PERFORMANCE PARAMETERS OF WIRELESS VIRTUAL PRIVATE NETWORK

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF INFORMATICS

OF

THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

SÜHEYLA İKİZ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

IN

THE DEPARTMENT OF INFORMATION SYSTEMS

JANUARY 2006

Approval of the Graduate School of Informatics

Assoc. Prof. Nazife Baykal
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assoc. Prof. Nazife Baykal
Head of Department

This is to certify that we have read this thesis and in our opinion, it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assoc. Prof. Nazife Baykal
Supervisor

Assist. Prof.Yusuf Murat Erten
Co-Supervisor

Examining Committee Members

Prof. Semih Bilgen	(METU, EEE)
Assoc. Prof. Nazife Baykal	(METU, II)
Assist. Prof.Yusuf Murat Erten	(METU, II)
Dr. Altan Koçyiğit	(METU, II)
Dr. Ali Arifoğlu	(METU, II)

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: SÜHEYLA İKİZ

Signature:

ABSTRACT

PERFORMANCE PARAMETERS OF WIRELESS VIRTUAL PRIVATE NETWORK

İKİZ, Süheyla
Ms.c, Department of Information Systems
Supervisor: Assoc. Prof. Dr. Nazife Baykal
Co-Supervisor: Assist. Prof. Dr. Yusuf Murat Erten

January 2006, 78 pages

As the use of PC's and handheld devices increase, it expected that wireless communication would also grow. One of the major concerns in wireless communication is the security. Virtual Private Network (VPN) is the most secure solution that ensures three main aspect of security: authentication, accountability and encryption can use in wireless networks. Most VPNs have built on IP Security Protocol (IPSec) to support end-to-end secure data transmission. IPSec is a well-understood and widely used mechanism for wired network communication. Because, wireless networks have limited bandwidth and wireless devices have limited power and less capable CPU, the performance of the networks when VPN's are used is an important research area.

We have investigated the use of VPNs in wireless LANs to provide end – to – end security. We have selected IPSec as the VPN protocol and investigated the effects of using IPSec on the throughput, packet loss, and delay of the wireless LANs. For this purpose, we have set up a test bed and based, our results on the actual measurements obtained from the experiments performed using the test bed.

The wireless LAN we have used is an 802.11g network and the results show that the performance of the network is adversely affected when VPN’s are used but the degradation is not as bad as expected.

Keywords: Wireless, VPNs, Performance, IEEE 802.11g

ÖZ

KABLOSUZ İLETİŞİMDE SANAL ÖZEL AĞ KULLANIM PEFORMANS DEĞERLERİ

İKİZ, Süheyla
Yüksek Lisans, Bilişim Sistemleri
Danışman: Assoc. Prof. Dr. Nazife
Y. Danışman: Assist. Prof. Dr. Yusuf Murat Erten

Ocak 2006, 78 Sayfa

Kablosuz yerel alan ağı uygulamaları kullanımı hava alanları, kafeler, oteller, evler gibi çeşitli ortamlarda de yaygınlaşmaktadır. Mobil bilgisayarlarının ve el cihazlarının yaygın kullanılması ile kablosuz iletişim ağı uygulamalarının artacağı düşünülmektedir. Kablosuz iletişimin en büyük sorunu olan güvenli iletişim, Sanal Özel Ağ (VPN) kullanımı ile aşılabilmektedir. Sanal Özel Ağ kullanılması ile güvenliğin temelini oluşturan kimlik kanıtlama, izlenebilirlik ve şifreleme kavramları kablosuz iletişimde de sağlanmıştır. Günümüzde uçtan uca güvenliğin sağlanabilmesi için kablolu iletişimde kendini ispatlamış IPSec metodu en güvenilir çözüm olarak kabul edilmektedir. Kablosuz iletişimde cihazların sınırlı veri aktarım hızı, sınırlı güç ve işlem kapasitesine sahip olmalarından dolayı kablosuz sistemler Sanal Özel Ağ kullanımı önemli bir araştırma alanı oluşturmaktadır. Tezin amacı, kablosuz yerel alan ağı sistemlerinde Sanal Özel Ağ performans değerlendirmesini yapmaktır. Sanal Özel Ağ yöntemi olarak IPSec seçilerek birim zamanda gönderilen veri miktarı, paket kaybı ve gecikme değerleri incelenmiştir. Ölçümleri yapabilmek için 802.11g kablosuz iletişim standardına uygun test ortamı kurulmuş ve gerçek ölçümler yapılmıştır. Sonuç olarak Sanal Özel Ağ kullanımının kablosuz yerel alan ağında kullanılması performans düşüşüne sebep olmakla beraber bekleninden değerlerden daha az etkilemiştir.

Anahtar kelimeler: 802.11g, performans, Sanal Özel Ağ, Kablosuz

ACKNOWLEDGEMENTS

I would like to thank the many people who have supported me with the realization of my thesis.

First and foremost, I want to thank Assistant Professor Yusuf *Murat* Erten for his extraordinary supervision, support and guidance in conducting research and preparing my thesis. Special thanks go to him for his invaluable comments, suggestions, stimulating discussions and hi thorough review of early versions of this thesis.

I am grateful to my friend Volkan Ertürk for his support, his advice and for sharing with me his experience, time and thoughts.

I would also like to thank my colleague, Emrah Tomur who is Phd. student of the same department for his collaboration and discussions.

I want to thank my family, especially my sister, Selma, for their constant encouragement, support and love.

TABLE OF CONTENT

CHAPTER

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACK :	Acknowledgement
AES :	Advanced Encryption Service
AH :	Authentication Header
AP :	Access Point
ATM :	Asynchronous Transfer Mode
BSS :	Basic Service Set
CBC-MAC:	Cipher Block Chaining Message Authentication Code
CCMP :	Counter-mode / CBC MAC Protocol
CHAP :	Challenge-Handshake Authentication Protocol
CPU :	Computer Processor Unit
CRC-32:	Cyclic Redundancy Code
CSMA/CA:	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD:	Carrier Sense Multiple Access with Collision Detection
CTS :	Clear To Send
CW :	Contention Window
DCF :	Distributed Coordination Function
DES :	Data Encryption Standard
DHCP :	Dynamics Host Configuration Protocol
DIFS :	DCF inter frame space
DLL :	Data Link Layer
DOI :	Domain of Interpretation
DoS :	Denial of Service
DSSS :	Direct Sequence Spread Spectrum
EAP :	Extensible Authentication Protocol
EAPOL:	Extensible Authentication Protocol over LAN
EAP-TLS:	Extensible Authentication Protocol – Transport Layer Security

EAP-TTLS:	Extensible Authentication Protocol – Tunnelled Transport Layer Security
EBSS :	Extended BSS
ESP :	Encapsulated Security Protocol
FCC :	Federal Communications Commission
FCS :	Frame Check Sequence
FDM :	Frequency Division Multiplexing
FHSS :	Frequency Hopping Spread Spectrum
FR :	Frame Relay
GRE :	Generic Routing Encapsulation
GTK :	Group Transient Key
HMAC :	Hashed Authentication Message Code
IBSS :	Independent BSS
IEEE :	Institute of Electrical and Electronics Engineers
IETF :	Internet Engineering Task F
IKE :	Internet Key Exchange
IPSec :	Internet Protocol Security
ISAKMP/ Oakley:	Internet Security Association and Key Management Protocol
ISDN :	Integrated Services Digital Network
ISM :	Industrial, Scientific and Medical
IV :	Initialization Vector
L2F :	Layer 2 Forwarding
L2TP :	Layer 2 Tunnelling Protocol
LLC :	Logical Link Layer
MAC :	Medium Access Protocol
MD5 :	Message Digest 5 Algorithm
MIC :	Michael’s Message Integrity Code
MSDU :	MAC Service Data Unit
OFDM :	Orthogonal Frequency Division Multiplexing
OSI :	Open Systems Interconnection
PAP :	Password Authentication Protocol
PCF :	Point Coordination Function
PFS :	Perfect Forward Secrecy
PIFS :	PCF Inter Frame Spacing
PKI :	Public Key Infrastructure
PMK :	Pair wise Master Key

PPTP	:	Point to Point Tunnelling Protocol
PRF	:	Pseudo-Random Function
PSK	:	Pre-Shared Keys
PTK	:	Pair wise Transient Key
QoS	:	Quality of Service
RADIUS:		Remote Authentication Dial-in User Server
RAM	:	Random Access Memory
RC4	:	Ron's Code
RF	:	Radio Frequency
RFC	:	Request for Comment
RTS	:	Request To Send
SA	:	Security Association
SHA1	:	Secure Hash Function version 1
SIFS	:	Short Inter Frame Spacing
SSID	:	Secure Set Identifier
TCP	:	Transmission Control Protocol
TKIP	:	Temporal Key Exchange Protocol
UDP	:	User Datagram Protocol
VPN	:	Virtual Private Network
WAN	:	Wide Area Networks
WEP	:	Wired Equivalent Privacy
WLAN	:	Wireless Local Area Network
WPA	:	Wi-Fi Protected Access
WVPN	:	Wireless Virtual Private Networks

CHAPTER 1

INTRODUCTION

1.1 The challenges of Wireless Networks:

The productivity, flexibility and cost-savings are major concerns that accelerate the deployment of wireless networks. According to Gartner, wireless markets will reduce costs and new business opportunities will be introduced with new enterprise projects in 2005 – 2010 [1].

The key differences that make it more difficult to design a wireless network lies in the characteristic of medium used. Wire provides guided transmission and the wiring reduces the effects of attenuation. Error rate of wired network has smaller values compared to wireless medium, which is caused a small packet loss rate in lower layers. At the same time, wired networks' have more bandwidth to tolerate the retransmissions and congestion recovery mechanism [2], [6].

Moreover, there is one problem of wireless networks that does not occur in the wired networks; that is not every node can communicate with every other station in a WLAN. In addition to these, the regulations concerning the use of electromagnetic frequencies are restricted and vary from country to country. Until now, the highest bandwidth achieved is 54 Mbps by IEEE 802.11 g wireless physical layer standard. Wireless MAC layer uses Carrier Sense Multiple Access with Collision Avoidance where Carrier Sense Multiple Access with Collision Detection is used in wired networks. Collision detection is not possible in wireless networks hence this mechanism is replaced with collision avoidance.

Security becomes a dominant parameter when we consider the upper layers in the wireless networks. First, the authentication and integrity ensured by using Wired Equivalent Protocol (WEP) has not protected a wireless network against Man-in-the-Middle, Peer-to-Peer and Denial Service attacks. While IEEE 802.11 security group is working on how to build a security protocol against those attacks, Wi-Fİ Protected Access is introduced by Wi-Fİ Alliance as a part of emerging 802.11i standard. It is clear that this standard improves wireless LAN security considerably by enhanced encryption, authentication and key management methods. Yet, there are still issues not addressed by this standard. 802.11i cannot protect the network against threats such as RF jamming and DoS attacks and there is no way to provide granular access control unless a firewall is used. Furthermore, security methods of 802.11i have not been tested long enough to be proven as to be strong as claimed. [4] [5].

1.2 Security Challenges and VPNs:

The Virtual Private Network technology is well understood in wired networks. The main purpose of using VPN is to provide a Local Area Network simulation between branch offices and remote users over the Internet or public telecommunications infrastructures. The secure tunnels are established between the distant offices and the data inside the tunnels is encrypted. Both sites agree on cryptographic entities [7].The most widely used VPN protocol is IPSec protocol [3]. Basically, IPSec Protocol provides authentication through a different authentication protocol such as CHAP, PAP, EAP, certificates, tokens and provides message integrity with the encryption. It is a well understood protocol and is widely used in many real world applications. However, because it introduces extreme overhead its use in wireless network is not very common.

1.3 Thesis Objective and Organization:

In this thesis, we have investigated the effects of using VPN’s in wireless Local Area Networks. We looked at throughput, delay and packet loss in WLANs when VPN’s are used. Chapter 2 covers terms and concepts of wireless data networks and chapter 3 covers virtual private networks. Both technologies are combined in chapter 4 and their advantages and disadvantages are presented. The methodology used for experiments are explained in Chapter 5 in detail. The results are presented and discussed in chapter 6 and conclusion is included in chapter 7 together with further research areas in wireless virtual private networks.

CHAPTER 2

WIRELESS NETWORKING

Although wireless data networks are not a new technology, wired networks lead the deployments in Local Area Networks. Wireless installations are exploding as the wireless product prices decrease and the wireless networks subject are being studied in detail. One of the key developments to trigger the popularity of wireless growth has been the IEEE 802.11 standard, introduced in 1997. This standard provides the same services as wired networks and interoperability with wireless vendors.

The IEEE 802.11 protocol stack is based on the first two OSI layers, Physical Layers and Data Link Layer. Basically, physical layer defines the rules of bit transmission, voltage level, encoding techniques and some electrical and mechanical specifications.

Data Link layer defines the set of rules to use in the transmission offered by physical layer, provide error free transmission to the upper layers. This layer also offers flow control, error detection and recovery. The sub layer of data link layer, Medium Access Control layer is dedicated for broadcast issue that is access methods to share the medium by many stations for the effective use of the bandwidth offered by physical layer.

IEEE 802.11 protocol supports two types of network structures. First one is Ad Hoc networks, which is composed of some wireless nodes connected without an infrastructure. All nodes can communicate with each other if there is a link between them. If there is no direct link then all nodes may use some algorithms to make connections over a group of wireless nodes. The most popular usage of ad hoc networks is for military or disaster purposes. The Ad hoc structure is displayed in Figure 2.1.

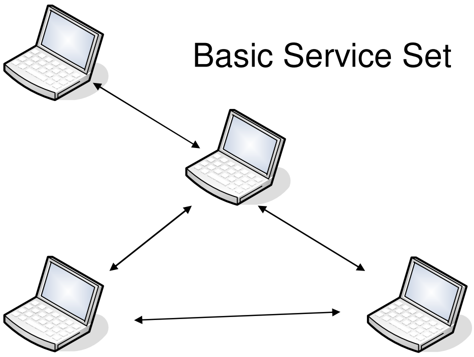

Figure 2-1 : The ad-hoc network structure in the IEEE 802.11 protocol

The second structure is the infrastructure network, which is a common deployment method. A fix Access Point (AP) is used to connect the all wireless nodes that can be connected to the AP with RF links. Wireless Nodes can move in the range of AP without interrupting the communications.

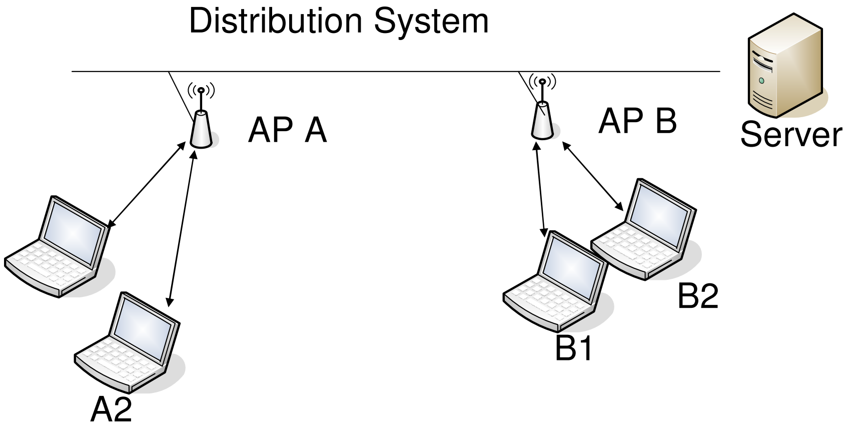

Figure 2-2 : The infrastructure network structure in the IEEE 802.11 protocol

A set of connected wireless nodes form a Basic Service Set. If the wireless nodes are in Ad Hoc network structure then this BSS is called an Independent BSS (IBSS). If more BSS's are connected to each other then it forms an Extended BSS (EBSS) [8].

2.1 IEEE 802.11 Physical Link

IEEE 802.11 supports only 2 Mbps bandwidth which is too slow for most applications. Two extensions of IEEE 802.11 are introduced. One of them is IEEE 802.11a and the other one is IEEE 802.11b

IEEE 802.11b is a new IEEE 802.11 standard and supports up to 11 Mbps. IEEE 802.11b operates on 2.4 GHz radio signalling frequency using direct sequence spread spectrum (DSSS). 2.4 GHz ISM band is a crowded band and used by microwave ovens, baby monitors, cordless phones, and Bluetooth. 802.11a operates on 5 GHz ISM band and uses Orthogonal Frequency Division Multiplexing. OFDM operates extremely efficiently and offers higher data rates while minimizing the effects of multi-path propagation. In June 2003, IEEE 802.11g standard is submitted as an extension of 802.11b and offers 54 Mbps bandwidth using OFDM as IEEE 802.11a standard but takes main functions from the IEEE 802.11b standard. [8], [9].

Spread Spectrum Modulation:

In 1985, the FCC (Federal Communications Commission) allocated three frequency bands for a radio transmission technique, which is called Spread Spectrum. These three bands are Industrial, Scientific and Medical (ISM).Basically, Spread Spectrum uses wider band of frequencies to spread signals compared to normally needed to achieve the same bandwidth. This transmission technique has much greater immunity to noise and interference if they are compared to other radio transmission techniques. ISM bands are in three ranges, 902-928 MHz, 2.4.-2.4835 GHz and 5.725-5.850 GHz [10].

Direct Sequence Spread Spectrum:

In IEEE DSSS, one bit is transmitted as 11 chips and this chip sequence is known as Barker word. The following Barker word is used by every IEEE 802.11 compliant device: 10110111000. 0 is sent as the sequence 10110111000 while 1 is sent as the complement of 0 in sequence of 01001000111. The result in frequency domain is a signal that is spread over a wider bandwidth operates, on 14 frequency channels, each occupying 22 MHz across 2.4 GHz ISM band. DSSS has highest cost and the highest power consumption while it provides highest potential bandwidth (11 Mbps for 802.11b products) [11], [12].

Frequency Hopping Spread Spectrum:

FHSS uses 79 frequency channels and each occupies 1 MHz over 2.4 GHz ISM band. By hopping from one frequency channel to another, it reduces interference since external noise produced by narrowband system would affect the carrier signal. The standard requires 2.5 hops per second while distance between the hops is minimally 6 MHz and various frequency hop sequences may be defined sequentially to number of channels. If a station initializes itself to BSS then one of the valid hops is assigned. These hop sequences are orthogonal to each other to prevent interference. FHSS has lower cost and lower power requirement than DSSS techniques. It is insensitive to radio interference; however and FHSS at most achieves 2 Mbps [13].

Orthogonal Frequency Division Multiplexing:

OFDM modulation is a technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions. 802.11a WLAN technology uses OFDM and transmits up to 54 Mbps in the wider 5 GHz ISM band [14].

2.2 IEEE 802.11 Data Link Layer

IEEE 802.11 is based on Physical Layer and Medium Access Control Layer (MAC). MAC layer builds a bridge between wireless and wired networks. 802.11 MAC layer is very similar to 802.3 and both are designed to support multiple users to access same shared medium.

802.3 Ethernet LANs uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol for detecting and handling the collisions, (two or more station starts the data transmission simultaneously). To detect the collision, a node can transmit and listen in the same time. However, this is not possible in 802.11 WLANs. To handle this problem, 802.11 uses a slightly modified protocol known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) .Due to the possibility of undetected collisions, CSMA/CA uses explicit packet acknowledgment (ACK). The receiver checks the Frame Check Sequence field to detect erroneous frames. The sender sends the frame and waits for acknowledgement frame. The failure of frame exchange is experienced in transmission frame or transmission acknowledgement frame. If ACK is not received in a certain time then the frame is retransmitted.

Since not all stations are in the range of a certain area there may some stations that cannot hear each other but can hear to the Access Point. This 802.11 MAC layer Problem is called Hidden Station problem. To solve this problem Request to Send (RTS) and Clear to Send (CTS) frames are exchanged before the actual data transmission starts.

- A station wishing to send frame send RTS frame to the destination
- If the destination is ready to accept frames it sends CTS
- The third node hears this CTS since it is in the range of AP
- After receiving the CTS the sender starts to send data frames
- If destination node receives correctly then it sends ACK frame

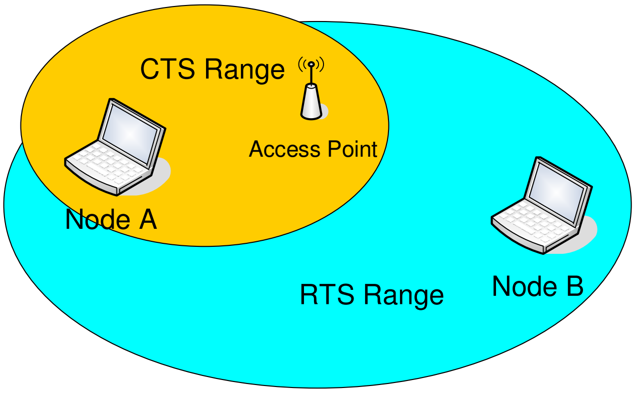

Figure 2-3: Hidden Node Problem

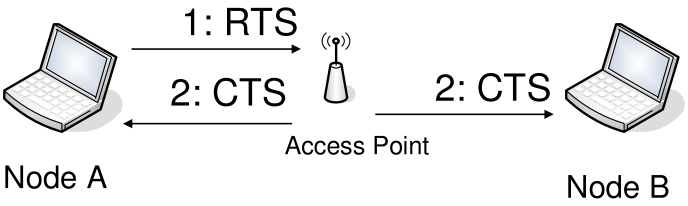

Figure 2-4: RTS and CTS Usage

The basic access method for 802.11 is the Distributed Coordination Function (DCF), which uses CSMA / CA. Each node listens for other nodes and if the channel is idle, the node may transmit. However if it is busy, each node waits until transmission stops, and then enters into a time interval which is calculated by a random back off algorithm. This prevents multiple stations immediately attempting to access the medium after the completion of the preceding transmission.

