VPN over a Wireless Infrastructure: Evaluation and Performance Analysis

Kumudu S. Munasinghe

A thesis submitted in fulfillment of the requirements for the award of the degree

Master of Science (Honours)

to

The University of Western Sydney

on

March 2005
Declaration

This is to certify that to the best of my knowledge and belief, the work presented in this thesis is original, unless specified otherwise, and that no part of this material has been submitted, either in full or in part, at this or any other institution.

Kumudu S. Munasinghe

March 2005
To my darling wife and respected parents,
with love
Acknowledgements

The production of any thesis naturally requires valuable contributions, moral support, and blessings from many people. First and foremost, I would like to thank my wife, Savithri and parents, Dr. Sarath Rohana Munasinghe and Dr. Nanda Irani Munasinghe. It is through their immeasurable sacrifices, encouragements, blessings and prayers that I have been able to come this far. With the deepest gratitude, I dedicate this thesis to them.

I am deeply indebted to my principle supervisor Dr. Seyed A. Shahrestani, for being my guide and guru throughout this amazing journey. His in-depth knowledge, unfailing advice, and uplifting moral support helped me overcome many moments of depression and uncertainty in this roller coaster ride. His constructive criticism and continuous feedback immensely helped me in formulating and crystallising ideas. Furthermore, the introduction to the philosophy of scientific research and an intensive training in the art of scientific writing, tremendously contributed towards producing a manuscript, several magnitudes beyond my expectations. If not for Dr. Shahrestani’s unrelenting interest and precious time, a research on wireless virtual private networks would have been virtually impossible. So, thank you!

Additionally, I would like to thank the academic staff of the School of Computing and Information Technology, University of Western Sydney for their stimulating suggestions and encouragements in improving the quality of my work. Thanks also due to my dear colleagues at the Networking Research Laboratory: Houssein Hallani and Davinder Bains for their valuable support and feedback throughout my research. Also, many thanks to Mr. Ian Walsh, the Technical Coordinator of the School of Computing and IT and his team, in providing me with the facilities required for my experiments in the minimum possible time.

I would also like to thank Professor Athula Ginige, the Associate Head of School - Research, for introducing me to my principle supervisor, and for his continuing support and encouragement in accomplishing my goals. Thanks also to the School of Computing and IT for the teaching assistantship provided, and to the University of Western Sydney for the UWS Completions Scholarship, which helped me financially sustain throughout my candidature. Last but not least, my gratitude to Ms. Patricia Skinner, for the proofreading services provided for the production of this thesis.

MY HEARTFELT THANKS TO ALL!
Abstract

This thesis presents the analysis and experimental results for an evaluation of the performance and Quality of Service (QoS) levels of a Virtual Private Network (VPN) implementation over an IEEE 802.11b wireless infrastructure. The VPN tunnelling protocol considered for the above study is IP Security (IPSec). The main focus of the research is to identify the major performance limitations and their underlying causes for such VPN implementations under study.

The experimentation and data collection involved in the study spans over a number of platforms to suit a range of practical VPN implementations over a wireless medium. The collected data includes vital QoS and performance measures, such as the application throughput, packet loss, jitter, and round-trip delay. It further investigates the contribution of the CPU, inter-packet generation rate, payload data size, geographical distance and the number of simultaneously operating VPNs to the behaviour of the above QoS measures.

Once the baseline measure is established, a series of experiments are conducted to analyse the behaviour of a single IPSec VPN operating over an IEEE 802.11b infrastructure, after which the experimentation is extended by investigating the trends of the performance metrics of a simultaneously operating multiple VPN setup. Finally, the work is extended to a geographically spanned multi-campus site-to-site VPN. The two sites are connected via an IPSec VPN tunnel, which is implemented over a public network infrastructure. Furthermore, the two VPN tunnel end-points are connected to a wireless mesh network and an IEEE 802.11b wireless ad hoc network. The performance measures for each of the above scenarios are comparatively analysed for defining acceptable performance and QoS levels for a wireless VPN.

