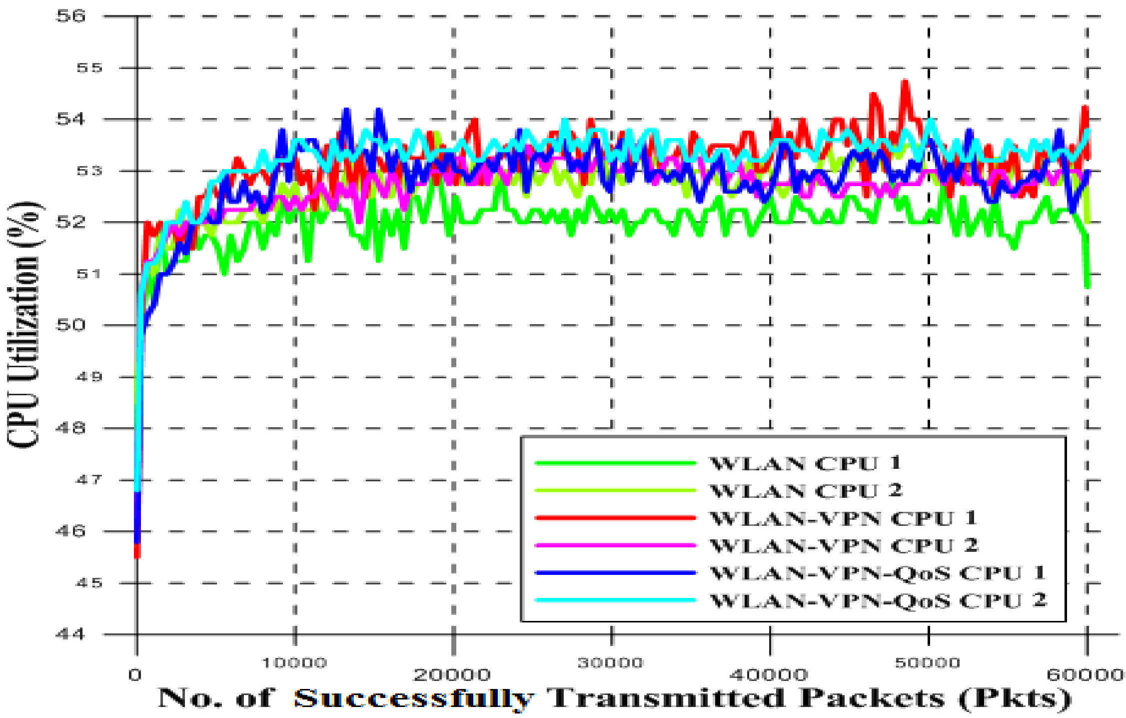

Figure (8): Average simulation CPU utilization.

إستخدام جودة الخدمة اللاسلكية للتقليل من تأثير الشبكة الخاصة الظاهرية على إداء الشبكة المحلية اللاسلكية

صبحي اسود مهند قاسم

moony_q@yahoo.comsubhiaswad@yahoo.com

جامعة النهرين

كلية هندسة المعلومات

قسم هندسة الشبكة الدولية

الخلاصة:

وفرت تكنولوجيا الاتصال اللاسلكي الاتصالات على مدى أكثر منقرن من الزمان، و توفر للمستهلكين حرية في التنقل لم تكن معروفة سابقا. إضافة الى ذالك اصبحت تكنلوجيا الاتصال اللاسلكي تتنافس مع تكنلوجيا الاتصالاتالسلكية. في السنوات الأخيرة، اتسع دورالتكنولوجيا اللاسلكية بشكل كبير، و على نحو متزايد وبما يخدم شبكات المحمول. مع زيادة الاعتماد على الشبكات المحلية اللاسلكية (WLAN)، أصبح أمن هذه الشبكات مصدر قلق كبير لهذه التكنولوجيا لأنها أصبحت خاضعة لهجمات عديدة. من بين المقترحات لتوفير الأمن في الشبكات المحلية اللاسلكية هي الشبكات الإفتراضية الخاصة (VPN). توفر الشبكات الإفتراضية الخاصة الأمن عن طريق الدمج والتوثيق والتشفير والتحكم في الوصول وإدارة الاتصال.

تستخدم الشبكات الإفتراضية الخاصة تقنيات التشفير لمنع اعتراض وتحليل حزم البيانات أثناء وجودها في الشبكات العامة وهذا يؤدي الى زيادة فيتأخر وصول حزم البيانات والتذبذب في مقدار التأخر وصول حزم البيانات من حزمة الى اخرى وفقدان حزم البيانات والزيادة في حجم الحزمة. ونتيجة لذلك فإن أداء الشبكة اللاسلكية يضعف. تمكن جودة الخدمة (QoS) من الحد من تأثير الشبكات الإفتراضية الخاصة. الهدف الرئيسي لجودة الخدمة هو توفير الأولوية وذالك من خلال تخصيص عرض نطاق ترددي والتحكم في التذبذب في مقدار التأخر في وصول حزم البيانات من حزمة الى اخرى وزمن وصول حزم البيانات و التقليل من فقدان البيانات.

يقدم هذا العمل تصميم لشبكة محلية لاسلكية آمنة من خلال استخدام تقنية الشبكة الإفتراضية الخاصة ويوفر حلا لتحسين أدائها عن طريق استخدام تقنية جودة الخدمة اللاسلكية (WQoS). تم اختبار مجموعة من المعايير وتشمل كمية البيانات المرسلة و تأخر وصول حزم البيانات و التذبذب في مقدار تأخر وصول حزم البيانات من حزمة الى اخرى وفقدان حزم البيانات. يتم التحقق من هذه المعايير ولشبكة محلية لاسلكية (WLAN) ثم لشبكة محلية لاسلكية محمية بشبكة إفتراضية خاصة (WLAN with VPN) ثم لشبكة محلية لاسلكية محمية بشبكة إفتراضية خاصة مع جودة الخدمة اللاسلكية (WLAN with VPN and WQoS).