Packet reception in DCF requires acknowledgement as shown in Figure 2.5. Short Inter Frame Space (SIFS) is a time between completion of packet transmission and start of the ACK frame. ACK frames have a higher priority than other traffic. Fast acknowledgement is one of the salient features of the 802.11 standard. Packets other than ACKs must wait at least one DCF inter frame space (DIFS) before transmitting data. If sender senses the medium as busy then it determines a random back-off period. The obtained value is set to an internal timer and the station waits for it to each zero. The timer begins to decrement when DIFS expires. If the timer reaches zero, the station may begin transmission. However, if the channel is started to be used by another node before the timer reaches zero, the timer setting is frozen at the decremented value and it restarts from this frozen value when the medium is free.

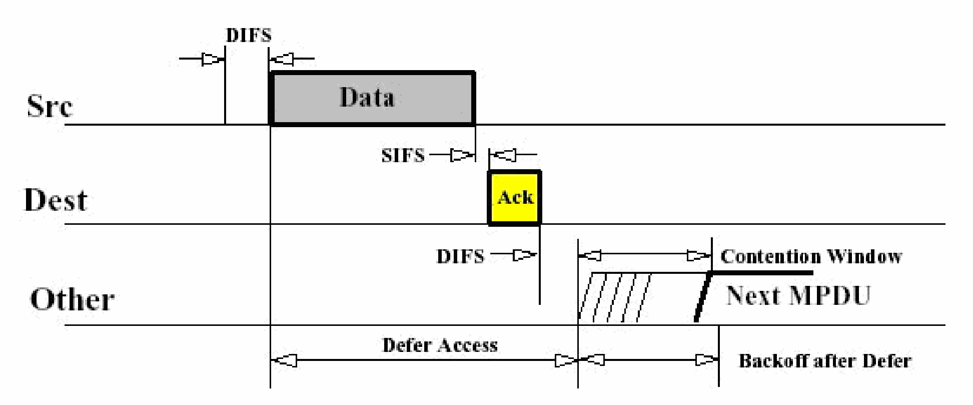

Figure 2-5: CSMA/CA Back off Algorithm

The other mode is Point Coordination Function (PCF) to allow contention-free communication between AP and nodes. In PCF mode, AP polls each node in round-robin fashion. PCF is optional where DCF is a must. A node polled by AP must answer the AP with in PCF Inter Frame Spacing (PIFS) with SIFS interval, if it has data to send. The AP enters and ends the contention free period by sending a beacon frame.

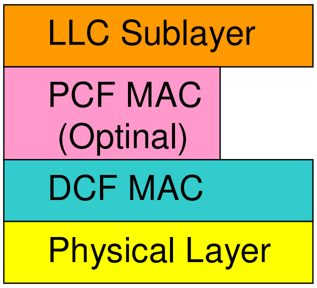

Figure 2-6: 802.11 Layers

To sum up inter frame times are given as:

- SIFS – shortest IFS. Highest Priority. Used by ACK, CTS and 2nd or subsequent MSDU of a fragment burst.
- PIFS – Used by stations operating under the PCF to gain access to the medium. Higher priority than DCF based frames.
- DIFS – All stations operating under the DCF mode.
- EIFS – Used by DCF stations when a frame transmission results in a bad FCS value.

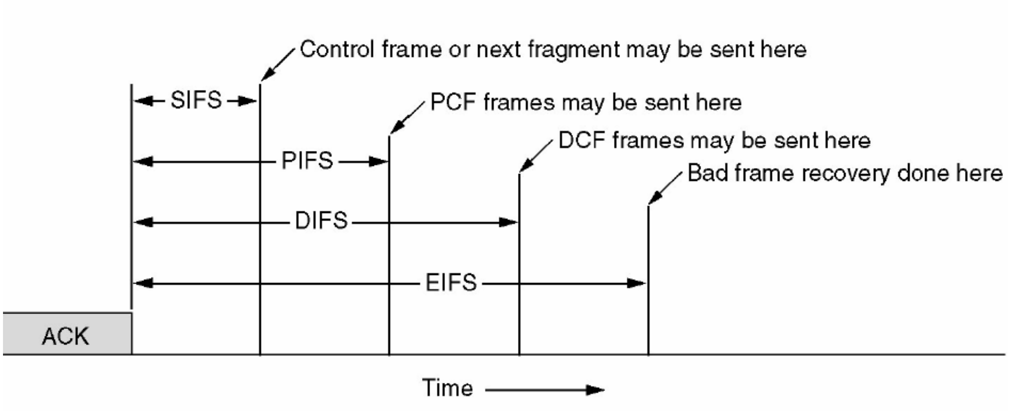
Control frame or next fragment may be sent here
SIFS
PCF frames may be sent here
PIFS
DCF frames may be sent here
Bad frame recovery done here
DIFS
EIFS
ACK
Time

Figure 2-7: Wireless LAN Protocol CSMA/CA Inter frame Spacing in 802.11

2.3 IEEE 802.11 Security

The main aspect that makes wireless security different than security of wired networks is the uncontrollability of physical access due to transmission of data with radio waves. This fact makes 802.11 networks vulnerable to eavesdropping. Wired Equivalent Privacy (WEP) is designed mainly to mitigate these weaknesses in wireless LAN security by aiming to provide privacy of transmitted data using encryption and trying to prevent tampering of messages by means of integrity checking. RC4 algorithm is used for encryption with 64 or 128 bit long keys, 24 bits of which is a random number known as Initialization Vector (IV), and CRC-32 integrity checking algorithm is used for message integrity. A detailed explanation of WEP can be found in IEEE 802.11 standard [17].

In addition to data privacy and integrity, another issue needed for security in any network is authentication of parties involved in communication. In the context of wireless LANs, this means prevention of unauthenticated clients from accessing the network and ensuring that legitimate users communicate with genuine access points. In 802.11 standards, only authenticity of wireless clients, not access points, can be controlled by checking whether the client possesses the correct WEP key. Use of Service Set Identifiers (SSIDs) and Media Access Control (MAC) address of client devices are the other common methods implemented in 802.11 networks for authentication.

Traditional 802.11 security mentioned in first two paragraphs of this section is considered to be inadequate because of many weaknesses that could enable attackers to break security of wireless networks. WEP, for instance, has much vulnerability in both its encryption and integrity checking processes. Because of insufficient IV space, an unauthorized person can read the transmitted data using decryption dictionaries [18], or he/she can crack the WEP key utilizing the weaknesses in generation of key streams [19]. Also, frailty of CRC-32 algorithm against attacks can be exploited by malicious people to modify packets or even insert new messages into the network [20]. Missing a key management mechanism, flaws of shared key authentication [21], and not having a way to authenticate access points are the other weaknesses of conventional 802.11 securities.

IEEE soon realized the deficiencies in conventional 802.11 security protocols and formed Task Group I (TGi) to address these issues. However, realizing that IEEE would not be ready to finalize the standard in time to meet their customer demands, Wi-Fi Alliance decided to use some of 802.11i's capabilities and created an interim solution named Wi-Fi Protected Access (WPA) [22]. In this way, vendors implemented improved security protocols such as TKIP and 802.1X in their products and provided WLAN users with relatively more secure solutions. After a three and a half years work, IEEE 802.11i standard [23] was finally ratified on June 24 of last year. In addition to the IEEE 802.1X port based authentication protocol and TKIP encryption included in WPA, 802.11i has AES encryption in counter mode with CBC-MAC (CCMP) and a four-way handshake mechanism for robust key management. All of these protocols and methods are discussed in the rest of the section.

The 802.11i specification can be seen as a three-fold enhancement to traditional WLAN security. Firstly, data privacy and integrity is improved with TKIP encryption (Temporal Key Integrity Protocol) used with MIC (Michael Message Integrity Code) and AES (Advanced Encryption Standard) used with CCMP. Secondly, entity authentication, that is the authenticity of wireless clients and access points, is accomplished by 802.1X protocol. And, finally, strong key generation and automatic key distribution is performed based on 802.1X and EAPOL (Extensible Authentication Protocol over LAN).

TKIP, also called WEP2, uses the same encryption algorithm RC4 as WEP to allow compatibility with legacy wireless hardware. However, its implementation is different to avoid WEP's vulnerabilities. In order to ensure that encryption keys are not reused, length of Initialization Vector is increased to 48 bits. Also, a 128-bit secret key called temporal key (TK) shared by encryptor and decryptor is employed. This TK is combined with MAC address of the client and the first 16 bits of IV are padded producing the key stream used for encryption. This is called per packet key mixing and ensures that each computer uses a different key. TKIP uses IV also as a sequence counter to prevent replay attacks. Moreover, for bringing improvement to integrity checking of 802.11 networks, Michael's Message Integrity Code is employed. By means of a 64-bit MIC computed with Michael's algorithm, alterations in the contents of transmitted data can be detected. TKIP is optional in 802.11i.

In addition to TKIP, 802.11i defines CCMP as a long-term solution. CCMP employs the stronger encryption of AES, which uses the CCM mode with a 128-bit key and a 128-bit block size of operation. The CCM mode uses counter-mode (CTR) together with cipher block chaining message authentication code (CBC-MAC). CTR is used to encrypt the payload and the MIC to provide confidentiality. CBC-MAC computes the MIC to provide packet integrity. CCM requires a fresh TK for each session and needs to refresh the TK when the packet number (PN) is repeated. The PN is incremented for each MPDU and can be used to prevent a replay attack with the receiver's replay counter. Though CCMP can provide much stronger security compared to TKIP, it requires additional hardware to improve encryption performance. Therefore, legacy 802.11 hardware will not be upgradeable in many cases. CCMP is mandatory in 802.11i.

802.1X is a port based authentication framework, and when used with Extensible Authentication Protocol (EAP) in a wireless LAN, mutual authentication between clients (supplicant) and access points (authenticator) can be achieved via an authentication server, which is usually a RADIUS server. In 802.1x, port represents the association between the supplicant and authenticator. There are two main types of ports in 802.1x. These are uncontrolled ports and controlled ports. Uncontrolled ports allow communication between devices on a LAN without having to make an access control decision. In a typical 802.11i environment, uncontrolled ports are only used for the authentication exchange that occurs between supplicant and authentication server through authenticator. A controlled port is an entry point to the LAN resources that a supplicant requests access to and the same resources an authenticator is there to protect. Until a client is authenticated by the authentication server, the only port that allows communication is the uncontrolled port. The authentication exchanged in 802.1X takes place over EAP. The major advantage of this is that several mechanisms such as EAP-MD5, EAP-TLS, EAP-TTLS or EAP-PEAP can be chosen as authentication method. Thus, either certificate or password based authentication of both parties can be performed. The typical EAP message exchange that occurs during 802.1X authentication process is shown in Figure 2.8.

Key management and establishment of 802.11i relies on 802.1X and consists of two phases called four-way handshake and group key handshake. First one is to establish transient keys for unicast traffic and the letter is for broadcast traffic. Before four-way handshake, however, supplicant and authentication server independently generates pair wise master key (PMK) and authentication server sends PMK to the authenticator through a secure channel. The four-way handshake then uses PMK to derive and verify pair wise transient key (PTK).

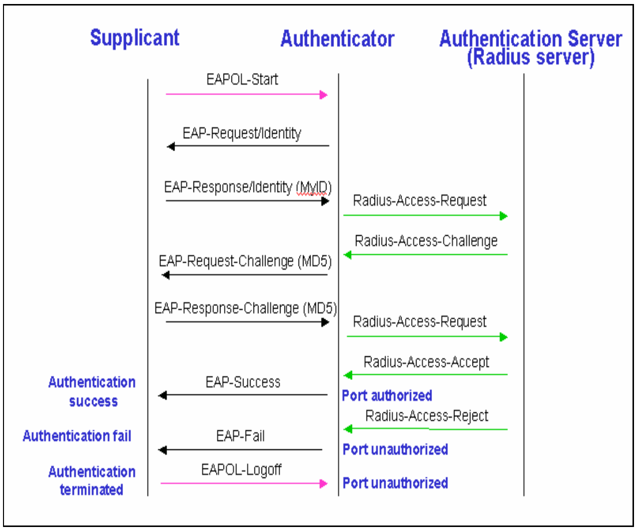

Figure 2-8: 802.1x message exchange

Thus, it is ensured that session key between supplicant and authenticator is fresh. Four-way handshake starts with authenticator sending a message to the supplicant. The first message contains key information and Anonce. In the four-way handshake, Anonce will never be reused. So, it is safe against replay attack. Receiving the first message, supplicant validates Replay Counter field and generates a new nonce called Snonce. By using Pseudo-Random Function (PRF) algorithm with Anonce, Snonce, PMK, and other information as inputs, supplicant derives PTK. Supplicant then sends back the second message containing key information, Snonce, supplicant's RSN IE, and MIC back to the authenticator. Upon receiving this message, authenticator validates the message by checking the replay counter. It then derives

PTK if second message is validated. Because authenticator uses the same algorithm and the same inputs, PTK derived by authenticator will be the same as the one in the supplicant. Authenticator also verifies MIC and RSN IE bits. If these identical, authenticator sends the third message to the supplicant. The third message includes the key information, Anonce, MIC, and authenticator's RSN IE. Receiving third message, supplicant first verifies message by checking Replay Counter and Anonce and then compares RSN IE with the one received If RSN IE is correct, supplicant further checks MIC. Supplicant sends back the fourth message to the authenticator if the MIC is valid. The fourth message includes key information and MIC. After fourth message is received by authenticator, it checks Replay Counter and MIC, and four-way handshake is completed if they are valid. The fourth message is used to acknowledge to the authenticator that the supplicant has installed the PTK. The PTK is only known by the supplicant and authenticator. It is used as a key to encrypt data. Similarly, group key handshake enables the authenticator to deliver the group transient key (GTK) to the supplicant so that the supplicant can receive broadcast messages. Like the four-way handshake, the messages exchanged in the group key handshake also use the EAPOL-Key format.

IEEE 802.11i standard have been studied in this section. It is clear that this standard improves wireless LAN security considerably by enhanced encryption, authentication and key management methods. Yet, there are still issues not addressed by this standard. First of all, 802.11i cannot protect against threats such as RF jamming and DoS attacks and there is no way to provide granular access control unless a firewall is used. Furthermore, security methods of 802.11i have not been tested long enough to be proven as strong as claimed. Another point is that legacy Wi-Fi hardware cannot be upgraded to use 802.11i just by a firmware update but new hardware is needed. To sum up, IEEE 802.11i standard improves security of WLANs considerably, but it will certainly not be the last word in this area.

CHAPTER 3

VIRTUAL PRIVATE NETWORKING

Many large or medium corporations have geographically distributed systems that have to be connected together. The Internet is very common public network and high speed networks like the metro Ethernet brings higher speeds in transmission compared to the past. Therefore the corporations use the Internet as public network for point to point connection. This logical connection topology usually needs s secure technique and the most common of these is a Virtual Private Network (VPN).

The VPN is defined as “a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed though some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis” [24]. Huston and Ferguson also had a simpler, more approximate, and much less formal description: “A VPN is a private network constructed within a public network infrastructure, such as the global Internet.”

VPN technology is first introduced by AT&T known as Software Defined Networks (SDNs) in late eighties. The dedicated and switched lines are used in long-distance WANs to provide connectivity. The data is routed to public networks and according to lines setup or switched database the data is routed to the other end. The cost of lines between long-distance is incredibly high and the WAN line speeds were limited to support LAN speeds.

The second improvement came with X.25 and Integrated Services Digital Network (ISDN) technologies. These two technologies allow data packet streams across the public network structure. So, the lower cost is obtained then the popularity of internetworking is gained. The speed was still low and the performance was not obtained in the usable level.

To solve the performance issue, the cell based networking is introduced. These technologies are called as Frame Relay (FR) and Asynchronous Transfer Mode (ATM). This virtual circuit switching concept was a new concept for the earlier technologies. Firstly, the sender request a circuit with the given destination information. The communication devices in public network establish the specified circuit between sender and receiver according to the manually or automatically obtained databases / switching tables. After the initialization, the sender inserts the data packets and these data packets are switched to the receiver with specified length cells. The specific cell length improves the Quality of Service. ATM also supports different transmission agreement which takes the guaranteed bandwidth, usable bandwidth or variable guaranteed bandwidth e.g. VBR, CBR, ABR...

As the Internet started to be used widely, IP became the fundamental protocol of data communications. Due to this, user requirements changed. The requirements can be list as global accessibility, easy to implement and end-to-end security with loss of details. Then, IP based VPNs are introduced to provide all of these user requirements. The IP based VPNs are developed over tunneling technology which is based on encapsulation original data packets with some cryptographic techniques. Then the encapsulated packets are routed to public network and the public network routes the packet to the destination. Two major protocols of IP VPNs are implemented and used widely. These are Internet Protocol Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and L2TP / Internet Protocol Security (L2TP/IPSec).

3.1 Types of VPN Usage

There are also three types of VPN usages. First one is Remote Access VPNs, the user /client can access remotely to network resources anytime and anywhere. To be able to implement remote access, the remote user / branches need to have a local connection to Internet Service Provider. The Remote Access VPN Server is located in the main site and allows / rejects the remote users according to policies and users access rights.

.

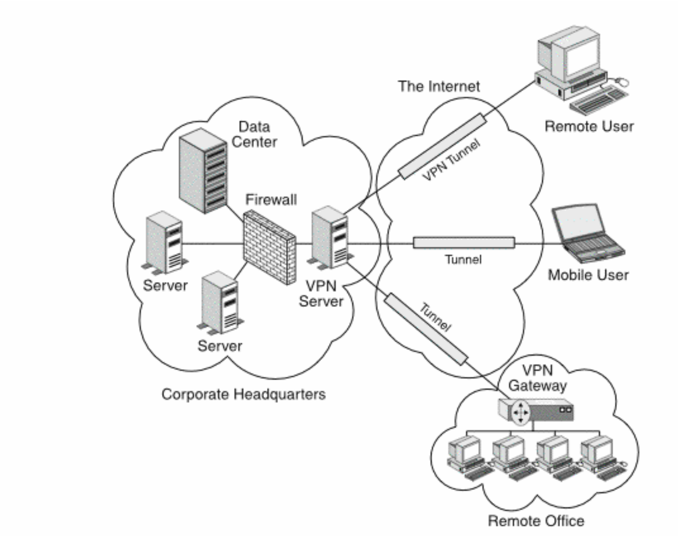

Figure 3-1: The Remote Access VPN

Second, one is Intranet VPNs. This usage is for connecting the branch offices to the main site. The connection between the main side and branches are setup over the Internet connection [25].

The last usage is the extranet VPNs. The tunnel is established between a company and the company's partners, for the customers to access extranet resources [26], [27].

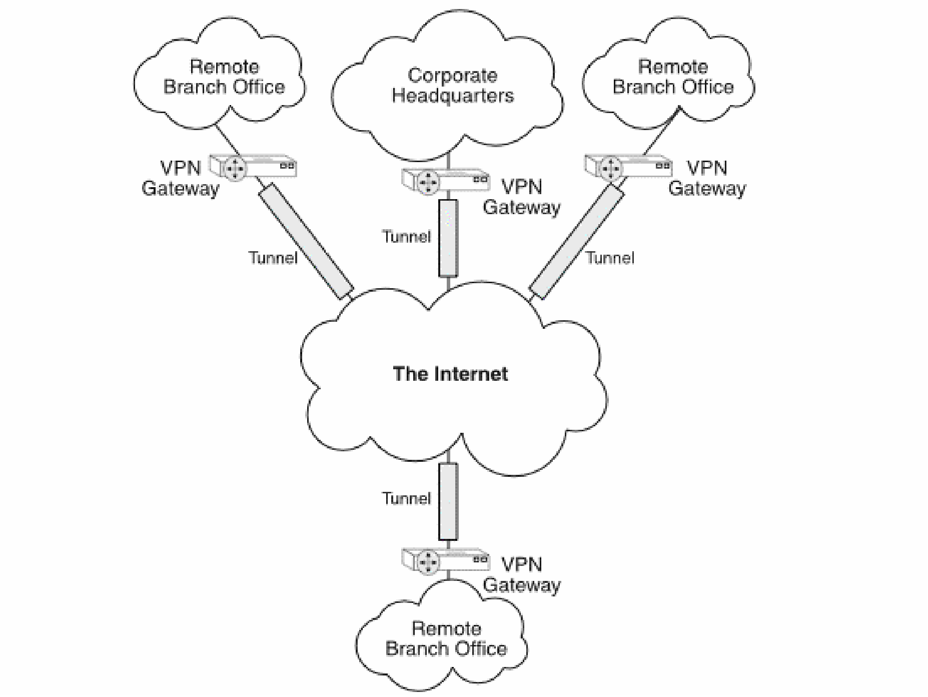

Figure 3-2: The Intranet setup based on VPN

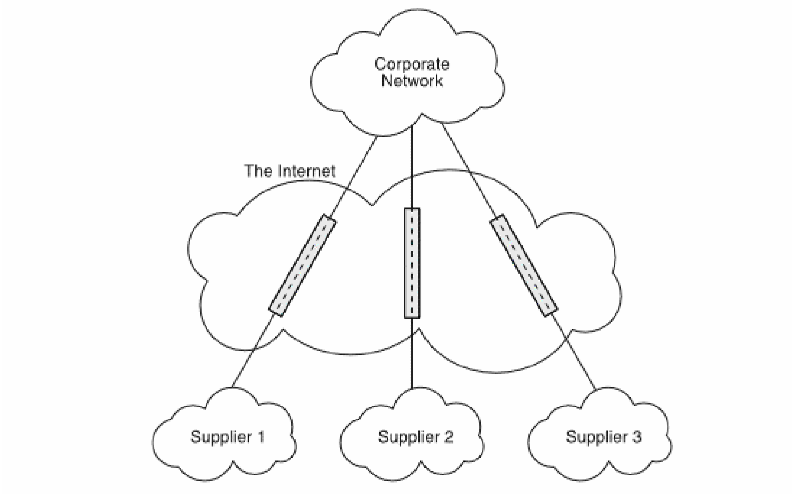

Figure 3-3: The Extranet VPN setup

VPN requirements can be classified into five categories. [25], [26], [27]

- Security: The security level in public network is very low due to intranet security level. Security is provided by authorizing users per packet / per session, data encryption for confidentially, integrity and authenticity.