The overall results and analysis of the investigations concludes that the CPU processing power, payload data size, packet generation rate and the geographical distance are critical factors affecting the performance of such VPN tunnel implementations. Furthermore, it is believed that these results may give vital clues for enhancing and achieving optimal performance and QoS levels for VPN applications over WLANs.
Author’s Publications


# Table of Contents

Declaration ......................................................................................................................... ii

Acknowledgements ............................................................................................................... iv

Abstract ................................................................................................................................... v

Author’s Publications ............................................................................................................ vi

List of Figures and Tables ...................................................................................................... x

Glossary of Acronyms and Abbreviations ....................................................................... xiv

### Introduction

1.1 Wireless LAN Security: an Overview ........................................................................ Error! Bookmark not defined.
   1.1.1 General Security Threats and Attacks on WLANs ........................................ Error! Bookmark not defined.

1.2 Security Solutions for Wireless LANs ................................................................ Error! Bookmark not defined.

1.3 The Quality of Service of Wireless VPNs ................................................................. Error! Bookmark not defined.

1.4 Objectives .................................................................................................................. Error! Bookmark not defined.

1.5 Approach ..................................................................................................................... Error! Bookmark not defined.

1.6 Contribution ................................................................................................................. Error! Bookmark not defined.

1.7 Outline of the Thesis ................................................................................................. Error! Bookmark not defined.

### Wireless LAN Security: Research Trends and Issues

2.1 The IEEE 802.11 Standard .................................................................................. Error! Bookmark not defined.
   2.1.1 Wireless LAN Topologies .............................................................................. Error! Bookmark not defined.

2.2 The IEEE 802.11 Security ..................................................................................... Error! Bookmark not defined.
   2.2.1 Authentication ............................................................................................... Error! Bookmark not defined.
   2.2.2 The Wired Equivalent Privacy (WEP) ............................................................. Error! Bookmark not defined.

2.3 Security Flaws of the IEEE 802.11 Standard ......................................................... Error! Bookmark not defined.
   2.3.1 Security Flaws of the IEEE 802.11 Authentication ...................................... Error! Bookmark not defined.
   2.3.2 Security Flaws of the WEP ........................................................................... Error! Bookmark not defined.

2.4 Alternative Solutions for Securing WLANs ......................................................... Error! Bookmark not defined.
   2.4.1 The 802.1x Standard ..................................................................................... Error! Bookmark not defined.
   2.4.2 The 802.11i Standard ..................................................................................... Error! Bookmark not defined.
   2.4.3 The VPN Security Solution .......................................................................... Error! Bookmark not defined.

2.5 VPN Overview .......................................................................................................... Error! Bookmark not defined.
   2.5.1 Types of VPN Services .................................................................................. Error! Bookmark not defined.
   2.5.2 VPN Protocols ............................................................................................... Error! Bookmark not defined.

2.6 VPNs in a WLAN Environment .............................................................................. Error! Bookmark not defined.
2.7 Current and Future Research Trends.......................... Error! Bookmark not defined.

Research Methodology............................................. Error! Bookmark not defined.

3.1 Performance Metrics ............................................. Error! Bookmark not defined.

3.2 Experimental Setup ............................................. Error! Bookmark not defined.

3.2.1 Hardware....................................................... Error! Bookmark not defined.

3.2.2 Software....................................................... Error! Bookmark not defined.

3.2.3 Case 1: Setup of a Single Wireless VPN..................... Error! Bookmark not defined.

3.2.4 Case 2: Setup of Multiple Wireless VPNS ................ Error! Bookmark not defined.

3.2.5 Case 3: Setup of a Site-to-Site VPN........................ Error! Bookmark not defined.

3.3 Experimentation and Data Collection ......................... Error! Bookmark not defined.

3.3.1 Establishment of Baseline Performance Measurements..... Error! Bookmark not defined.

3.3.2 Performance Measurement for a Single Wireless VPN..... Error! Bookmark not defined.

3.3.3 Performance Measurement of Multiple Wireless VPNS ...... Error! Bookmark not defined.

3.3.4 Performance Measurements for a Site-to-Site VPN Tunnel. Error! Bookmark not defined.

Analysis of Performance Results ................................. Error! Bookmark not defined.