- Availability and Reliability: the availability and reach ability is extremely depends on public network performance. VPN setup time may vary in time, speed and the location.
- Quality of Service: The critical application requires more QoS during the data transmission. This is also depends on the public network and its performance parameters.
- Manageability: The two parts of management is required. First one is enterprise resources management and the second one is the management of public network.
- Compatibility: The public network operates on IP protocols and the VPN software must work together with public network and also the intranet protocols

Basically, two types of VPN structure is defined by Microsoft to support 3 different VPN usages as mentioned above. A remote client / single computer request an access to the enterprise intranet in first usage. The remote client is authenticated with the VPN server in the enterprise network and then send encrypted data packets originating from the remote client. That is called “Remote Access VPNs”. Two private networks are connected to each other between “Router-to-Router VPN Connection “. The calling router is authenticated with the other end router by the help of VPN server attached to the other private network. First, router-to-router connection is established then the packets between the routers are encrypted. Both types of connection mentioned above uses 2 main tunneling protocols; PPTP, L2TP / IPSec

3.2 Point-to-point Tunneling Protocol

In March 1996, Microsoft and US Robotics demonstrated PPTP at Networld. The PPTP was in beta version at first demonstration then the PPTP is released by early 1997. Cisco was the top router manufacturers in late June 1996, Cisco has developed Layer 2 Forwarding (L2F) VPN protocol .Microsoft and Cisco® Systems, Inc submitted an application to the Internet

Engineering Task Force PPP Extensions working group to propose a combination of Microsoft's PPTP implementation to date with Cisco's Layer 2 Forwarding (L2F). ETF has then announced one industry-wide specification for a Virtual Private Networking: Point-to-point Tunneling Protocol is defined in RFC 2637. PPTP assumes to have a common / public connection between PPTP client and PPTP server. PPTP use TCP connection to create, maintain and terminate the tunnel. PPTP encapsulated the data packets into IP packets at two sides. The data packets can be encrypted, compressed or both. The authentication between PPTP client and server takes place in creation of the tunnel. This type of VPN may use Extensible Authentication Protocol (EAP), Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) for authenticating remote clients. An IP connection between PPTP client and PPTP server is made by allocation of TCP port 1723.

There are two types of PPTP packet type. The first one is Control packets and the other one is Data packets. Control packets are used for setup, maintain and terminate the tunnel and also periodically send inquiries on status of the clients and servers.

A PPTP connection control message is formatted as follows:

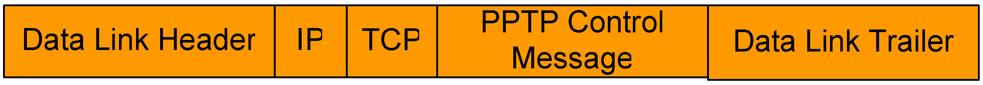

Figure 3-4 : PPTP Connection Control Packet

After the tunnel is established, all the parameters are agreed on how to encapsulate the data packets. PPTP protocol is an extension of Point-to-Point Protocol (PPP) and data packets are created in PPP packet format. This makes the application is independent of IP protocol and allows to operate on multiple protocols. PPTP encapsulates these PPP packets with modified Generic Routing Encapsulation (GRE) header. GRE is defined in

RFC 1702 and is used for lightweights, general purpose and simple transmission over IP connectivity. And GRE header includes the VPN client IP address and VPN server IP addresses as source and destination addresses. The data link layer encapsulation takes place according to the access type. PPTP encapsulated data packet is formatted as:

PPP Header	IP Header	GRE Header	PPP Header	Encrypted PPP Payload	PPP Trailer

Figure 3-5 : PPTP Packet Deployment

Media Header
IP Header
GRE Header
Payload Packet

Figure 3-6 : Packet Format in general

The following figure out the all PPTP setup, data exchange and termination of the tunnel. [29], [28]

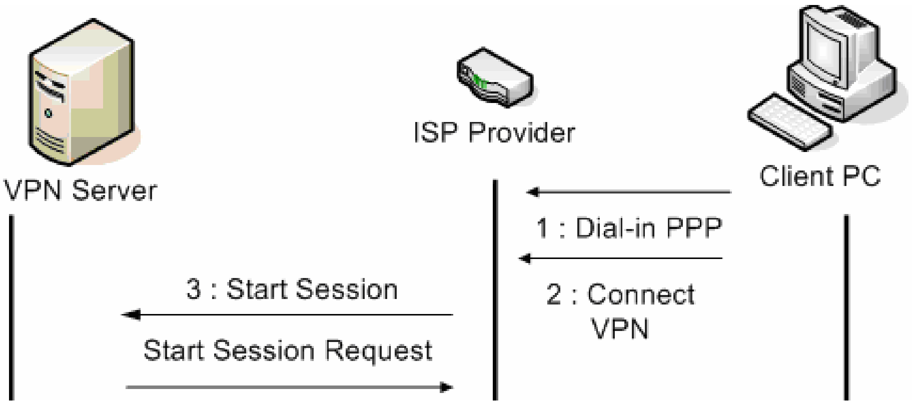

Figure 3-7 : PPTP setup and transmission

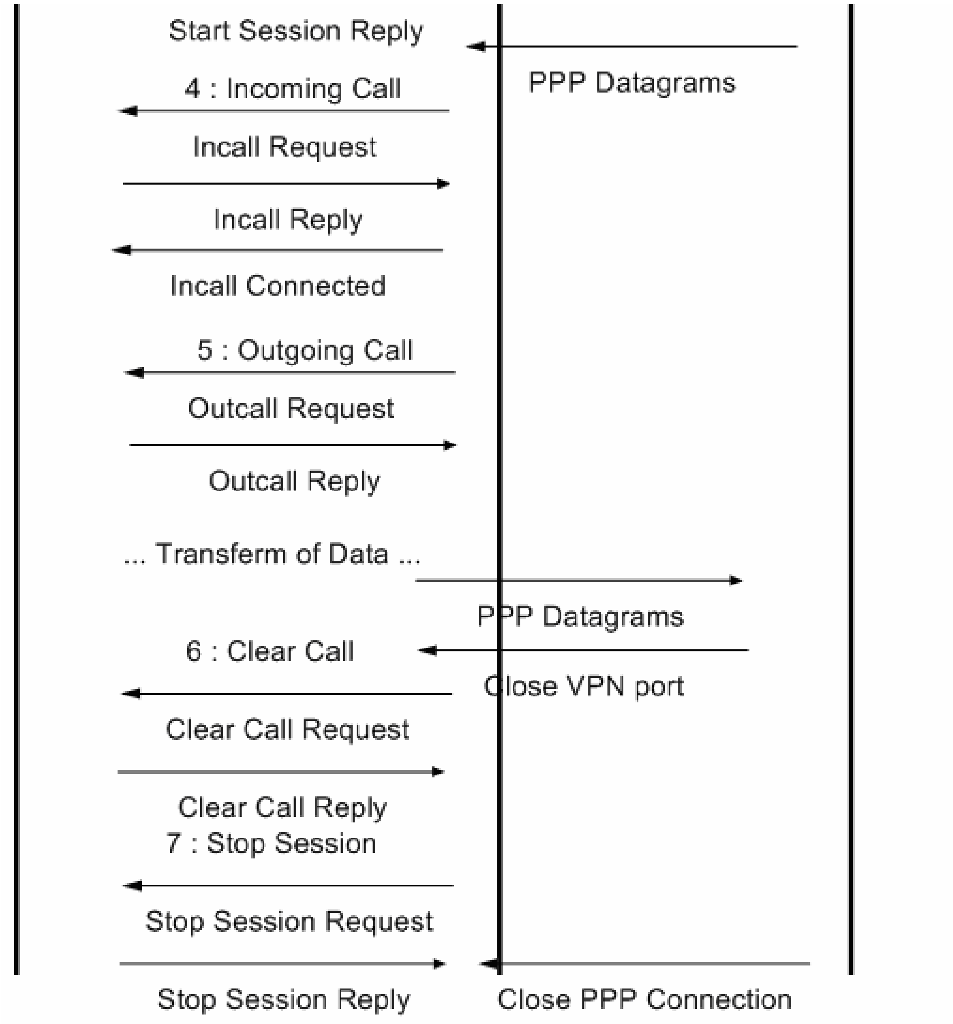

Figure 3-7 : PPTP setup and transmission (contd.)

3.3 Layer Two Tunneling Protocol

Layer Two Tunneling Protocol (L2TP) is a combination of PPTP and Layer 2 Forwarding (L2F), a technology proposed by Cisco® Systems, Inc. Two incompatible tunneling protocols are placed in the marketplace and causing customer confusion, the IETF mandated that the two technologies be combined into a single tunneling protocol that represents the best features of PPTP and L2F. L2TP is documented in RFC 2661. L2TP also encapsulated data packet to be sent over public IP networks. Unlike PPTP, L2TP encapsulates the packet into UDP packets. These UDP messages are exchanged for tunnel setup, maintenance and termination and also data transmission. The data packets can be encrypted, compressed or both. L2TP provides encryption of the data by means of IP Security Protocol (IPSec) that is placed in network layer. The authentication between L2TP client and server is done during the creation of the tunnel. This type of VPN may use Extensible Authentication Protocol (EAP), Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) for authenticating remote clients. An IP connection between PPTP client and PPTP server is done by allocation UDP port 1701. There are also two types of L2TP packet types. The first one is Control packets and the other one is Data packets. Control packets are used to setup, maintain and terminate the tunnel and also periodically send inquiries on status of the clients and servers. An L2TP connection control message is encrypted since TCP connection is not established. The L2TP control message is formatted as follows:

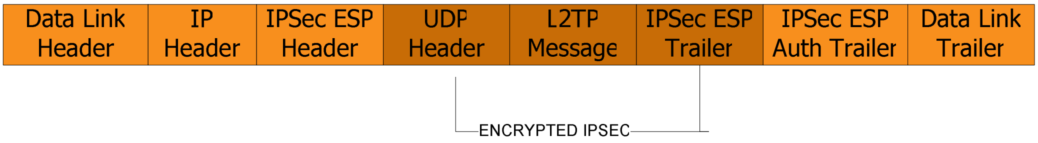

Figure 3 Error! No text of specified style in document.**-8: L2TP Control Message**

L2TP data encapsulation is done in many steps. The data is encapsulated into PPP packet and L2TP Header is appended to PPP packets. Then the total encapsulated packets are inserted into UDP packet format. Then encryption takes place and the packet is encrypted and appended with IPSec header and trailer. Then the remote VPN client and VPN server IP addresses are located in IP header. At the end, the data link encapsulation takes place according to the transmission medium [30].

The L2TP data packet format is shown below:

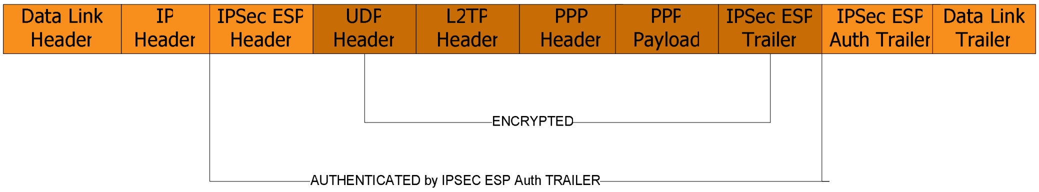

Figure 3-9: L2TP Packet Encapsulation

3.4 Internet Protocol Security

Internet Protocol Security, shortly IPSec is designed by IETF. The main aim is to provide Network Later security mechanism. IPSec is very tightly integrated to IP protocol and this integration removes the modification of the other OSI layers. IPSec is also transparent to the users from the point of their IP.

Security Association is the major concept of IPSec. SA is the unidirectional connection using set of VPN parameters. An SA defines the authentication algorithm, protocols, keys, modes and authentication keys for Authentication Header and Encapsulation Security Protocol, encryption and decryption algorithm keys, source address and time-to-live for each key, some cryptographic parameters for synchronization. Since the SA is unidirectional, two SA (SA bundle) is defined for the communication between two sides.

IPSec protocol has 3 major parts. These are authentication and data integrity, confidentially and Key Management. The authentication and data integrity part provides authenticity of the sender and detects modification on the packets, if any. The confidentiality part ensures that unauthorized access does not take place by means of some cryptographic functions. Internet Key Exchange Protocol is used for key exchange and IKE negotiated the encryption parameters and security protocol before the transmission starts. And also, the key updates are managed by IKE. These are two main protocol basis of IPSec framework. These are Authentication Header Protocol and Encapsulated Security Protocol. These protocols provide 2 of the major parts, authentication and data integrity and confidentiality.

Authentication Header is an additional IP header added to IP packet. AH places between the IP header and Transport Layer Header. The AH format is shown figure.

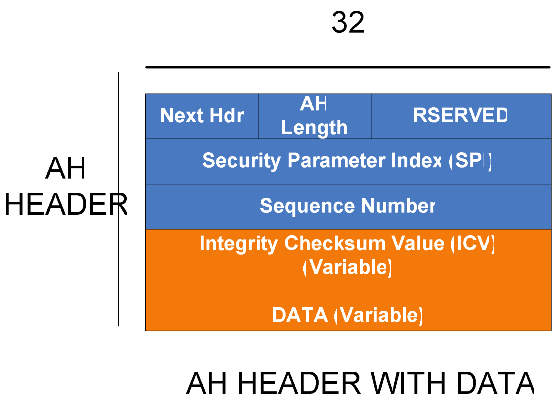

Figure 3-10: Authentication Header

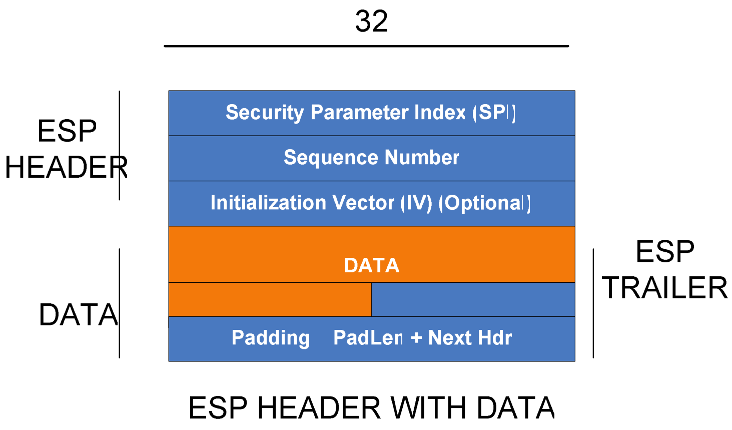

Figure 3-11: ESP Header

IPSec AH provides data integrity and replay protection for whole IP packet that is against IP-Spoofing and session hijacking attacks. Hashed Authentication Message Code (HMAC) is generated at the sender end and this hash code is generated based on the specified SA. Then HMAC value is added to the packet after IP header as a part of IPSec AH. At the receiver end, the HMAC is decoded and serves to establish the authenticity of the sender as well as the integrity of the message. AH uses the modified version of a hash function such as MD5 or SHA1. The IPSec authentication header provides no data encryption; clear-text messages can be sent, and the authentication header ensures that they originated from a specific user and were not modified in transit. [25] [8], [31]

The Encapsulating Security Payload (ESP) Protocol provides the data confidentiality, data integrity and replay protection. The main aim of IPSec ESP is sender authentication and data integrity during transmission in addition to confidentiality. To achieve this aim, IPSec ESP encrypts the content of the packet using advanced encryption algorithm specified on SA. It uses a symmetric key algorithm like 3DES, AES, IDEA. The authentication algorithms used in here are similar to IPSec AH uses. Unlike AH, ESP does not protect the entire packet protect only the payload. [25] [8], [31]

IPSec provides two different modes to exchange protected data across the different kinds of VPNs. AH and ESP can operate in both of modes.

- **Transport Mode:** This mode protects the upper-layer protocols and applications. This mode is applicable only for host-to-host security. Here protection extends to the payload of IP data. The IP addresses of the hosts must be public IP addresses.

IPSec Header is inserted between IP header and upper-layer header, transport layer header.

The Figure 3.13 show that the AH in transport mode.

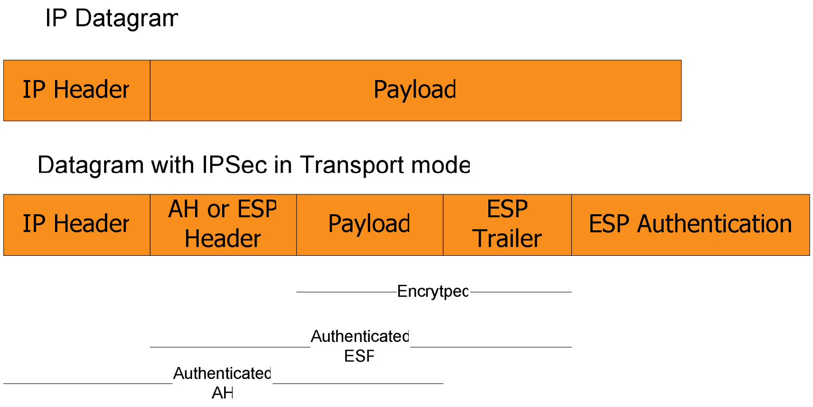

Figure 3-12 : IPSec Transport Mode

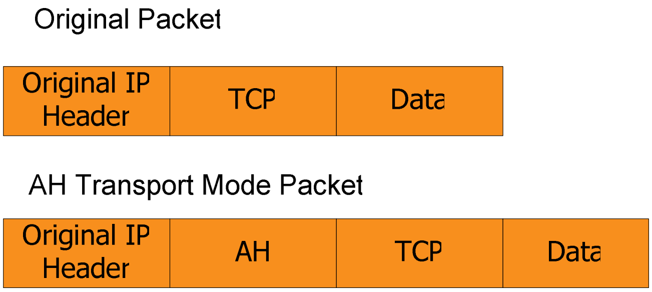

Figure 3 Error! No text of specified style in document.**-13: AH Transport Mode**

ESP header and trailer are inserted before the payload. The new header is inserted before the payload, ESP header, ESP trailer or ESP authentication data as shown in figure 3.14.

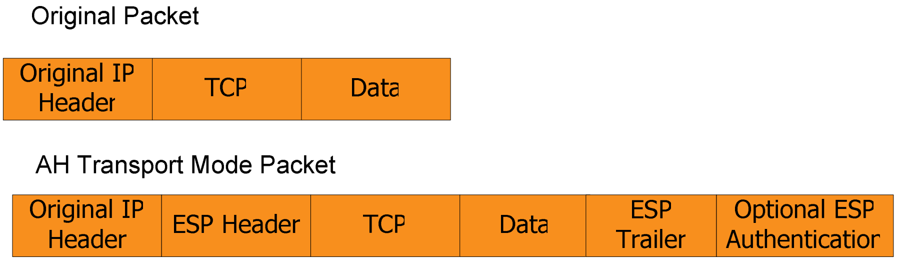

Figure 3-14: ESP Transport Mode

- **Tunnel Mode:** This mode is used to provide data security between two networks. It provides protection for the entire IP packet and is sent by adding an outer IP header corresponding to the two tunnel end-points. The unprotected packets generated by hosts travel through the protected "tunnel" created by the gateways on both ends. The outer IP header in Figure 3.15 corresponds to these gateways. Both intranet and extranet VPNs are enabled through this mode. Since tunnel mode hides the original IP header, it facilitates security of the networks with private IP address space.

  The IPSec header is inserted between the new IP header and original IP header.

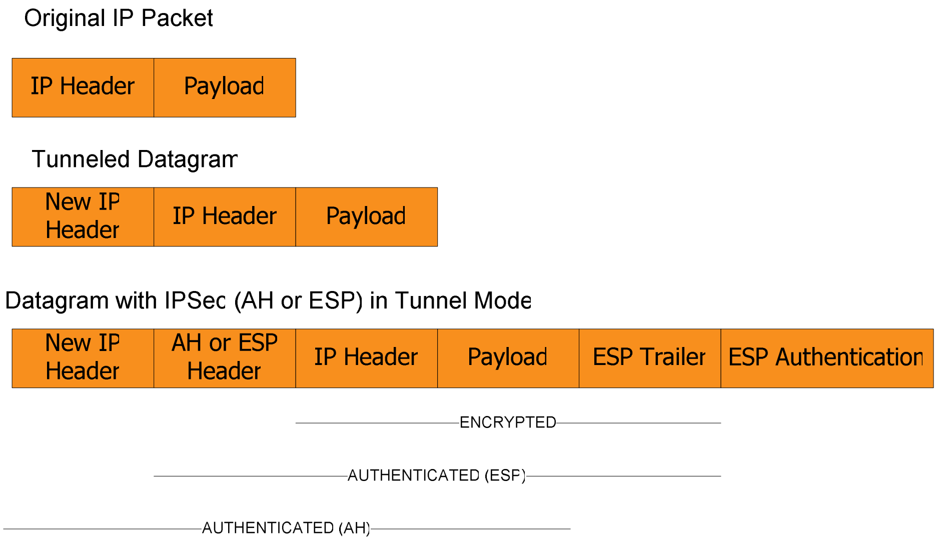

Figure 3-15: IPSec Tunnel Mode

The AH is inserted between the original and new IP header. The ESP is inserted at the original packet [25] [8], [31].

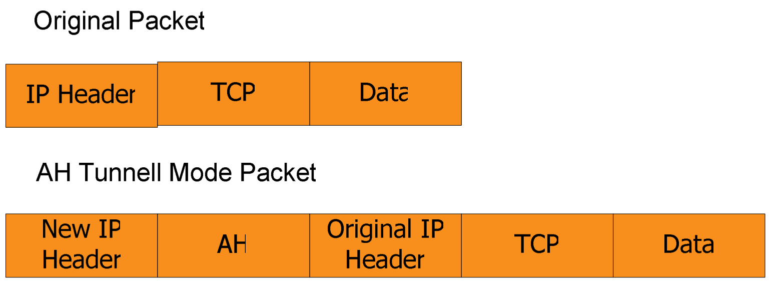

Figure 3-16: AH Tunnel Mode

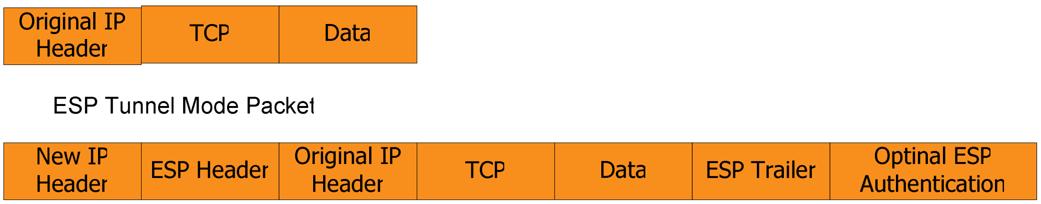

Figure 3-17: ESP Tunnel Mode

Header adding can be presented in figure simply:

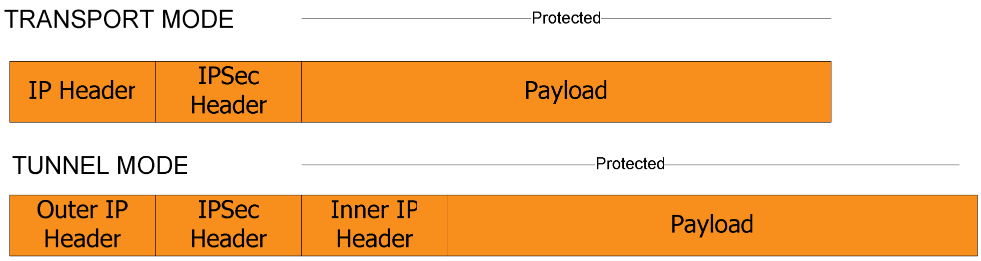

Figure 3-18: IPSec modes of operation – tunnel and transport

Internet Key Exchange has originally known as ISAKMP/ Oakley (Internet Security Association and Key Management Protocol). IKE defines a secure mechanism to negotiate parameters of SAs and authentication keys before a secure IPSec session is implemented. These parameters are security parameters and cryptographic keys. IKE may modify security parameters and keys during the transmission. And also, IKE is responsible for deleting these SAs and keys after an IPSec-based communication session is completed. The IPSec domain of interpretation (DOI) document defines all the security parameters .IKE performs as an UDP application and use port number 500. IKE has two main advantages. The first advantage is that IKE is independent of technology so the interoperability is widely defined. The second one is the negotiating SAs in few packet exchanges which allow managing large number of SA negotiating. IKE operates in two phases these are Authentication Phase and Key Exchange phase. These phases are consequent of each other and make up IKE-based session.

IKE Phase I is used to establish a secure channel before negotiating SAs starts. The authentication of communicating peers takes place in Phase I. After successful authentication, peers agree on the SA, that includes encryption algorithm, hash functions, authentication methods of exchanging encryption keys. If peers agree on SA then Shared Master Secret Key is generated. The peers exchange their public key and generate their secret keys by using shared master secret key. The peers exchange their secret keys without using over the network. Two main modes are available on IKE Phase I, main mode and aggressive mode. Both methods serve for the same purpose, but aggressive mode is faster than main mode while prone to denial-of-service (DoS) attacks.

In the main mode, six messages are exchanged between the communication peers. First two messages are used to negotiate the security policy. The next two messages are used to pass Diffie-Hellman keys and nonce which is a random value different from previous choices and inserted in a message to protect against replays. And the last two messages are used to authenticate the communication peers by means of signature, hashes. There are four methods of IKE standard to authenticate the peers.

- **Pre-Shared Keys (PSK):** The communicating peers use pre-shared keys to create hash values and nonce that will be used in authenticating messages.

- **Digital Signatures (RSA or DSS):** The hash values are calculated in term of certificate and send in the last two messages. There are many protocols and standards available now that ease the process of certificate enrollment, certificate request, and certificate status checking. Some popular ones are RSA Labs' PKCS #7, PKCS #10, Cisco's Simple Certificate Enrolment Protocol (SCEP), and Online Certificate Status Protocol (OCSP).

- **RSA Public Key Encryption**: In this method, there is no need to exchange the first two messages. Since peers have public keys of each other and private keys of themselves. Nonces exchanged are secured through this encryption with peer's public key.

- **Revised RSA Public Key Encryption:** This method is similar to the RSA Public Key Encryption method, only this method reduces the number of public key operations from four to two.

The following figure gives an idea for authentication of data payload.

In aggressive mode, three messages are exchanged instead of six messages. The first message is used to agree on security policy, required data for key calculation and signed nonce. The second message authenticates the peers and agreed on security policy. The last message is for authentication initiator.

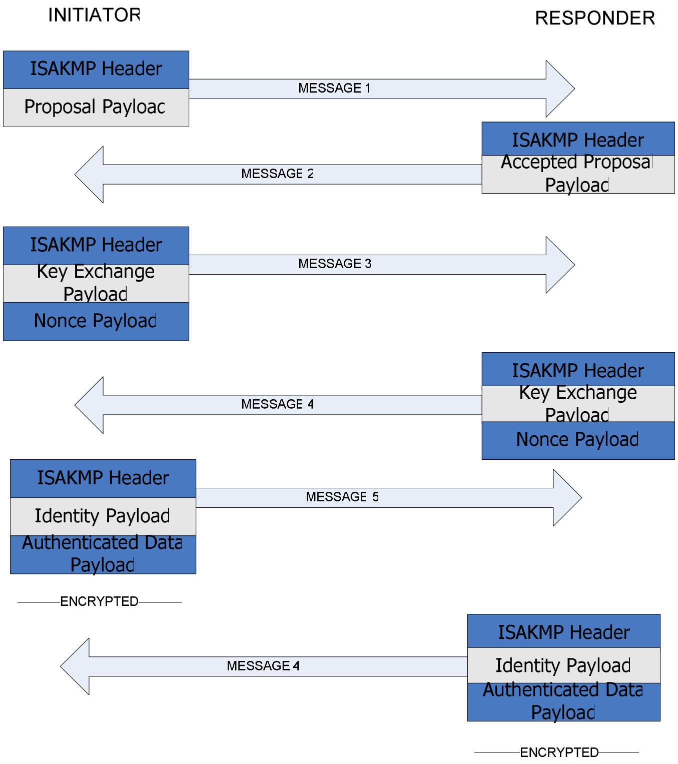

Figure 3-19: IKE Main mode message exchange

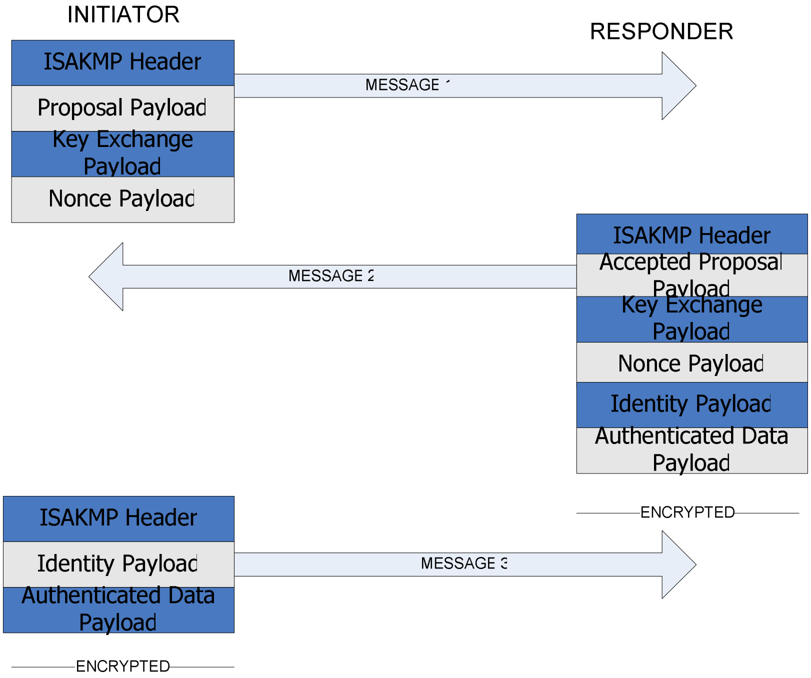

Figure 3-20: IKE Aggressive mode message exchange

IKE Phase II aims to establish the IPSec SA. Various parameters are negotiated in IPSec SA such as authentication mechanisms, hash functions, and encryption algorithms. Phase II occurs in certain period to prevent hackers attack and renew keys. If the policy of Perfect Forward Secrecy (PFS) is negotiated in the Phase I, a full Diffie Hellman key exchange is initiated. If not, new keys are generated using hash values. One IKE Phase I can be associated with many IKE Phase II. The basic Quick mode message exchanges are illustrated in below:

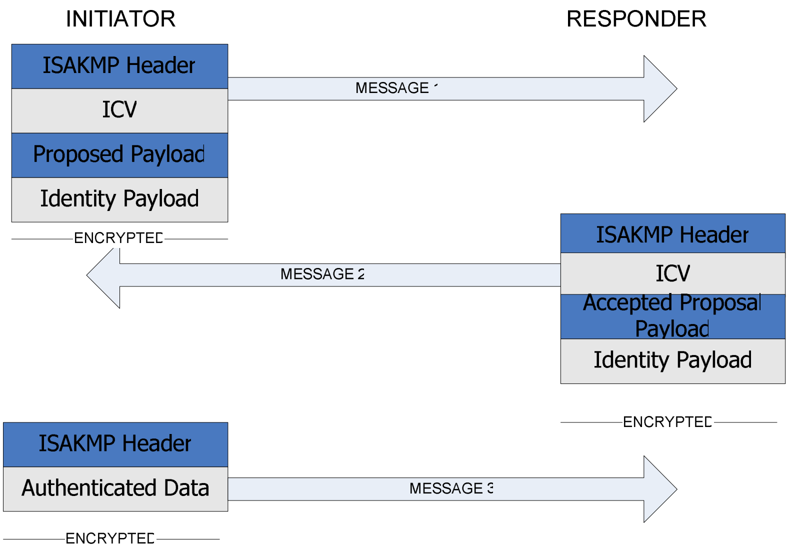

Figure 3-21: IKE Quick mode message exchange

The following two figures explain the whole structure of sending and receiving process of IPSec packets. [25], [8], [31]

IPSec gives a complete solution of protecting IP traffic. IPSec protects the traffic against eavesdropping, unauthorized modification in transit and provide secure authentication of communication peers. IPSec requires Public Key Infrastructure (PKI); however, there is no wide-scale PKI provider that is independent of operating system. IPSec makes it possible to connect offices, users, and partners to the corporate network securely and is a very cost-effective solution to exchange information. In addition, IPSec is completely transparent to the end users. As the networks migrate to Ipv6, IPSec will become an integral component of those networks as well.

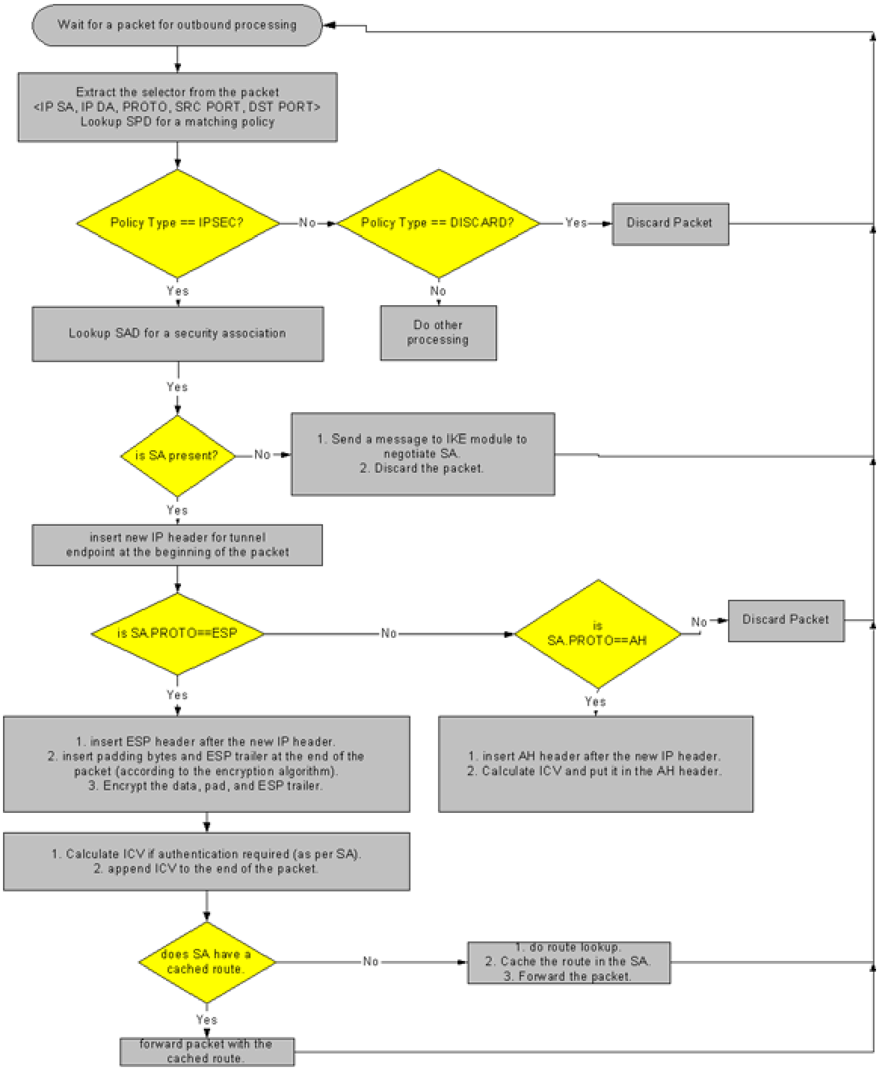
Wait for a packet for outbound processing
Extract the selector from the packet
<IP SA, IP DA, PROTO, SRC PORT, DST PORT>
Lookup SPD for a matching policy
Policy Type == IPSEC?
No
Policy Type == DISCARD?
Yes
Discard Packet
Yes
No
Lookup SAD for a security association
Do other processing
Yes
is SA present?
No
1. Send a message to IKE module to negotiate SA.
2. Discard the packet.
Yes
insert new IP header for tunnel endpoint at the beginning of the packet
is SA.PROTO==ESP
No
is SA.PROTO==AH
No
Discard Packet
Yes
Yes
1. insert ESP header after the new IP header.
2. insert padding bytes and ESP trailer at the end of the packet (according to the encryption algorithm).
3. Encrypt the data, pad, and ESP trailer.
1. insert AH header after the new IP header.
2. Calculate ICV and put it in the AH header.
1. Calculate ICV if authentication required (as per SA).
2. append ICV to the end of the packet.
does SA have a cached route.
No
1. do route lookup.
2. Cache the route in the SA.
3. Forward the packet.
Yes
forward packet with the cached route.

Figure 3-22: IPSec Packet Generation Process - Outbound

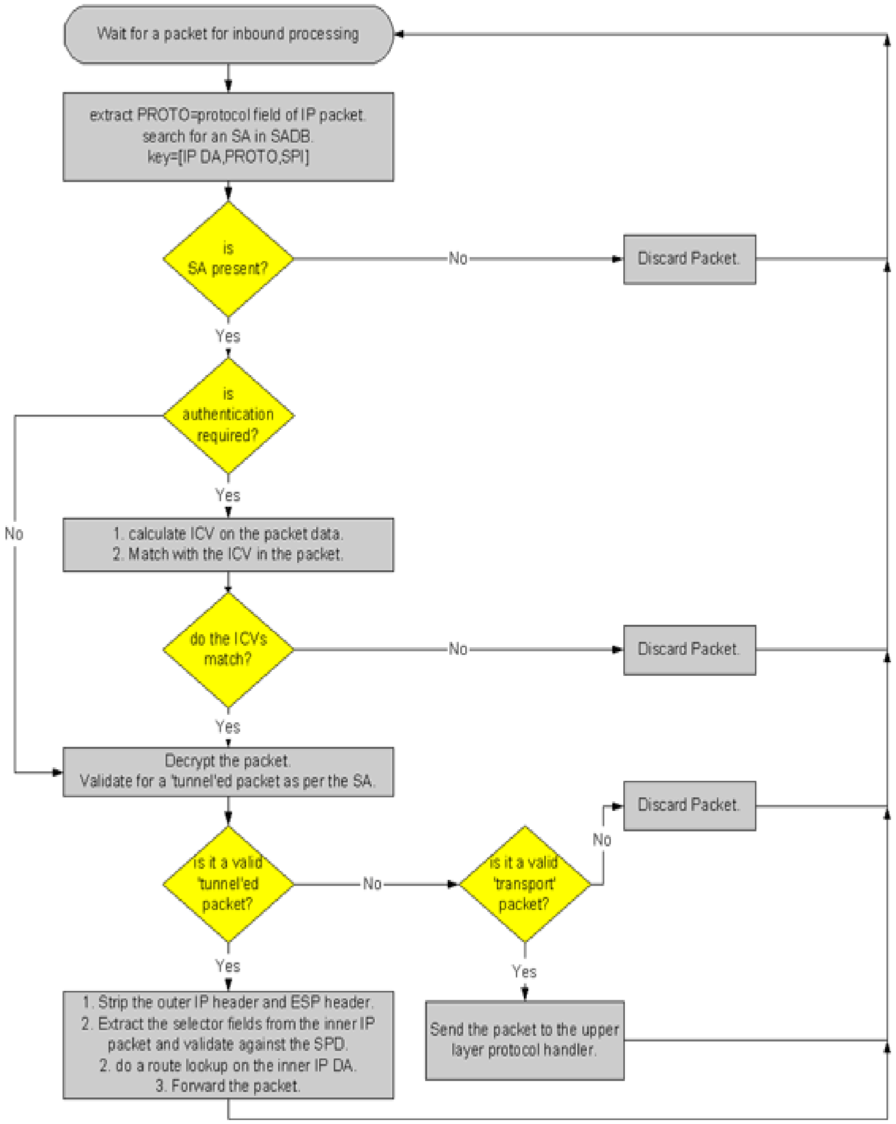
Wait for a packet for inbound processing
extract PROTO=protocol field of IP packet.
search for an SA in SADB.
key=[IP DA,PROTO,SPI]
is SA present?
No
Discard Packet.
Yes
is authentication required?
No
Yes
1. calculate ICV on the packet data.
2. Match with the ICV in the packet.
do the ICVs match?
No
Discard Packet.
Yes
Decrypt the packet.
Validate for a 'tunnel'ed packet as per the SA.
Discard Packet.
No
is it a valid 'tunnel'ed packet?
No
is it a valid 'transport' packet?
Yes
Yes
1. Strip the outer IP header and ESP header.
2. Extract the selector fields from the inner IP packet and validate against the SPD.
2. do a route lookup on the inner IP DA.
3. Forward the packet.
Send the packet to the upper layer protocol handler.

Figure 3-23: IPSec Packet Generation Process - Inbound

CHAPTER 4

WIRELESS VIRTUAL PRIVATE NETWORKS

We have so far defined Virtual Private Networks (VPN) and Wireless networks in detail. We shall attempt to combine the two technologies to provide end-to-end security for wireless system users [1]. The combination is referred to as Wireless Virtual Private Networks (WVPNs). The wireless security is a long investigated area and there are many known drawbacks [2]. Current recommendations for wireless deployments suggest the use of VPN for wireless client to provide both authentication and privacy [35]. Some universities like University of Illions at Springfield, University of Michigan, and University of British Columbia [32], [33], [34] have already started to implement VPN to secure their wireless data networks.