4.1 Throughput ....................................................... Error! Bookmark not defined.

4.1.1 Throughput Analysis for a Single Wireless VPN............ Error! Bookmark not defined.

4.1.2 Throughput Analysis for a Multiple Wireless VPNS........ Error! Bookmark not defined.

4.1.3 Throughput Analysis for a Site-to-Site VPN................ Error! Bookmark not defined.

4.2 Packet Loss ...................................................... Error! Bookmark not defined.

4.2.1 Packet Loss Analysis for a Single Wireless VPN........... Error! Bookmark not defined.

4.2.2 Packet Loss Analysis for a Multiple Wireless VPNS........ Error! Bookmark not defined.

4.2.3 Packet Loss Analysis for a Site-to-Site VPN............... Error! Bookmark not defined.

4.3 CPU Utilisation .................................................. Error! Bookmark not defined.

4.3.1 CPU Utilisation Analysis for a Single Wireless VPN...... Error! Bookmark not defined.

4.3.2 CPU Utilisation Analysis for a Multiple Wireless VPNS..... Error! Bookmark not defined.

4.3.3 CPU Utilisation Analysis for a Site-to-Site VPN............ Error! Bookmark not defined.

4.4 Round-trip Delay ................................................ Error! Bookmark not defined.

4.4.1 Round-trip Delay Analysis for a Single Wireless VPN..... Error! Bookmark not defined.

4.4.2 Round-trip Delay Analysis for a Multiple Wireless VPN... Error! Bookmark not defined.

4.4.3 Round-trip Delay Analysis for a Site-to-Site VPN.......... Error! Bookmark not defined.

4.5 Jitter .............................................................. Error! Bookmark not defined.

4.5.1 Jitter Analysis for a Single Wireless VPN.................. Error! Bookmark not defined.

4.5.2 Jitter Analysis for a Multiple Wireless VPNS.............. Error! Bookmark not defined.

4.5.3 Jitter Analysis for a Site-to-Site VPN....................... Error! Bookmark not defined.

Performance Limitations and Causes ......................... Error! Bookmark not defined.

5.1 Throughput: Limitations and Causes.......................... Error! Bookmark not defined.

5.2 Packet Loss: Limitations and Causes........................ Error! Bookmark not defined.

5.3 Round-trip Delay: Limitations and Causes................... Error! Bookmark not defined.

5.4 Jitter: Limitations and Causes ................................ Error! Bookmark not defined.
Summary, Conclusions and Future Work

References
List of Figures and Tables

Figures

Figure 2.1: The IEEE 802.11 Standards Compared against the OSI Reference Model. 21
Figure 2.2: An Independent Basic Service Set (IBSS). 22
Figure 2.3: Infrastructure Basic Service Set. 23
Figure 2.4: Extended Service Set (ESS). 23
Figure 2.5: Shared Key Authentication Process. 25
Figure 2.6: EAP Architecture. 28
Figure 2.7: IEEE 802.1X Architecture. 29
Figure 2.8: EAPOL exchange on an 802.11 network. 30
Figure 2.9: Intranet VPN Services. 34
Figure 2.10: Extranet VPN Services. 35
Figure 2.11: Remote Access (Dial-Up) VPN Services. 36
Figure 2.12: The concept of VPN tunneling. 38
Figure 2.13: VPN Security for IEEE 802.11 WLANs. 40
Figure 3.1: The Basic Hardware Setup. 46
Figure 3.2: Setup of a Single Wireless VPN. 48
Figure 3.3: Setup of Multiple Wireless VPNs. 49
Figure 3.4: Setup of a Site-to-Site VPN Tunnel. 51
Figure 4.1: The Average Throughput Graphs for Traffic Generated with a 1ms Inter-packet Generation Gap. 66
Figure 4.2: The Average Throughput Graphs for Traffic Generated with a 5ms Inter-packet Generation Gap. 66
Figure 4.3: The Average Throughput Graphs for Traffic Generated with a 1ms Inter-packet Generation Gap. 69
Figure 4.4: Expanded Section of Figure 4.3; the Average Throughput Graph for Payload Data Sizes of 25 to 200 Bytes. 70
Figure 4.5: The Average Throughput Graphs for Traffic Generated with a 5ms Inter-packet Generation Gap. 70
Figure 4.6: The Average Throughput Graphs for Traffic Generated with 1 ms Inter-packet Generation Gap.