Remote access VPNs are dependent on the end users access methods. With the emergence of high speed data networks with 2G and 3G wireless technologies, we believe that the wireless VPN concept will also be evolving in those research areas [36].

As mentioned before, employing VPN in wireless networks affect parameters like throughput, round trip time and packet loss. These parameters are directly related to the quality of service (QoS) requirements of the network. These affects are investigated using the test bed described in the next section.

Before, we explain our test bed and experiments; the wireless medium behavior will be described briefly. Since the collisions are not detectable in the wireless medium, CSMA/CA MAC protocol is used to avoid and ACK frames are used by receiver node to acknowledge the receipt of the frame. If a node wants to send data then it senses the wireless medium. If it is busy or it wants to send another frame then it waits for medium to be idle for DIFS period. Then at the end of DIFS period, the node enters the contention period. Contention is done by choosing a random back-off time which is a random number chosen between 0 and Contention Window (CW). The random back-off time determines the number of slots to be waited. If the medium is sensed as idle at the end of the back-off time then data transmission is started. Before reaching the end of back-off time, if the medium becomes busy then the timer is frozen until the end of the data transmission. After the destination node successfully receives the packet, it transmits ACK frame following SIFS time. If ACK is not received in a certain time then the packet is retransmitted [49], [50]. If the packet size is larger than 1472 bytes, fragmentation may happen. Here the only difference is that the contention period is not repeated for each sequence of fragmented packets. The initial contention period is used and all sequence of fragmented packets is sent after this initial contention period. The throughput may be calculated using the parameters defined for 802.11g and the protocol overhead in the upper layers. These are summarized in the Table 1. IEEE 802.11g is defined SIFS as 10 µs [51] and the rest is defined as Table1. The IEEE 802.11g defines CWmin as 31 slots. Therefore, in the scenario of single station transmitting; the average random back-off time is 15.5 slot times.

Table 1 : 802.11g parameter specification

Parameter	802.11g (us)	Notes
T_{DIFS}	29 µs	SIFS + 2 * T_{SLOT}
T_{SLOT}	9 µs	
T_{BOFF}	139,5 µs	Back-off * T_{SLOT}
T_{POH}	9.19 µs	(IP 20 bytes, UDP 8 bytes, 34 bytes MAC)
T_{PHY}	24 µs	Preamble + PLCP

Table 2 : 802.11g parameter specification (contd.)

Parameter	802.11g (us)	Notes
T_{SIFS}	10 µs	
T_{ACK}	2.07 µs	Time to transmit 14 bytes at 54 Mbps date rate of 802.11g
T_{DATA}	(framesize * 8) / 54Mbps	Time to transmit data at 54 Mbps date rate of 802.11g

Time to transmit a packet is indicates as TP and

$$T_{P} = T_{DIFS} + T_{BOFF} + T_{POH} + T_{DATA} + T_{PHY} + T_{SIFS} + T_{ACK} + T_{PHY} \quad (1)$$

If fragmentation is evaluated then the overhead should also be included in the calculation. Throughput in our case is given by

$$\text{Throughput} = (\text{frame size}) / (\text{Transmit period}) \quad (2)$$

The calculated throughput is plotted in figure 4.1

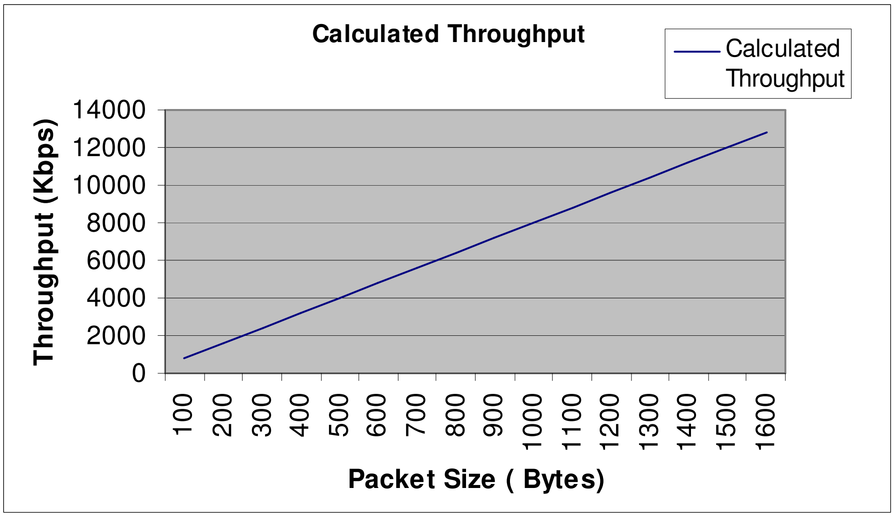

Figure 4-1 : Calculated throughput in order to IEEE 802.11g parameters vs. packet size

Single node throughput calculation can be obtained as the above time and wireless link data rate. All the packet transmission time is less than 1msec and also 5 msec which indicates that the one baseline connection and one IPSec connection have a constant traffic rate without any burst. If we increase the number of simultaneous connections to two then burst traffic is generated.

CHAPTER 5

EXPERIMENTAL SETUP

An experimental network is set up to measure the effects of using VPN in wireless Local Area Networks. The setup includes two computers one of them is a wireless client and the second one serves as a server. The wireless network connection between them is established through an access point. The Virtual Private Network connections are obtained by a trial version of commercial VPN products. Traffic is generated between the computers over wireless network using commercial software, which is also used to log events.

The server computer has Microsoft Windows 2000 Server operating system with the latest hot fixes and latest service packs, SP4. The minimal operating system is installed on the server and in order to do that, the unnecessary services and processes are stopped and unnecessary software, utilities and system tools are uninstalled. The server has Intel(R) Pentium (R) 4 Central Processor Unit (CPU) operating at 3.00 GHz and has 1 GB Random Access Memory (RAM). To connect the server to the network, Realtek RTL8139 (A)-Fast Ethernet Adapter is used. This network cards support 100 Mbps connection speeds. The network card is connected to the access points using 4 meters 100BaseT cable.

The wireless computer is a laptop computer and has Microsoft Windows XP Pro operating system with latest hot fixes and latest service packs, SP2. The minimal operating system is installed on the client computer and unnecessary services, programs and utilities are uninstalled or stopped in the same way as the server. The CPU of wireless client is Intel (R) Pentium (R) III 995 MHz processor and the wireless client has 248 MB RAM. To connect to the access point, the wireless client uses a wireless adapter. The wireless adapter is Linksys WPC54GS Wireless-G Notebook adapter with SpeedBooster. The wireless adapter operates on 802.11g wireless standard as described in the previous chapters.

The access point is a Dlink DSL-604G Wireless ADSL Router that provides 802.11g/802.11b wireless LAN connection. The access point has 4 100 Mbps Ethernet ports. The antenna transmit power is set to be maximum. Only 802.11g protocol is used on the wireless connections. The DSL port is unplugged and it has not been activated. The access point service is enabled and the channel number is set to be 6. No security mechanism such as WEP, WPA which are supported by Dlink Wireless access point is used. The access point's DHCP service is enabled and the only one IP address is assigned to the IP pool. This is done to prevent unauthorized access. The access point is placed 3-3.5 meters away from wireless client and 4 meters to the server.

The connection is shown in figure 5.1. To verify that the connections are active the ping utility is used.

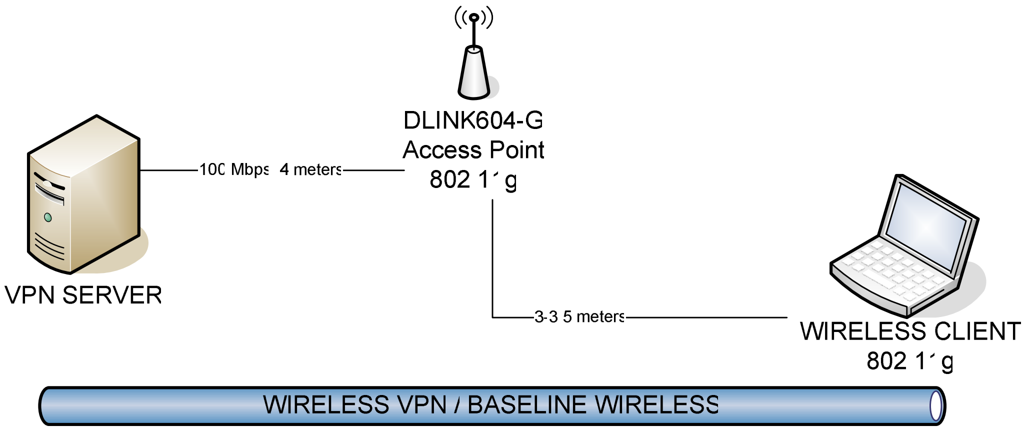

Figure 5-1: Lab Setup Design

The trial version of Check Point VPN-1 Pro NGX software is used to established VPN connections. The Check Point VPN-1 Pro NGX software is widely used around the world and it leads the VPN software market. This software is easy to install, configure and use. We used the basic functions of this software in our experiments. The Check Point VPN-1 Pro NGX software is installed on the server. The components of this software is

- Check Point CPinfo NG_AI_R55W
- Check Point R55 Compatibility Package
- Check Point R55W Compatibility Package
- Check Point Smart Console NGX R60
- Check Point VPN-1 Edge Compatibility Package
- Check Point VPN-1 Pro NGX R60

The component of software suite helps us to configure VPN parameters, VPN connections and users. The software suite has firewall utility, but to obtain pure VPN connection performance, this utility is disabled. This way we could reduce the firewall processing delay. Only one policy is defined on the server and the encryption algorithm chosen is 3 DES with MD5 algorithm for authentication. There is also an option to use SHA1 algorithm for authentication; according to [2] SHA1 or MD5 does not affect the network load or transaction numbers. And also, SHA1 has %9 increase in transfer time compared to MD5. [40]

The Check Point Secure Remote is used on the client side. This enables us to create VPN tunnel between a remote user and the server. This VPN tunnel guarantees authentication, integrity and privacy. The client software components are as follows:

- Check Point Smart Console NG_AI_R55
- Check Point Smart Console NGX R60
- Check Point VPN-1 SecuRemote NG_AI_R56

To allow a user to reach and access the server resources, a VPN connection is established between the user computer and server. To establish VPN connection, the initially, an IKE (Internet Key Exchange) negotiation takes place between the peers. During IKE negotiation, the peers' identities are authenticated. The Gateway verifies the user's identity and the client verifies that of the Gateway. The authentication can be performed using several methods, including digital certificates issued by the Internal Certificate Authority (ICA). It is also possible to authenticate using third-party PKI solutions, pre-shared secrets or third party authentication methods (for example, SecurID, RADIUS etc.). Our experiment verifies the client with username and password. This username and password is set on the policy. After the IKE negotiation ends successfully, a secure connection (a VPN connection) is established between the client and the server. All connections between the client and the server are encrypted inside this VPN connection, using the IPSec standard.

Once, the baseline wireless connections and IPSec connections are ready to use, the traffic generator software is installed on both client and server. The LAN Traffic v2 software is used for this purpose. It is a COTS and the trial version is used in the experiment. The trial version is downloadable from [47]. The software is traffic generator software of IP Networks including LAN, MAN, WAN, WLAN, Cellular, Satellite and so on. Since the software supports only Windows 2000, the server's operating system is chosen to be Windows 2000 Server. Data flows can be set to TCP or UDP with the program options. TCP is connection oriented protocol and triggers the congestion recovery algorithm. And the TCP is designed for low loss rate connections. However, the wireless links have high bit error rates, hence total performance of connection is significantly decreased when TCP is used [41] [42]. In contrast, UDP is lightweight transport protocol. The TCP has 20 bytes protocol header [43] [44] while the UDP has 8 bytes protocol header [45], [46] The LAN Traffic v2 has two components, sender and receiver. Both parties should have LAN Traffic v2 software and the connections should be defined as TCP or UDP with user-defined ports. The software allows user to change the inter frame time between the packets in the experiments we used two inter frame times, 1 msec and 5 msec. The traffic generator program also allows users to connect multiple simultaneous connections between the peers. At most three simultaneous connections are established during the experiments. The sender software is configured according to experiment parameters and the same configuration is made on the receiver side. The receiver (server) receives the packet and sends it back to the sender; the server echoes the traffic back.

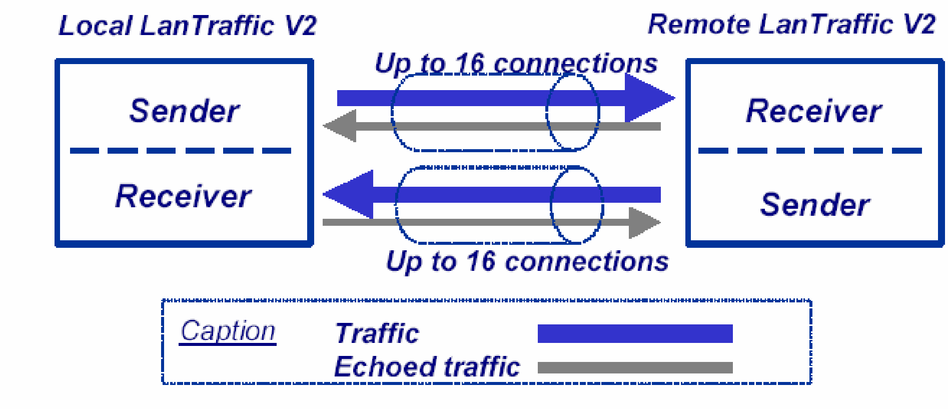

Figure 5-2: LAN Traffic v2 Connection Setup

LAN Traffic v2 software has an interface to choose the properties, but since our experiment used only one interface on the client and the server, no configuration was necessary on the client or server. The logging capability records down the transmitted and received throughput, packet loss, Round Trip Time, Packet Number sent and received volume of packet sent and received. The logging is enabled during all the experiments on both client and server sides. Throughput is measured as the average amount of data payload transferred from the server to the wireless client in unit time [48]

LAN traffic v2 has property that the packet size can be modified and during the tests packet size is modified between 25-1600 bytes at the each level, 10000 packets are sent for each trial. Tests are repeated 5 times and the average value is taken.

The following table summarizes all the tests in the experiment.

Table 3 : List of Tests

No	Test Explanation	Inter frame time
1)	One baseline connection is established and 25-1600 byte packets are sent 10000 packets sent for each case	1 msec
2)	Two baseline connections are established and 25-1600 byte packets are sent in every level 10000 packets sent for each case	1 msec
3)	Three baseline connections are established and25-1600 byte packets are sent in every level 10000 packets sent for each case	1 msec
4)	One IPSec connection is established and 25-1600 byte packets are sent in every level 10000 packets sent for each case	1 msec
5)	Two IPSec connections are established and 25-1600 byte packets are sent in every level 10000 packet sent for each case	1 msec
6)	Three IPSec connections are established and 25-1600 byte packets are sent in every level 10000 packets sent for each case	1 msec
7)	One baseline connection is established and 25-1600 byte packets are sent in every level 10000 packets sent for each case	5 msec
8)	Two baseline connections are established and 25-1600 byte packets are sent in every level 10000 packets sent for each case	5 msec
9)	Three baseline connections are established and25-1600 byte packets are sent in every level 10000 packets sent for each case	5 msec

Table 4 : List of Tests (contd.)

No	Test Explanation	Inter frame time
10)	One IPSec connection is established and 25-1600 byte packets are sent in every level 10000 packets sent for each case	5 msec
11)	Two IPSec connections are established and 25-1600 byte packets are sent in every level 10000 packets sent for each case	5 msec
12)	Three IPSec connections are established and 25-1600 byte packets are sent in every level 10000 packets sent for each case	5 msec

The throughput sampling is done every 2 msec and UDP timeout value is set to 700 msec. The receiver and sender buffer sizes are set to 25000 bytes separately. In the following sections, the test results are discussed.

The results of the experiments are compared to those records in [37]. The client and server CPU's were different in those experiments but the tests were planned in the same way. The other difference is that the 802.11b is replaced with 802.11g.

CHAPTER 6

RESULTS

The results of the experiments will be presented in this section. Experiments described in the preceding section are performed and the results of throughput, round trip time and packet loss is analyzed.

6.1 Throughput

Throughput is measured as the average amount of data payload transferred from the wireless client to server in unit time [48]. The client logs are analyzed and the results give us the expected transmitted throughput. The server logs` analyses shows that the actual throughput that is received from client. Packet size is taken as a parameter to analyze throughput.

6.1.1 Throughput with 1 msec Inter frame time

The result of tests where inter frame time between the packets is 1 msec is analyzed and reported. The results are grouped as baseline where IPSec is not used, and for number of UDP connections taken as 1, 2 and 3. The same experiments are repeated using IPSec and results are also grouped and presented together. Finally, all results are displayed on the same graph for ease of comparison.

One baseline connection (BASE1UDP) is setup and the LAN Traffic v2 is setup to send 10000 packets using UDP protocol with the packet size of 25 bytes and the packet size increased to 1600 bytes in linear intervals. The test is repeated 5 times and the logs are analyzed. The same approach is repeated for two and three baseline connections [(BASE2UDP), (BASE3UDP)].

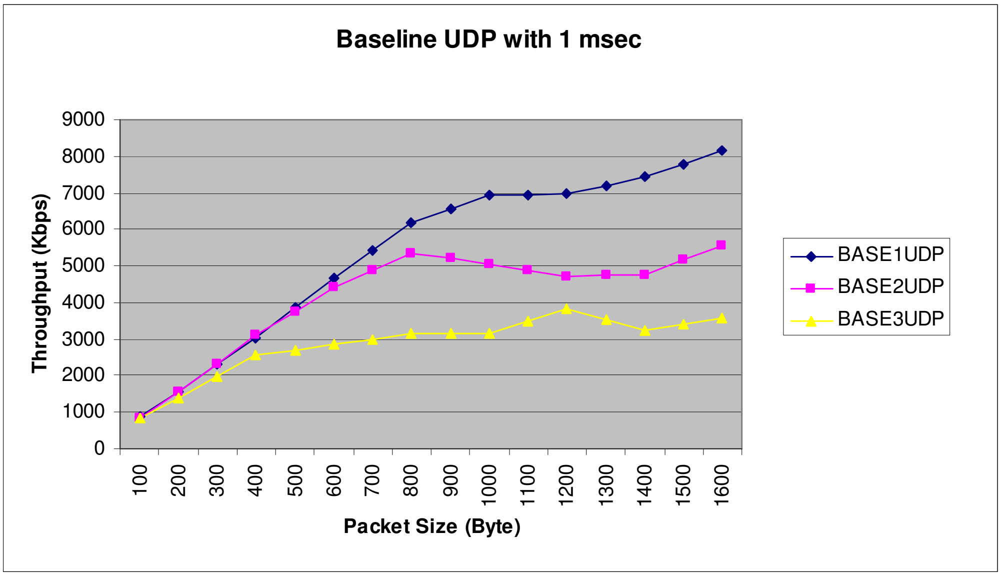

Figure 6-1: Throughput of Baseline Connections with 1 msec inter frame time

Figure 6.1 shows the baseline connection results. The maximum throughput is 8 Mbps which is achieved by one baseline connection (BASE1UDP) for 1600 byte packets sizes. BASE2UDP is very close to BASE1UDP series up to 600 bytes packet size. BASE1UDP series has advantage for all packet sizes.

After 800 bytes packets, generation of two packets with in 1 msec inter frame time may take longer than this period. BASE3UDP series has big difference compared to BASE1UDP and BASE2UDP as the result of sending 3 packets in the given unit time which is not possible, hence the packets wait for the contention period with some queuing delay. The fragmentation has no affect on transmitted throughput on the client side since the packets did not experience transmission. If the server side throughput is considered, as the figure 6.2 shows, BASE2UDP connection has achieved the maximum throughput as 7 Mbps. BASE2UDP is very close to BASE2UDP while BASE3UDP has significant differences between them. This decrease is because of the number of packets accessing the medium.

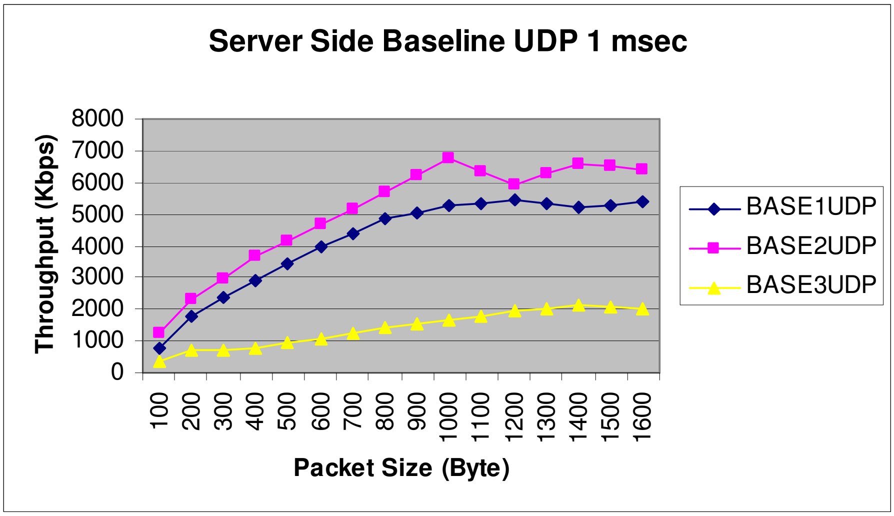

Figure 6-2: Server Side Throughput of Baseline Connections with 1 msec inter frame time

Then the same experiments are repeated using IPSec protocol. First, IPSec connection is established and it was checked with ping utility. LAN Traffic v2 is configured for only one UDP connection (IPSEC1UDP) and 10000 packets are generated starting with 25 bytes packet size and the packet size is increased up to 1600 bytes. Each test is repeated 5 times. The same method is applied to two and three simultaneous IPSec connections. The results are analyzed and plotted in figure 6.3 is:

The maximum throughput is achieved for 1500 byte packet sizes for one IPSec connection (IPSEC1UDP); the value of maximum throughput is 8.2 Mbps. IPSEC2UDP and IPSEC3UDP are very close to each other and the IPSEC1UDP results up to 1500 byte packets. The encryption time is added to the packet generation time which causes less packets to be delivered to the queue and the system does not experience contention as baseline connections have. The server side results which give the actual throughput received after passing through the wireless link is plotted in Figure 6.4.

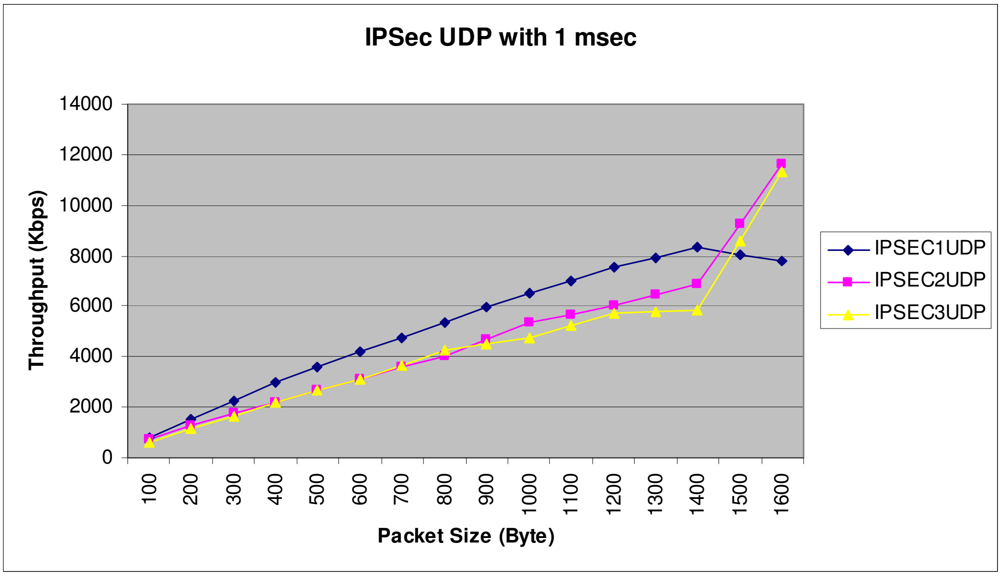

Figure 6-3: Throughput of IPSEC Connections with 1 msec inter frame time

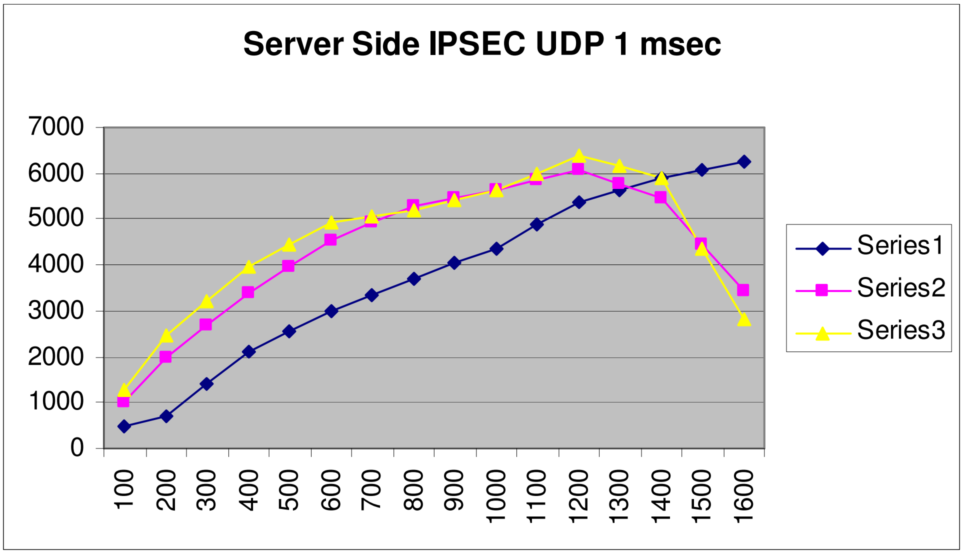

Figure 6-4: Server Side Throughput of IPSEC Connections with 1 msec inter frame time

IPSEC2UDP and IPSEC3UDP connections have very close results and the peak point of IPSEC3UDP and IPSEC2UDP is experienced for 1200 byte packet size as 6.53 Mbps. IPSEC1UDP series has less value up to 1500 byte packet sizes and has an advantage after 1500 byte packet sizes. IPSEC2UDP and IPSEC3UDP have experienced the contention period and some queuing delay during the transmission. This delay would be before the 1200 byte packet unless the encryption time is included in the packet generation time. The total throughput results are merged into one chart as shown in Figure 6.5 for the client side and in Figure 6.6 for the server side. The drop in throughput for the server side for packet greater than approximately 1500 bytes may be due to the fragmentation in the Ethernet connection between the AP and the server.

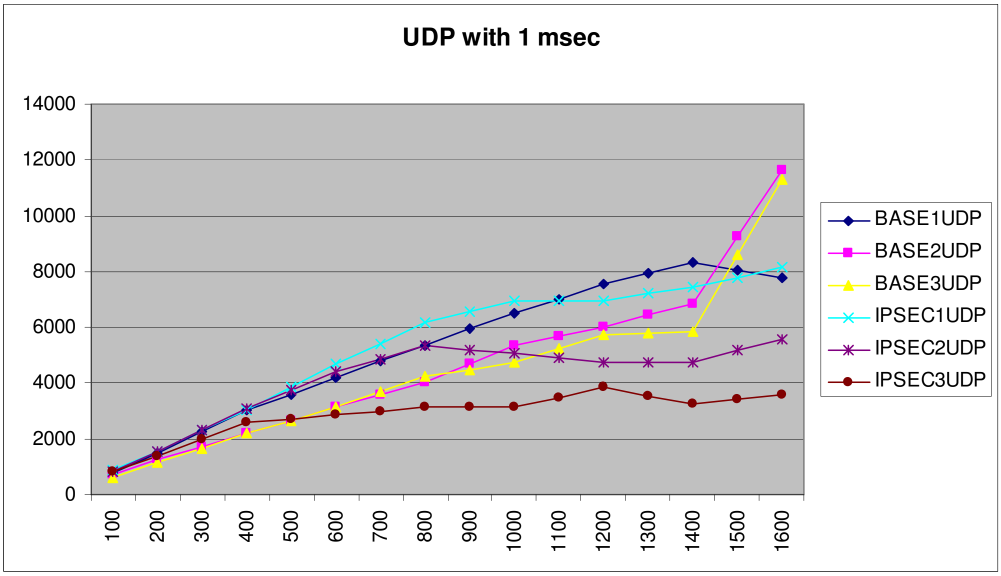

Figure 6-5: Throughput of All Connections with 1 msec inter frame time

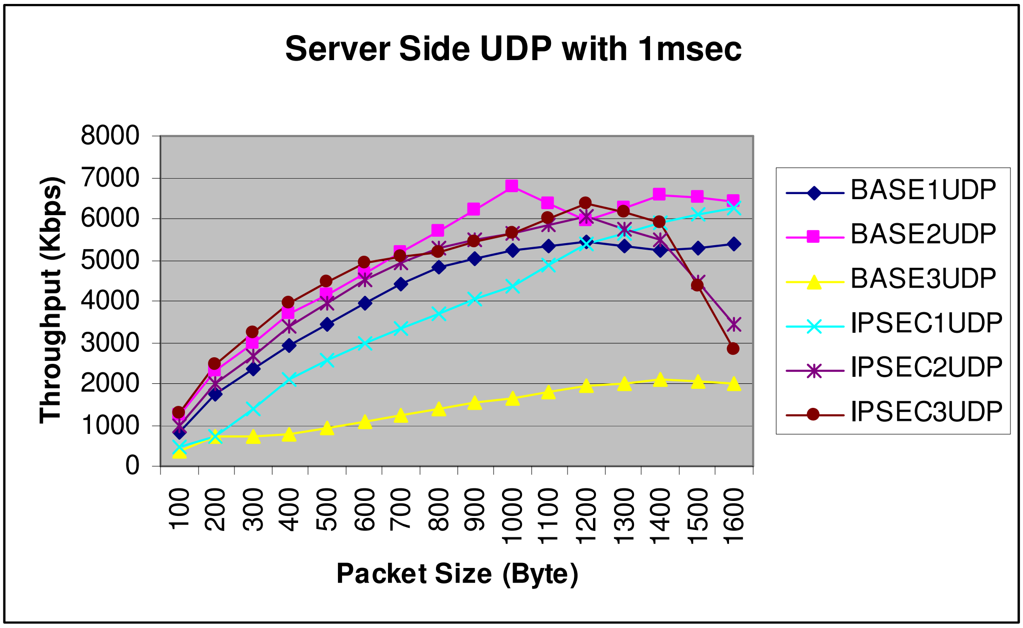

Figure 6-6: Server Side Throughput of All Connections with 1 msec inter frame time

6.1.2 Throughput with 5 msec Inter gap

Same tests are repeated using an inter frame time of 5 msec between the packets. The results are displayed in figures 6.7, 6.8, 6.9, 6.10, 6.11 and 6.12 respectively.

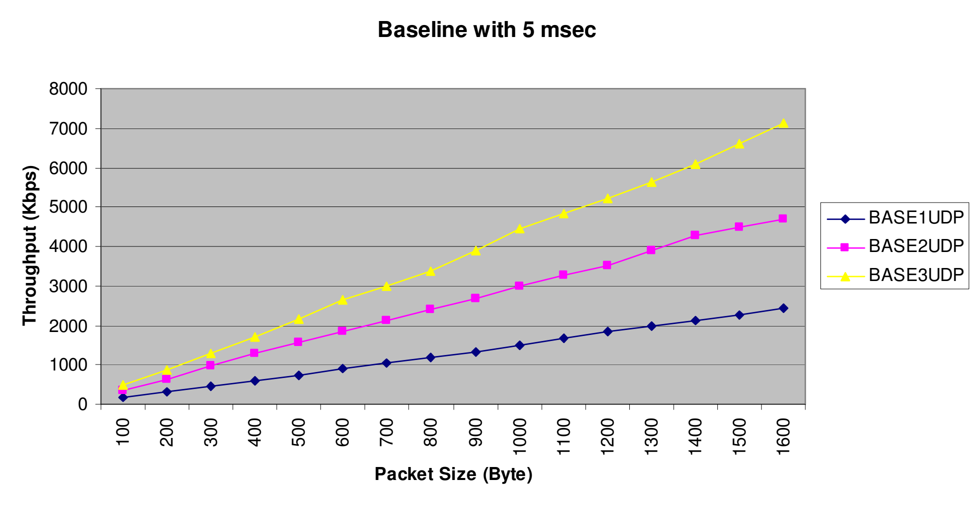

Figure 6-7: Throughput of Baseline Connections with 5msec inter frame time

The maximum throughput is achieved by BASE3UDP as 7 Mbps. BASE3UDP is almost three times that of BASE1UDP, and BASE2UDP is two times that of BASE1UDP. This result shows that the inter frame time is large enough to handle three simultaneous connections since no drop is experienced in simultaneous connections and also achieve higher throughput is achieved. The server side actual throughput values are presented in the Figure 6.8.

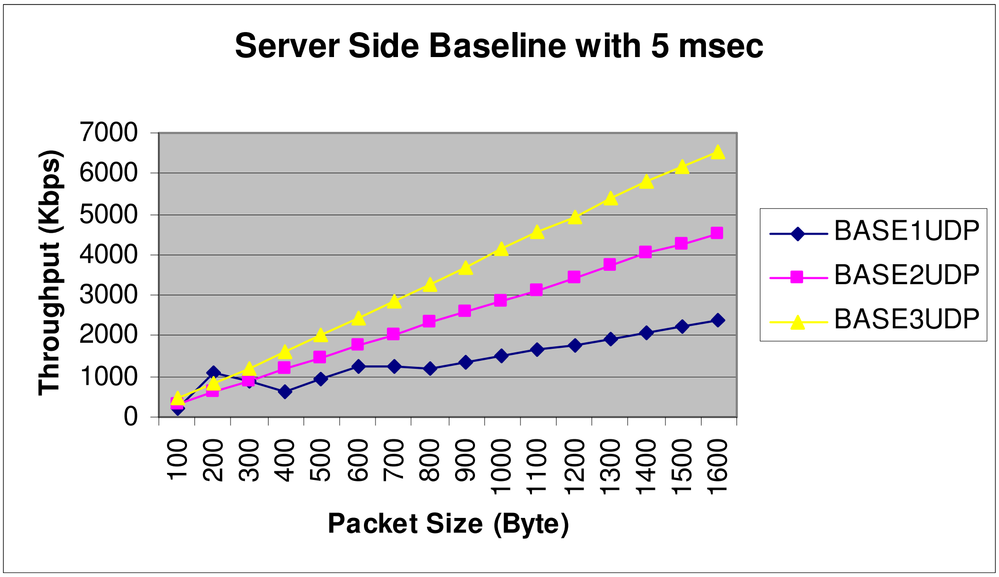

Figure 6-8: Server Side Throughput of Baseline Connections with 5msec inter frame time

Figure 6.7 and Figure 6.8 shows that the transmitted throughput is almost equal to the received throughput so if the inter frame time is large enough then the both sides have the same throughput results.

Same test are done for IPSec connections and Figure 6.9 and Figure 6.10 shows these results. As Figure 6.9 points, the maximum throughput, 6 Mbps, is achieved for IPSEC3UDP and the second highest value is obtained for

IPSEC2UDP. IPSEC1UDP reaches 2 Mbps at most. Here, results emphasize on the importance of the chosen inter frame time.

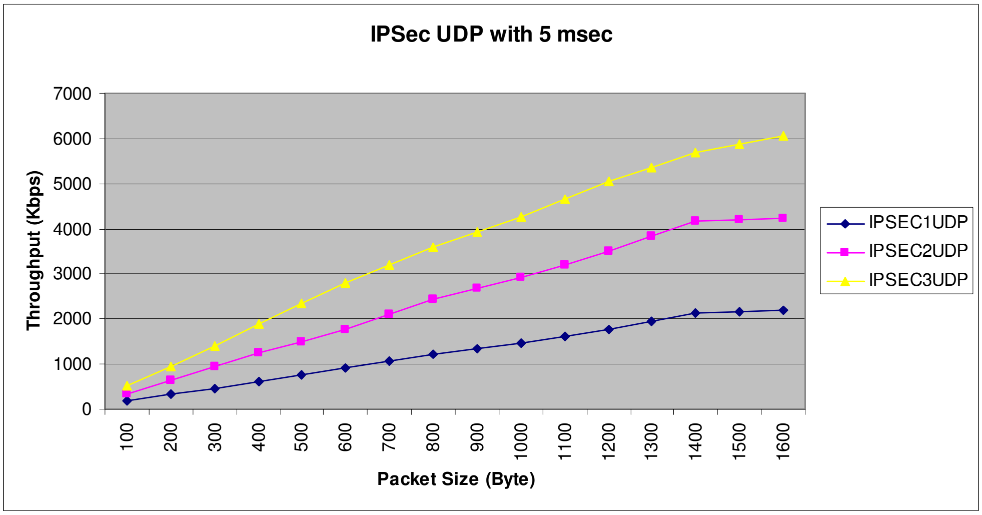

Figure 6-9: Throughput of IPSEC connections with 5msec inter frame time

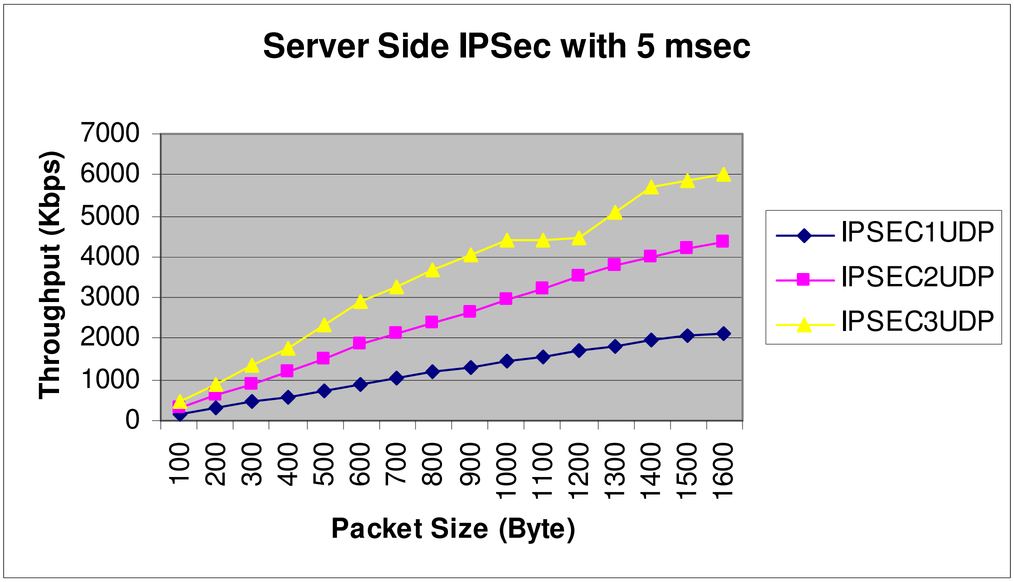

Figure 6-10: Server Side Throughput of IPSEC connections with 5msec inter frame time

All results are merged into one graph for ease of comparison in figures 6.11 and 6.12.

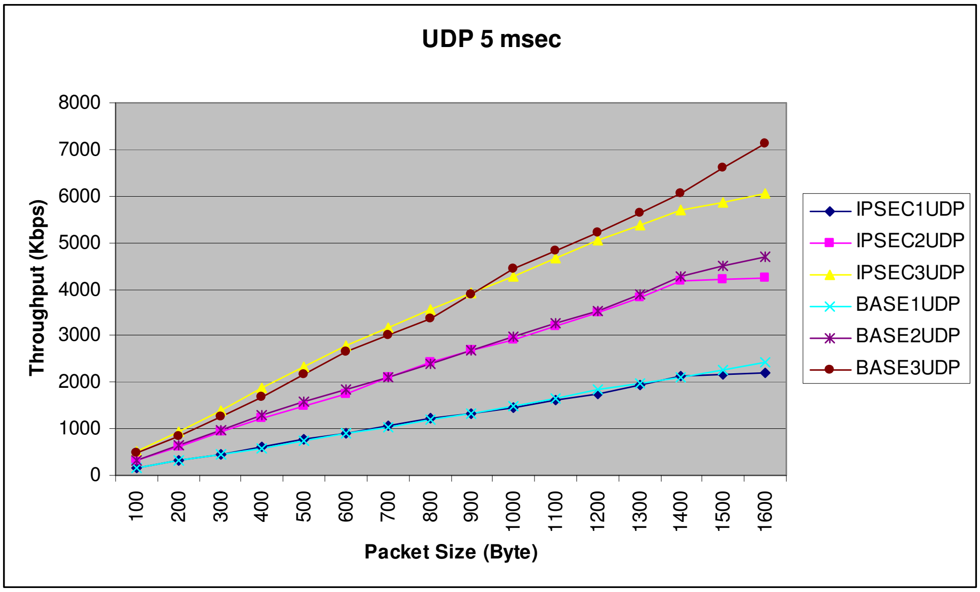

Figure 6-11: Throughput of All Connections with 5msec Inter frame time

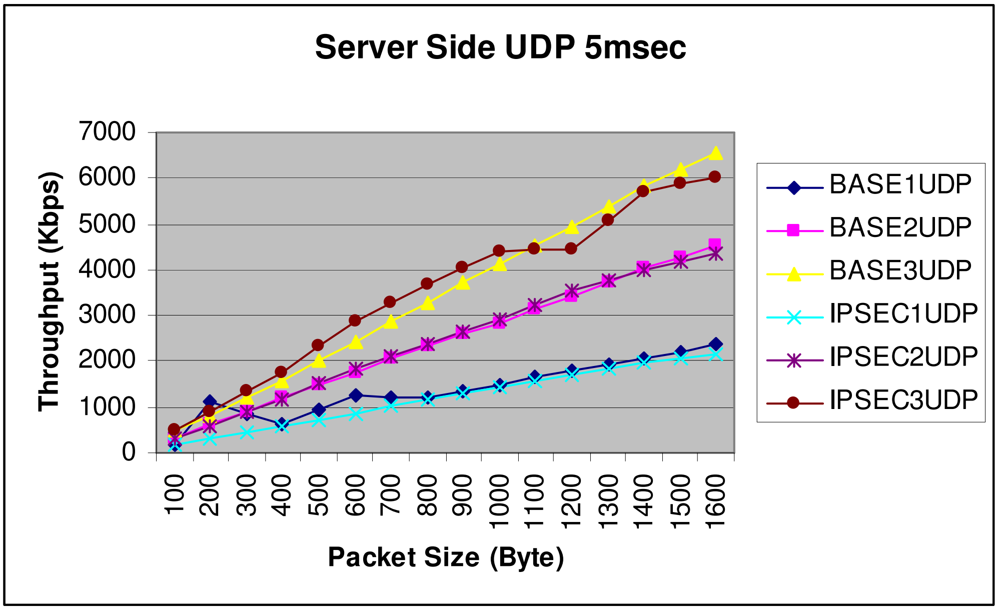

Figure 6-12: Server Side Throughput of All Connections with 5msec Inter frame time

To sum up, the inter frame time between the packets is a major concern of the wireless UDP and VPN connections. The IPSec connections are more sensitive if the small inter frame time is used. The baseline connections are affected more by fragmentation and delays due to contention for the medium compared to IPSec connections irrespective of the inter frame time. Since the generation time of an IPSec packet takes longer than a baseline packet, IPSec packets do not enter contention period and queuing delay as a result of contention period. The simultaneous connections are also affected by the inter frame time. More simultaneous connections can be used with larger inter frame times, however, and the performance is significantly decreased when smaller inter frame time is used. Here, 5 msec inter frame time can be declared as long and the smaller periods may be studied further.