Figure 4.7: The Average Throughput Graphs for Traffic Generated with 5 ms Inter-packet Generation Gap.

Figure 4.8: Packet Loss in Transmitting Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.9: Packet Loss in Receiving Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.10: Packet Loss in Transmitting Traffic Generated at 5 ms Inter-packet Delay.

Figure 4.11: Packet Loss in Receiving Traffic Generated at 5 ms Inter-packet Delay.

Figure 4.12: Packet Loss in Transmitting Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.13: Packet Loss in Receiving Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.14: Packet Loss in Transmitting Traffic Generated at 5 ms Inter-packet Delay

Figure 4.15: Packet Loss in Receiving Traffic Generated at 5 ms Inter-packet Delay.

Figure 4.16: Packet Loss in Transmitting Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.17: Packet Loss in Receiving Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.18: Packet Loss in Transmitting Traffic Generated at 5 ms Inter-packet Delay.

Figure 4.19: Packet Loss in Receiving Traffic Generated at 5 ms Inter-packet Delay.

Figure 4.20: The CPU Utilisation Graphs for Traffic Generated with a 1 ms Inter-packet Generation Gap.
Figure 4.21: The CPU Utilisation Graphs for Traffic Generated with a 5 ms Inter-packet Generation Gap. 86
Figure 4.22: CPU Utilisation for Traffic Generated at 1 ms Inter-packet Delay. 88
Figure 4.23: CPU Utilisation for Traffic Generated at 5 ms Inter-packet Delay. 88
Figure 4.24: CPU Utilisation for Traffic Generated at 1 ms Inter-packet Delay. 90
Figure 4.25: CPU Utilisation for Traffic Generated at 5 ms Inter-packet Delay. 90
Figure 4.26: The Round-trip Delay Graphs for Traffic Generated with a 1 ms Inter-packet Generation Gap. 92
Figure 4.27: The Round-trip Delay Graphs for Traffic Generated with a 5 ms Inter-packet Generation Gap. 92
Figure 4.28: Round-trip Delay for Traffic Generated at 1 ms Inter-packet Delay. 93
Figure 4.29: Round-trip Delay for Traffic Generated at 5 ms Inter-packet Delay. 94
Figure 4.30: Round-trip Delay for Traffic Generated at 1 ms Inter-packet Delay. 95
Figure 4.31: Round Trip Delay for Traffic Generated at 5 ms Inter-packet Delay. 96
Figure 4.32: The Jitter Graphs for Traffic Generated with a 1 ms Inter-packet Generation Gap. 97
Figure 4.33: The Jitter Graphs for Traffic Generated with a 5 ms Inter-packet Generation Gap. 98
Figure 4.34: The Jitter Graphs for Traffic Generated at 1 ms Inter-packet Delay. 99
Figure 4.35: The Jitter Graphs for Traffic Generated at 5 ms Inter-packet Delay. 99
Figure 4.36: The Jitter Graphs for Traffic Generated at 1 ms Inter-packet Delay. 101
Figure 4.37: The Jitter Graphs for Traffic Generated at 5 ms Inter-packet Delay. 101
Figure 5.1: Variation of Throughput and CPU Utilisation against Payload Data Size. 104
Figure 5.2: Variation of Packet Loss and CPU Utilisation against Payload Data Size. 106
Figure 5.3: Variation of Packet Loss and Throughput against Payload Data Size. 107
Figure 5.4: Variation of Round-trip Delay and CPU Utilisation against Payload Data Size. 109
Tables