6.2 Round Trip Time

Round Trip Time is measured as the time to travel from the client to the server and back for the packets

6.2.1 RTT with 1 msec Inter gap

The result of tests where inter frame time between the packets is 1 msec is analyzed and reported in figure 6.8, 6.9 and 6.10. The results for baseline transmission and for the case where IPSec is used are reported separately. The results are also merged into one graph to allow one to compare them. The tests are done as described in sections 6.1.1 and 6.1.2. RTT is measured for each connection.

The baseline connections' results are illustrated in figure 6.8
BASE3UDP experiences higher RTT values than BASE1UDP and BASE2UDP. BASE2UDP is almost two times BASE1UDP. But BASE3UDP is much more than three times of the BASE1UDP results. The packet generation rate is the reason of these higher values. Since 3 simultaneous connections are established the packet generation rate for each connection is more than inter frame time between the packets. This overloaded wireless link causes contention time and delays due to the back-off period which one

connection and two simultaneous connections do not have. After 1500 byte packets, the fragmentation is introduced and the sudden drop experienced is due to the variation in the queue lengths as a result of fragmentation and increase in the contention periods.

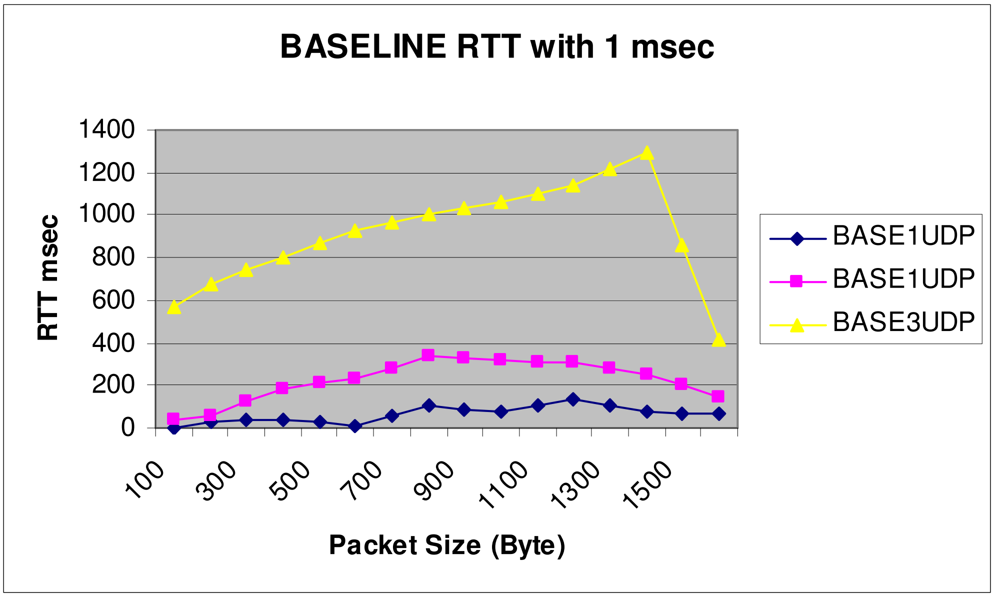

Figure 6-13: RTT of Baseline Connections with 1 msec Inter frame time Connections with 1 msec Inter frame time

The IPSec connections' results are illustrated in figure 6.14.

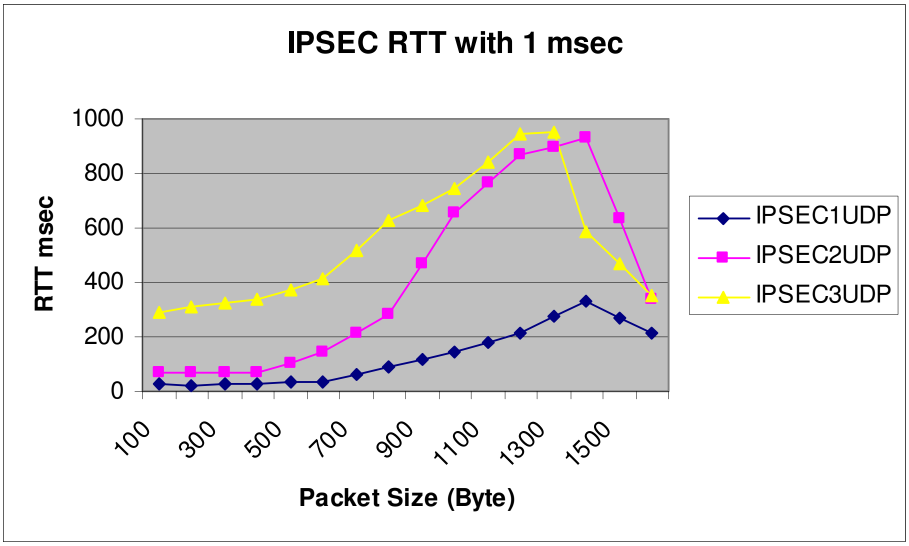

Figure 6-14: RTT of IPSec Connections with 1 msec Inter frame time

The maximum RTT is experienced with IPSEC3UDP, for reasons explained above. And also, packet generation time is more than pure packet generation time since encryption is involved. IPSEC2UDP and IPSEC1UDP have an increasing difference in higher packet sizes. After 1500 byte packets, the fragmentation is introduced and the sudden drop experienced is due to the variation in the queue lengths as a result of fragmentation and similar reasons as mention for the baseline results.

The total RTT results are merged in Figure 6.15:

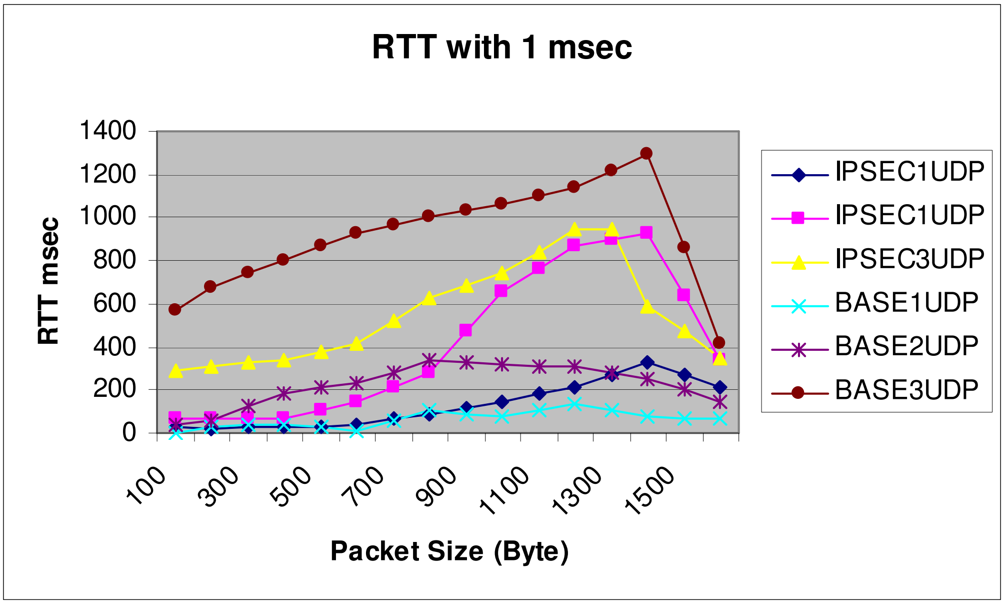

Figure 6-15: RTT of All Connections with 1 msec Inter frame time

The IPSec performs better than baseline with respect to RTT values. This is because the generation of an IPSec packet takes longer than a baseline packet. It seems to be contradiction but since the packet generation is longer, there are fewer packets waiting in the queue which also implies that there are fewer packets entering the contention period.

6.2.2 RTT with 5 msec Inter gap

The results of tests where inter frame time between the packets is set to 5 msec is also analyzed and reported. The results are analyzed as before and presented in Figure in 6.16, 6.17 and 6.18.

The results for baseline connections are illustrated in Figure 6.16

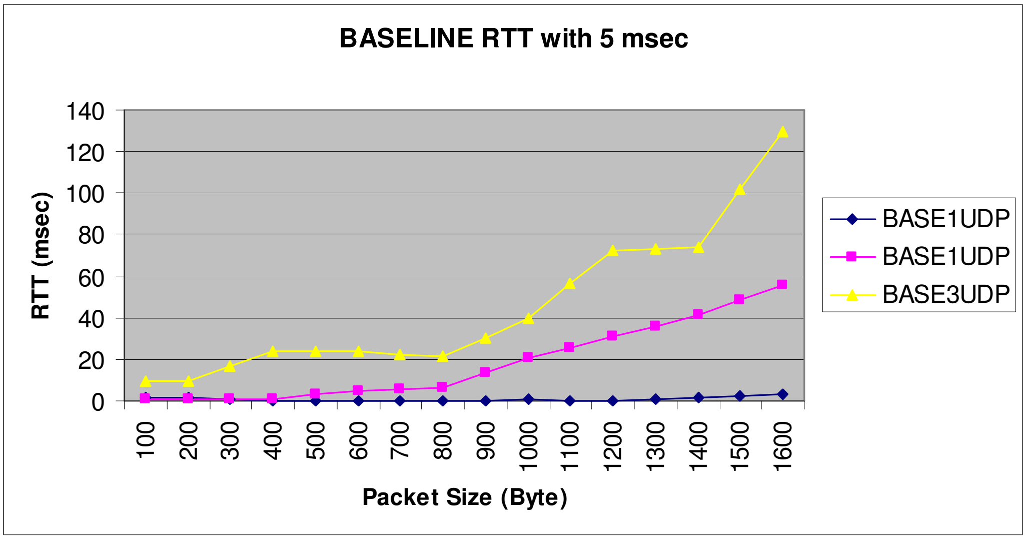

Figure 6-16: RTT of Baseline Connections with 5 msec Inter frame time

The tests show that BASE2UDP is almost two times that of BASE1UDP up to 800 bytes packet sizes. But RTT for BASE3UDP is much higher than three times the BASE1UDP results. The packet generation time is less than the inter frame time between the packets in smaller packet sizes. The packet generation rate delay is not significant in smaller packet sizes. After 800 byte packet size, BASE2UDP starts to cause an increase in packet generation times and larger packet processing delays in various part of the transmission. The fragmentation did not affect the queuing delay since the packet generation rate is high enough to tolerate queuing delays in BASE2UDP and BASE1UDP. But BASE3UDP experiences sudden increase with fragmentation since when the number of packets is increased, packet start to wait for contention time and have some queuing delays during the transmission.

The results of IPSec connections are illustrated in Figure 6.17

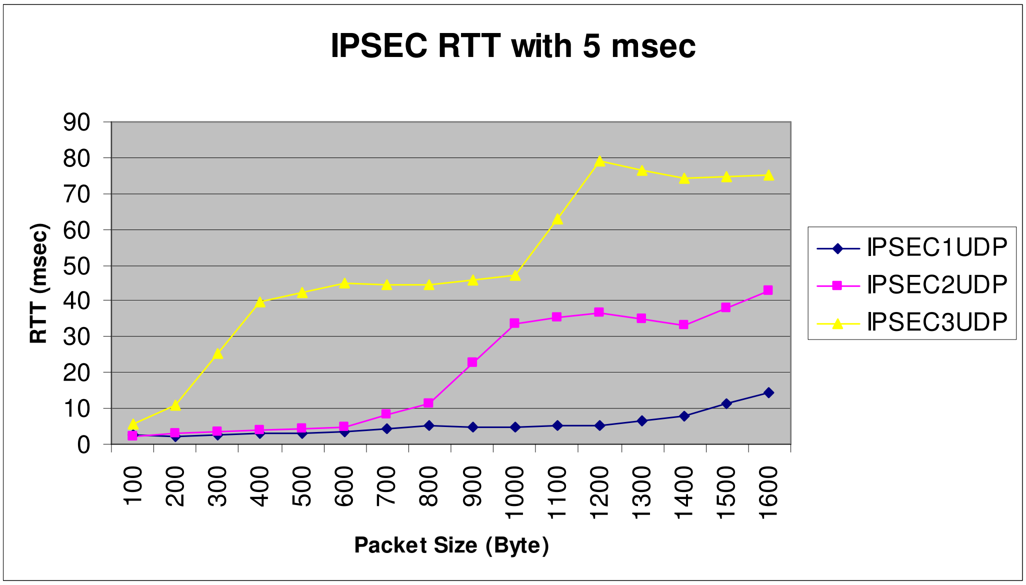

Figure 6-17: RTT of IPSec Connections with 5 msec Inter frame time

Both baseline and IPSec results are merged into one graph for the purpose of comparison and shown in 6.18.

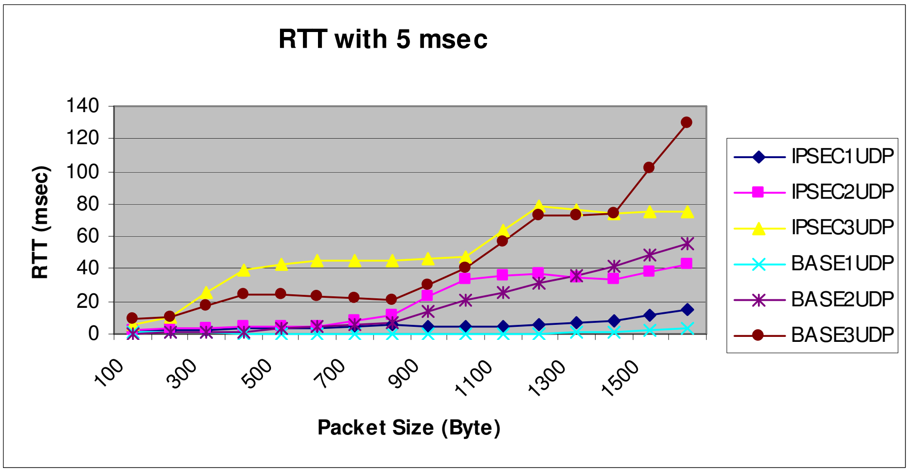

Figure 6-18: RTT of All Connections with 5 msec Inter frame time

6.3 Packet Loss

Packet loss is also measured and presented for the cases where baseline and IPSec VPN's are used.

6.3.1 Packet Loss with 1 msec Inter gap time

The tests are done as described in section 6.1.1 and 6.1.2. The packet loss value is obtained from the wireless client logs and it is measured for each connection. The packets are generated in the wireless client who sends them to the server through AP then the server echoes the received packets back to wireless client again trough the AP. The packet generation software is configured such that if a packet does not arrive in 700 msec it is considered as lost.

The results of the baseline connections' are illustrated in the figure 6.19

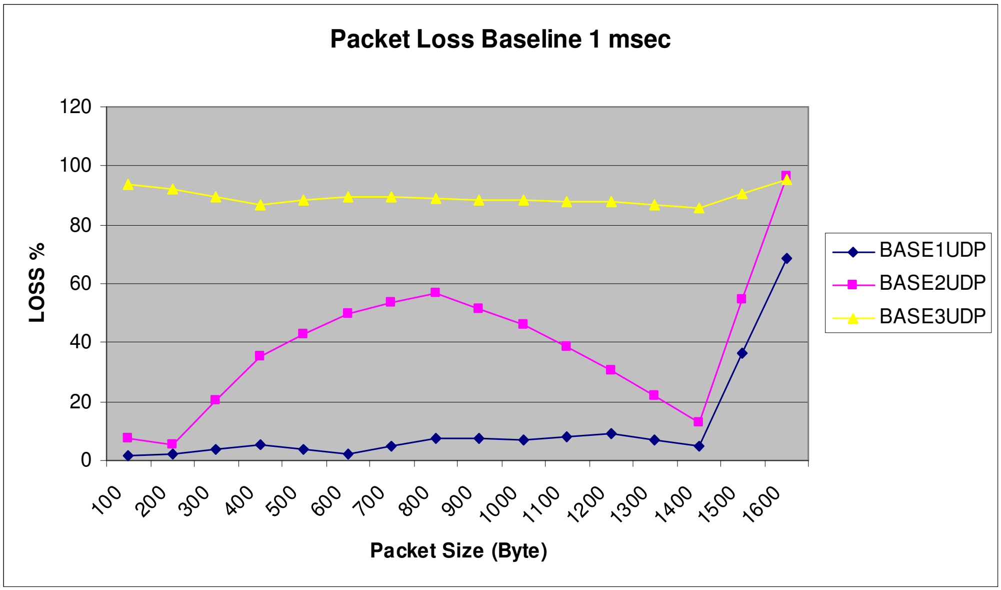

Figure 6-19: Packet Loss of Baseline Connections with 1 msec Inter frame time

BASE3UDP has experienced around %90 loss during the transmission whatever the packet size is. Since 3 simultaneous connections are established and the inter frame time between the packets is very small, packets spend longer than 700 msec in the system. BASE2UDP has very small loss values in the smaller packet sizes, and the loss increases as the packet size is increased up to 800 bytes. The loss is started to decrease although the packet sizes are still increasing up to 1400 bytes. This is the result of using small inter frame time between the packets. As the packet size is increased the packet generation rate is also larger than the inter frame time between the packets. The loss due to factors such as queuing delay, buffer overload are not experienced hence packet loss drops. BASE1UDP has very small loss values when using small inter frame time. All connections have a sudden increase when fragmentation starts to take place.

The IPSec connections' results are illustrated in the figure 6.20

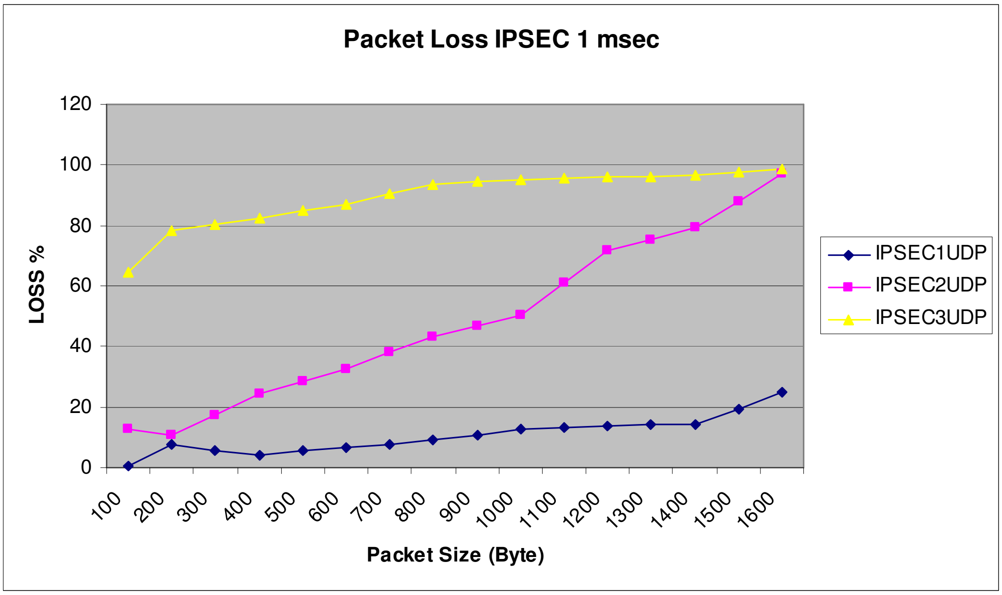

Figure 6-20: Packet Loss of IPSec Connections with 1 msec Inter frame time

When IPSec is used IPSEC3UDP has very high loss values, especially for packets larger than 800 bytes. The packet generation takes longer with the larger packet sizes hence the loss is not experienced. This is because when 3 simultaneous connections are established packet generation is composed of both encryption and generation. IPSEC2UDP has an increasing loss trend; if RTT values of IPSEC2UDP are considered in section 6.2.1 then the loss timeout threshold is reached and exceeded with 1000 byte packets. IPSEC1UDP has reasonable values until fragmentation occurs.

The total loss results with 1 msec are merged Figure 6.21.