Table 2.1:      IEEE 802.11 PHY Specifications            21
Table 3.1:      Hardware Configuration                  45
Table 3.2:      IPSec Policy Configuration for a Single VPN 49
Table 3.3:      IPSec Policy Configuration for Multiple Tunnels 50
Table 3.4:      IPSec Policy Configuration for a Site-to-Site VPN 52
Table 3.5:      Baseline Readings for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap 54
Table 3.6:      Baseline Readings for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap 55
Table 3.7:      Performance Readings of a Single Wireless IPSec VPN for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap 56
Table 3.8:      Performance Readings of a Single Wireless IPSec VPN for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap 57
Table 3.9:      Performance Readings for Two Simultaneous Wireless IPSec VPNs for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap 59
Table 3.10:     Performance Readings for Two Simultaneous Wireless IPSec VPNs for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap 59
Table 3.11:     Performance Readings for Three Simultaneous Wireless IPSec VPNs for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap 61
Table 3.12:     Performance Readings for Three Simultaneous Wireless IPSec VPNs for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap 61
Table 3.13:     Performance Readings for a Site-to-Site IPSec VPN Tunnel for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap 63
Table 3.14:     Performance Readings for a Site-to-Site IPSec VPN Tunnel for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap 64
## Glossary of Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>Triple Data Encryption Standard</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorising and Accounting</td>
</tr>
<tr>
<td>ACK</td>
<td>Acknowledgement</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>AMD</td>
<td>Advance Micro Devices</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>Av.</td>
<td>Average</td>
</tr>
<tr>
<td>BSS</td>
<td>Basic Service Set</td>
</tr>
<tr>
<td>BSSID</td>
<td>Basic Service Set Identifier</td>
</tr>
<tr>
<td>CAMA/CA</td>
<td>Carrier Sense Multiple Access with Collision Avoidance</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DP</td>
<td>Destination Port</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPoL</td>
<td>Extensible Authentication Protocol over LAN</td>
</tr>
<tr>
<td>EAPoW</td>
<td>Extensible Authentication Protocol over Wireless</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>ESS</td>
<td>Extended Service Set</td>
</tr>
<tr>
<td>ESSID</td>
<td>Extended Service Set Identifier</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>Hex</td>
<td>Hexadecimal</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>IBSS</td>
<td>Independent Basic Service Set</td>
</tr>
<tr>
<td>IDEA</td>
<td>International Data Encryption Standard</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPSecMon</td>
<td>Internet Protocol Security Monitor</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>ISM</td>
<td>Industrial Scientific and Medical</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IV</td>
<td>Integrity Vector</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LLC</td>
<td>Link Layer Control</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>Mbps</td>
<td>Mega bits per second</td>
</tr>
<tr>
<td>MIC</td>
<td>Message Integrity Check</td>
</tr>
<tr>
<td>ms</td>
<td>millisecond</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>Nos.</td>
<td>Numbers</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PAE</td>
<td>Port Authentication Entities</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Security</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical</td>
</tr>
<tr>
<td>Pkt.</td>
<td>Packet</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>PVC</td>
<td>Permanent Virtual Circuit</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In user Service</td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher four</td>
</tr>
<tr>
<td>RC5</td>
<td>Rivest Cipher five</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RSN</td>
<td>Robust Security Network</td>
</tr>
<tr>
<td>Rx.</td>
<td>Receiving</td>
</tr>
<tr>
<td>SCIT</td>
<td>School of Computing and Information Technology</td>
</tr>
<tr>
<td>SHA-1</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SP</td>
<td>Source Port</td>
</tr>
<tr>
<td>SP2</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td>SPI</td>
<td>Security Parameter Index</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>STA</td>
<td>Station</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TSN</td>
<td>Transitional Security Network</td>
</tr>
<tr>
<td>Tx.</td>
<td>Transmission</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UWS</td>
<td>University of Western Sydney</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive OR</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Over the past several years, wireless technology has revolutionised the way people communicate. In particular, the Wireless Local Area Network (WLAN) technology has become so popular that it has already been accepted as a convenient alternative to conventional wired LANs. Some of the key advantages of the WLAN technology can be identified as ubiquitous network access without wires, relatively high data rates, rapidly improving quality of service, and competitive pricing in contrast to its wired counterparts. These became major contributing factors for WLANs in gaining their market momentum.

With this rapidly growing adoption of the wireless networking technology, for many implementers, security and Quality of Service (QoS) remain as issues of the highest priority. The main reason for growing concerns in security is the susceptibility of the wireless media to a number of possible security threats. On the other hand, QoS is increasingly becoming important for the next generation of wireless multimedia applications.

The aim of this chapter is to establish the objective and scope of this research. Therefore, the first half begins by introducing the importance of security in wireless networks. This is followed by a general overview of security solutions for wireless LANs. Next, a brief introduction to wireless Virtual Private Networks (VPNs) is provided, with the importance of Quality of Service (QoS) in a wireless environment given due importance. The chapter concludes with a clear indication of how the entire research has been carried out and how it has been presented in this thesis.

1.1 Wireless LAN Security: an Overview

While wireless networks have many advantages over conventional wired networks, they expose the user to great risks, because when the physical media is replaced by Radio Frequency (RF) communication channels, the communication links do not have the basic physical security anymore. These high frequency RF waves cannot be confined to any controlled physical space. Therefore, the wireless technology is inherently open to interception
by a potential attacker who is even beyond the confines of a physically controlled area. Hence, a robust wireless security solution is a must for every WLAN deployment.

1.1.1 General Security Threats and Attacks on WLANs
Having established the need for wireless security and its importance, in this section, the possible types of threats and attacks on wireless LANs are discussed. General security threats and attacks can be categorised into two major types. The first category consists of active attacks. In the case of an active attack, the potential intruder gains access to the wireless network and may destroy or alter the data. In contrast, in the second category, which is known as passive attacks, the potential intruder gains access to the wireless network but only eavesdrops on the transmitted data.

1.1.1.1 Active Attacks:

a. Invasion and Resource Stealing or Spoofing: This is one of the basic types of active attacks launched to gain unauthorised access to network resources and services. The intruder will first try to determine the access parameters of a potentially vulnerable wireless network. Such access parameters may include a MAC address and an IP address of a particular client. When the client is not transmitting, the intruder will first reconfigure his/her terminal with the known information. Once this is done, the intruder’s terminal will appear as the authorised terminal and will be able to access most of the resources. This technique is known as MAC spoofing [1].

b. Denial of Service (DoS): A denial of service attack can take many forms. The most fundamental type of attack could be flooding of the network bandwidth with meaningless data. This will eventually bring the network to a halt. To initiate such an attack, an intruder identifies a potential wireless device on the network and will continue to bombard it with excessive amounts of data. This process will soon overwhelm the wireless device, causing it to become unusable. There may be more complex and sophisticated denial of service attacks, such as spoofing disassociation management frames to the wireless terminals or causing excessive RF interference to jam the communication channel [1].
c. **Replay Attacks:** Initially, the intruder may use a third-party wireless packet sniffing/monitoring utility to capture packets exchanged between two wireless entities. Once such packets are captured, the intruder can analyse the packet content and launch a number of attacks. One such example could be to initiate a denial of service attack. On the other hand, the intruder could collect sufficient data to crack an encryption key.

1.1.1.2 **Passive Attacks:**

a. **War-driving:** This is the most common form of passive attack. As we know, an RF signal may sometimes extend beyond the physical confines of a building. In such cases, any potential intruder with a portable computing device may be able to easily detect such RF signals. With appropriate war-driving tools, in no time the intruder will be able to penetrate into the network.

b. **Man-in-the-Middle Attacks:** This is an attack that requires some sophisticated hacking software and may cause significant levels of disruption and chaos. The potential intruder captures packets in transmission between two communicating entities. The two communicating entities see the intruder as its corresponding authenticated peer entity. The intruder is in a position to capture the legitimate information or even initiate a DoS attack.