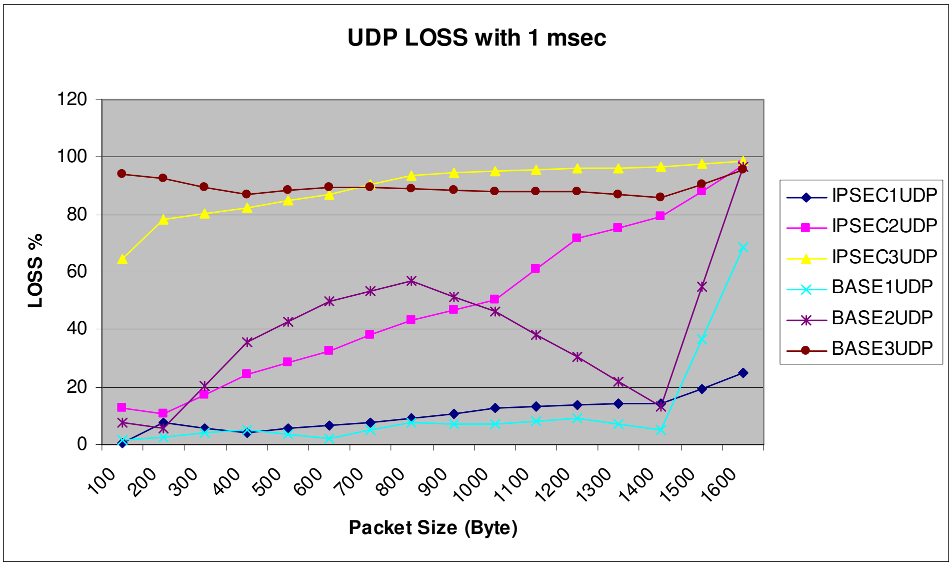

Figure 6-21: Packet Loss of All Connections with 1 msec Inter frame time

6.3.2 Packet Loss with 5 msec Inter gap

The result of tests where inter frame time between the packets is 5 msec is also analyzed and reported. The results are shown is Figures 6.22, 6.23 and 6.24.

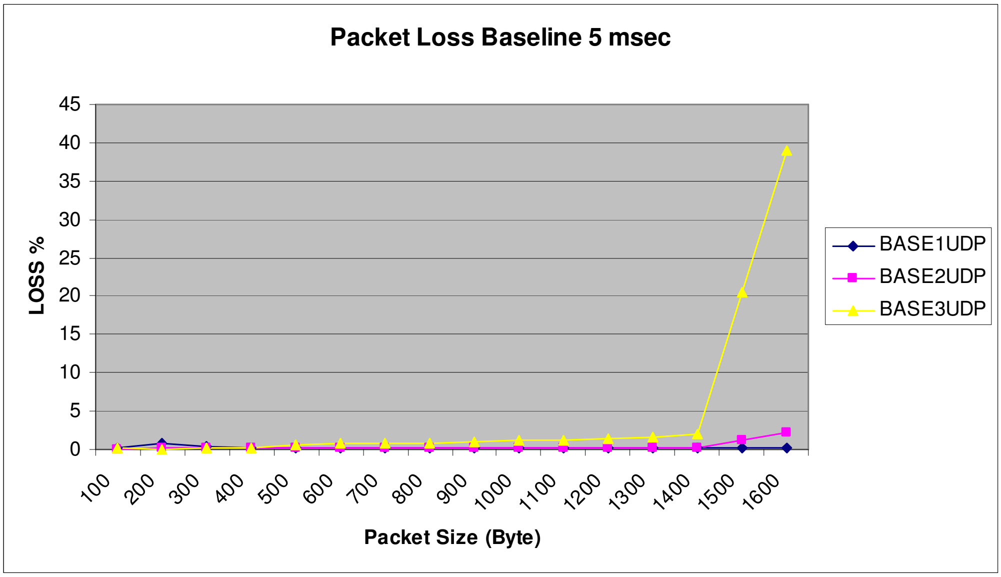

Figure 6-22: Packet Loss of Baseline Connections with 5 msec Inter frame time

BASE1UDP, BASE2UDP and BASE3UDP has very small loss values since the inter frame time between the packet plays a very important role in baseline connections. The sudden increased takes place after the fragmentation and congestion occurs the effects of these are felt in BASE3UDP connection significantly.

The IPSec connections' results are illustrated in following the figure 6.23.

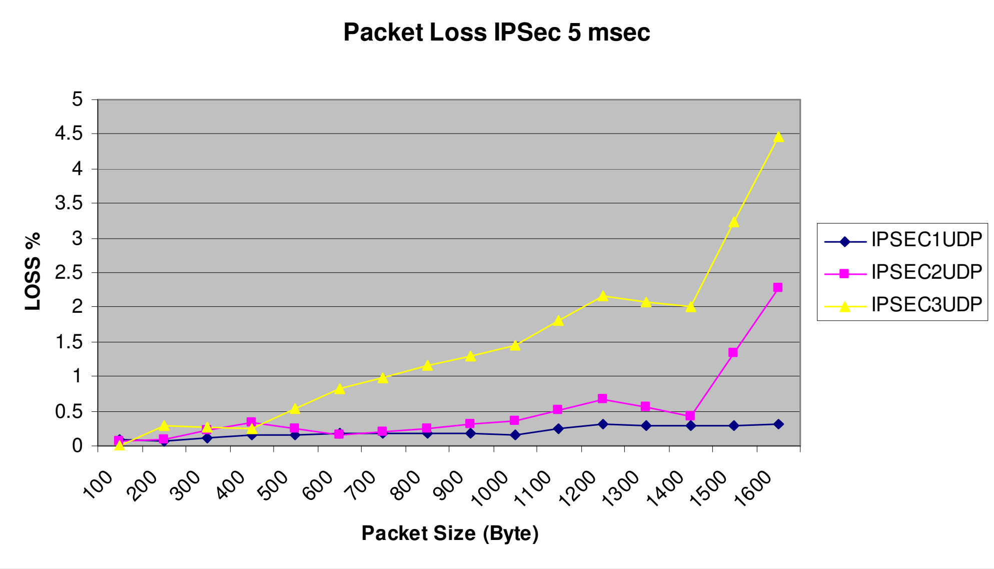

Figure 6-23: Packet Loss of IPSec Connections with 5 msec Inter frame time

The result are below %1 for most of the time and for IPSEC3UDP has increased to %5 with the increasing packet size and the sudden increase is experienced with the packet sizes of 1500 and more which is due to fragmentation and congestion.

The total IPSEC loss results are merged in Figure 6.24.

As mentioned before we have earned out our experiment using 802.11g wireless network. We compare our results with 802.11b experiments as described in [37]. We can clearly see the some differences between the

802.11b and 802.11g. The latter tests were earned out using only 1 baseline connection hence we compare them with our results accordingly.

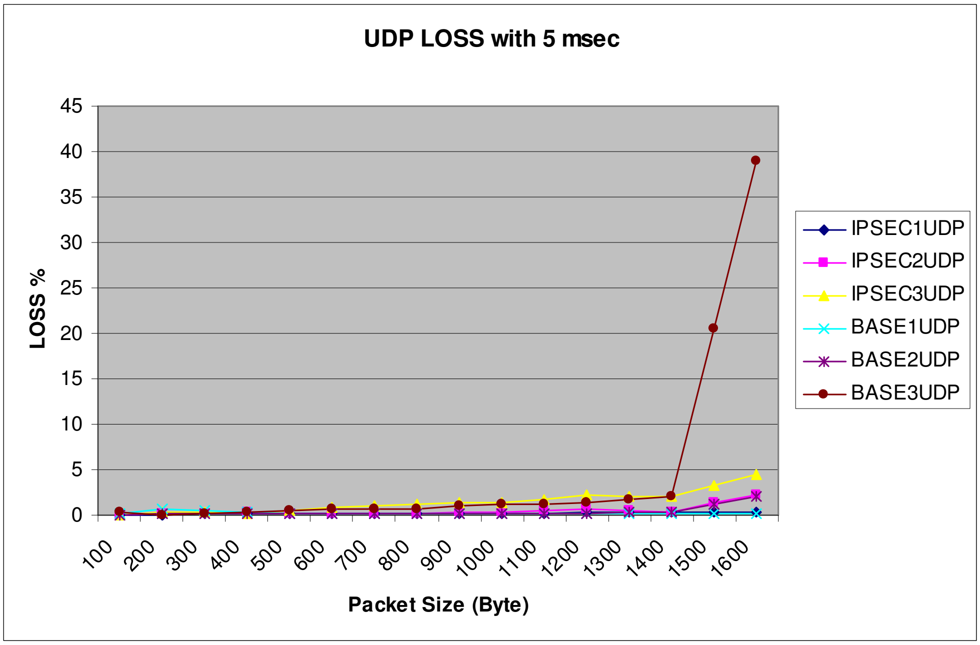

Figure 6-24: Packet Loss of All Connections with 5 msec Inter frame time

The maximum achieved throughput for 1 msec inter frame time is compared in Table 2. The baseline connection and all IPSec connections of 802.11g have higher throughput compared to 802.11b. As the number of simultaneous connection increase compared to the differences between throughputs of 802.11b and 802.11g becomes significant.

Table 5 : Throughput of 1 msec inter frame time for 802.11b and 802.11g

Throughput	802.11b	802.11g
BASE1UDP	6 Mbps	8 Mbps
IPSEC1UDP	5 Mbps	8 Mbps
IPSEC2UDP	3.8 Mbps	7 Mbps
IPSEC3UDP	3.7 Mbps	6 Mbps

The results of 5 msec inter frame time are displayed in Table 3. 802.11b used scenarios give higher results in one connection while the achieved throughput of 802.11g increase with the number of simultaneous connections and which IPSec is implemented.

Table 6 : Throughput of 5 msec inter frame time for 802.11b and 802.11g

Throughput	802.11b	802.11g
BASE1UDP	4 Mbps	2.5 Mbps
IPSEC1UDP	2.4 Mbps	2.3 Mbps
IPSEC2UDP	4.8 Mbps	4.3 Mbps
IPSEC3UDP	4.4 Mbps	6 Mbps

The experienced maximum packet loss of 802.11b and 802.11g are compared in Table 5 and Table 6. The inter frame time is taken as 1 msec in Table 5 where 5 msec is taken in Table 6.

The smaller packet loss is obtained for 802.11g of only one baseline connection and IPSec connection. While the number of simultaneous connection is increased the packet loss of 802.11g and 802.11b also increased.

Table 7 : Packet Loss of 1 msec inter frame time for 802.11b and 802.11g

Packet Loss	802.11b	802.11g
BASE1UDP	15 %	5 %
IPSEC1UDP	45 %	20 %
IPSEC2UDP	70 %	80 %
IPSEC3UDP	70 %	90 %

If 5 msec is used as the inter frame time then 802.11g generates significantly different values than 802.11b as displayed in Table 6.

Table 8 : Packet Loss of 5 msec inter frame time for 802.11b and 802.11g

Packet Loss	802.11b	802.11g
BASE1UDP	1.7 %	1.5 %
IPSEC1UDP	1.8 %	0.4 %
IPSEC2UDP	2 %	0.5 %
IPSEC3UDP	30 %	2 %

The maximum round trip time is the last parameters that are compared for 802.11b and 802.11g. The results are shown in Table 7 and Table 8.

802.11g of RTT results are very close to 802.11b in the one baseline and one IPSec connections are used. 802.11g displays significantly high values for more than one simultaneous connection.

Table 9 : RTT of 1 msec inter frame time for 802.11b and 802.11g

RTT	802.11b	802.11g
BASE1UDP	150	100
IPSEC1UDP	200	220
IPSEC2UDP	250	850
IPSEC3UDP	320	850

The results of 802.11g gives lower values when 5 msec is used as inter frame time. Only 3 simultaneous connections give close results in 802.11b and 802.11g.

Table 10 : RTT of 5 msec inter frame time for 802.11b and 802.11g

RTT	802.11b	802.11g
BASE1UDP	18	3
IPSEC1UDP	20	11
IPSEC2UDP	25	40
IPSEC3UDP	75	80

CHAPTER 7

CONCLUSIONS AND FUTURE WORK

In this study experiments were performed and their results are analyzed for the evaluation of the performance metrics when virtual private network are used over IEEE 802.11g wireless networks. The analysis points that the throughput, delay and packet loss parameters in WVPN depend on packet size as well as the packet generation rate. And also the numbers of simultaneous connections reduce the service quality level. If inter frame time is assigned a small value such as 1 msec then maximum throughput achieved is around 8 Mbps in baseline as well as for connections when IPSec is used. Using more than two simultaneous connections decreases the achieved throughput while using two and three simultaneous connections produce same values as one connection when IPSec is implemented. For all the results a reduction in throughput value is observed with 1 msec inter frame time is used. The effects such as delay at the AP and behavior of wired sink should be considered as well as fragmentation and congestion account for this drop. If the inter frame time is increased to 5 msec then the throughput value displays increasing results. The maximum value is obtained when using simultaneous connections in both baseline and IPSec. Multiple simultaneous connections give higher values compared to implementation of only one baseline or IPSec connection.

The fragmentation and congestion do not affect the throughput value much when 5 msec inter frame time is used. While 8.2 Mbps throughput is obtained when using 1 msec inter frame time, using 5 msec inter frame produces about 6 Mbps maximum throughput for 1600 packet sizes.

The delay limitations show that 3 simultaneous connections have always highest delay values in baseline and IPSec connections. Since the 3 simultaneous connections represent burst traffic longer contention windows should be added. And if the two simultaneous connections are considered then if IPSec is used in the connections, a sudden increase in delay is observed after 800 byte packet sizes. The delay value is reduced for 5 msec inter frame times compared to 1 msec. The maximum experienced delay with 1 msec inter frame time is almost 10 times the delay values when 5 msec inter frame time is used. Similarly, 3 simultaneous connections have higher delay as mentioned above. We can suggest that if simultaneous connections should be used then the inter frame times should be chosen large enough to tolerate multiple connections.

The experiments show that the packet loss is an effected by the parameters such as the inter frame time and the number of simultaneous connections. The simultaneous connections are prone to packet loss as the results illustrated. It is strongly recommended that only one connection should be preferred if loss sensitive applications are implemented using baseline or IPSec connections with 1 msec inter frame times. The baseline connections have smaller loss values than IPSec connections. If the inter frame time is increased to 5 msec than both connections have small loss values below %5 on average.

In summary we an say that the study shows that the inter frame time between the packets and number of simultaneous VPN connection and packet sizes are important parameters effecting throughput, packet loss and packet delays in wireless VPN networks.

Comparison of results with the experiments performed using an 802.11b network in [37] indicates that results are comparable. However, to be able to compare the results and deduce conclusions from them we believe we have to perform the experiments using the same test bed with the same software but an 802.11b network. It is hard for us to explain some results displayed in the tables such as achieved RTT of 802.11g vs. 80211b.

Detailed studies with smaller inter frame time and with other traffic models need to be investigated. Also, the environment conditions would be set as ideal by the help of simulation programs and computer simulation of the infrastructure using ns2 or a similar simulator may be used to determine optimum parameters of the wireless networks where VPNs are used.

REFERENCES

[1] J. Allen and J. Wilson. "Securing a Wireless Network", SIGUCCS'02

[2] L. Fazal, S. Ganu, M. Kappes, A.S.Krishnakumar, P. Krishnah (2004). "Tackling Security Vulnerabilities in VPN-based Wireless Deployments", 2004 IEEE International Conference on Volume 1, Page(s):100 - 104 Vol.1

[3] K. Byoung-Jo, S. Srinivasan (2003). "Simple mobility support for IPsec tunnel mode**",** 2003 IEEE Vehicular Technology Conference on Volume 3 Page(s):1999 - 2003 Vol.3

[4] W. Qu, S. Srinivas (2002). "IPSec-based secure wireless virtual private network", MILCOM 2002 on Volume 2, Page(s):1107 - 1112 vol.2

[5] K.S. Rawat, G.H. Massiha (2003). "Secure data transmission over wireless networks: issues and challenges", IEEE Region 5, 2003 Annual Technical Conference Page(s):65 – 68

[6] Gartner Wireless and Mobile Summit 2005, 18 April- 19 April 2005

[7] A.S. Tanenbaum (2000). Computer Networks, Prentice-Hall Press, Page(s): 781

[8] http://www.techonline.com/community retrieved on 30/12/2005

[9] http://compnetworking.about.com/ retrieved on 30/12/2005

[10] http://www.kmj.com/proxim/pxhist.html retrieved on 30/12/2005

[11] http://www.maxim-ic.com/ retrieved on 30/12/2005

[12] http://www4.dogus.edu.tr/bim/wireless.htm retrieved on 30/12/2005

[13] http://www.webopedia.com/ retrieved on 30/12/2005

[14] A. S. Tanenbaum (2000). Computer Networks, Prentice-Hall Press, Page(s): 292-302

[15] www.tutorial-reports.com/wireless retrieved on 30/12/2005

[16] B.S. Bakshi, P. Krishna, N.H. Vaidya, D.K. Pradhan (1997). "Improving performance of TCP over wireless networks ",Proceedings of the 17th International Conference, Page(s):365 - 373

[17] IEEE 802.11 1999. "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications"

[18] J. Walker (2000). "Unsafe at any key size: An analysis of the WEP encapsulation", IEEE 802.11 Task Group E.

[19] S. Fluhrer, I. Martin, A. Shamir (2001). "Weaknesses in the key scheduling algorithm of RC4", Eighth Annual Workshop on Selected Areas in Cryptography.

[20] N. Borisov, I. Goldberg, D. Wagner (2001). "Intercepting mobile communications: The insecurity of 802.11". In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking.

[21] W. A. Arbaugh, N. Shankar,J. Wan (2002). "Your 802.11 network has no clothes", IEEE Wireless Communications.

[22] "WPA Overview" Wi-Fi.org 2005. http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf retrieved on 30/12/2005

[23] IEEE 802.11i 2004. "Amendment 6: MAC Security Enhancements".

[24] P. Ferguson, G. Huston. "What is a VPN?". http://www.employees.org:80/ ferguson/vpn.pdf retrieved on 30/12/2005

[25] G. Meeta, Building a Virtual Private Network, Premier Press, chapter 6

[26] www.cisco.com retrieved on 30/12/2005

[27] http://itsolutions.forbes.com retrieved on 30/12/2005

[28] http://compnetworking.about.com/introductiontoVPNs retrieved on 30/12/2005

[29] RFC 2637, "Point to Point Tunneling Protocol"

[30] RFC 2661, "Layer Two Tunneling Protocol "

[31] www.microsoft.com retrieved on 30/12/2005

[32] http://www.uis.edu/cts/network/wireless.htm retrieved on 30/12/2005

[33] http://www.engin.umich.edu/caen/network/wireless/software.html retrieved on 30/12/2005

[34] http://www.wireless.ubc.ca/vpn/winxpvpn.html retrieved on 30/12/2005

[35] Y. Zahur, T. Andrew Yang (2004). "Journal of Computing Sciences in Colleges" on volume 19 Issue 3, Consortium for Computing Scineces.

[36] K. Guo, S. Mukherjee, S. Paul, S. Rangarajan (2004). **"**Optimal customer provisioning in network-based mobile VPNs Mobile and Ubiquitous Systems", MOBIQUITOUS 2004, Page(s):95 - 104

[37] K.S. Munasinghe, S.A. Shahrestani (2005). "Wireless VPNs: an evaluation of QoS metrics and measures", International Conference Page(s):616 - 622

[38] http://www.networkworld.com/news/2005/041805specialfocus.html retrieved on 30/12/2005

[39] A. Shneyderman, Mobile VPN, Wiley Press, Page(s): 192-196

[40] G.C. Hadjichristofi, N.J. Davis, S.F. Midkiff (2003). ”IPSec overhead in wire line and wireless networks for Web and email applications Performance”, Conference Proceedings of the 2003 IEEE International, Page(s):543 - 547

[41] P. Yong, W. Haitao, L. Keping, C. Shiduan (2001). ” Simulation analysis of TCP performance on IEEE 802.11 wireless LAN”, Info-net 2001 Proceedings on Volume 2, Page(s):520 - 525 vol.2

[42] R. Yavatkar, N. Bhagawat (1994). “Improving end-to-end performance of TCP over mobile internetworks”, Mobile Computing Systems and Applications Proceedings, Page(s):146 - 152

[43] http://www.networksorcery.com/enp/protocol/tcp.htm retrieved on 30/12/2005 retrieved on 30/12/2005

[44] RFC 793, “Transmission Control Protocol”

[45] http://www.networksorcery.com/enp/protocol/udp.htm retrieved on 30/12/2005

[46] RFC 768, “User Datagram Protocol”

[47] http://www.pds-test.co.uk/products/lan_trafficv2_cgi.html retrieved on 30/12/2005

[48] S. Ci, H. Sharif (2002). “A link adaptation scheme for improving throughput in the IEEE 802.11 wireless LAN”, Local Computer Networks Proceedings on Page(s):205 - 208

[49] G. Sachin, M. Kappes (2003). “An experimental study of throughput for UDP and VoIP Traffic in IEEE 802.11b networks “, IEEE Wireless Communication and Networking

[50] P. Chatzimisios,V. Vitsas, A.C. Boucouvalas (2003). "Throughput and delay analysis of IEEE 802.11 ", Network Appliances IEEE 5th International Workshop on Page(s):168 - 174

[51] IEEE 802.11g standard