Looking at these security issues relating to wireless networks, two major root causes can be identified. The first is the lack of understanding and proper management skills of wireless networks. Most network managers apply the conventional network management techniques and principles to WLANs. Such approaches may sometimes make the WLAN potentially more vulnerable to an attack. The second cause is the inherent security vulnerabilities in the IEEE 802.11-1997 standard itself [2]. The next section briefly introduces the security solutions for wireless LANs and introduces the importance of QoS for a wireless VPN.
1.2 Security Solutions for Wireless LANs

The fundamental security services addressed in the IEEE 802.11 standard are authentication and the Wired Equivalent Privacy (WEP) mechanism [2]. The authentication service is used in the process of association of stations and the Access Points (APs) in an infrastructure Basic Service Set (BSS) or for the association of two stations in an Independent Basic Service Set (IBSS). In these situations, a so called Service Set Identifier (SSID) is used to distinguish each BSS (or IBSS) from others. It is a common practice to use the SSID as a shared password, providing wireless stations and Wireless LANs (WLANs) with some form of access control mechanism. Furthermore, IEEE 802.11 standard specifies WEP as an optional mechanism for protecting authorised users of a wireless LAN from casual eavesdropping. The security services provided by the WEP are confidentiality, authentication and access control, in conjunction with layer management [2]. The shortcomings and deficiencies of these security services have been well identified and documented by several researchers [3], [4].

As a quick response to address the inadequacies of WEP, an umbrella standard referred to as the IEEE 802.1x standard was introduced. The IEEE 802.1x standard adopts an enhanced “port based network access control” framework for authentication and key exchange in wireless LANs [5]. The IEEE 802.11 Task Group i proposed yet another new-generation security standard. This solution initially proposed the Temporal Key Integrity Protocol (TKIP).

At the time, it appeared as the best short-term solution within the deployed hardware base. A further improvement to TKIP is the incorporation of the Advance Encryption Standard (AES). AES is a crypto brick, which is capable of providing an enhanced form of encryption. It is also a vital part of the IEEE 802.11i specifications, which recently received its final approval process [6]. However, its implementation may require the use of a much more powerful processor than what is currently available in most of the existing products.

An alternative and generally well-received solution is based on implementing a VPN tunnel over the wireless infrastructure. A VPN is a solution that aims to provide secure private communications over a public network infrastructure such as the Internet. VPNs can be deployed over wireless networks to secure communication between wireless clients and their conventional enterprise networks through secure virtual tunnels.
1.3 The Quality of Service of Wireless VPNs

Amongst many open research questions on wireless VPNs the issue of Quality of Service (QoS) remains, and how it is supported in these networks. Since the existing IEEE 802.11 standard does not address the above issue, wireless networks are susceptible to errors owing to the nature of their link layer environment. Furthermore, the data transmission capability of a wireless network suffers from the overhead traffic related to IEEE 802.11 control and management frames. This results in the reduction of the net throughput of a WLAN by 50 – 60 per cent of the nominal.

Implementation of a VPN over a wireless link to secure the transmission may further diminish its performance and QoS levels. Therefore, it is highly important for wireless network operators and application developers to understand the behavior trends of such QoS parameters.

On the other hand, as wireless networks become widely accepted for voice, video and data communications, wireless applications must be carefully designed to ensure reduced latency, accurate delivery and prioritisation. Therefore, the QoS expectations of each of these services and applications must be clearly defined and established. In many instances, such QoS expectations may exceed the inherent limitations of the wireless environment.

Unfortunately, not many researchers have contributed towards defining the acceptable performance and QoS levels of a wireless VPN setup. If such measures are established, wireless network operators and application developers will be able to customise applications in such a way that high availability and service reliability is achieved by a VPN.

1.4 Objectives

The objective of this thesis is to evaluate the performance and QoS levels of one of the most popularly used wireless network security solutions. More specifically, this thesis presents the analysis and experimental results for evaluation of the performance of a VPN implementation over an IEEE 802.11b wireless infrastructure. The VPN tunnelling protocol considered for the above study is IP Security (IPSec). The main focus of the research is to identify the major performance limitations and their underlying causes for such VPN implementations under study.
1.5 Approach

The experimentation and data collection involved in the study spans over a number of platforms to suit a range of practical VPN implementations over a wireless medium. The collected data includes vital QoS and performance measures such as the application throughput, packet loss, jitter, and round-trip delay. It further investigates the contribution of the CPU, inter-packet generation rate, payload data size, geographical distance and the number of simultaneously operating VPNs. Once the baseline measure is established, a series of experiments are conducted to analyse the behaviour of a single IPSec VPN operating over an IEEE 802.11b infrastructure, after which the experimentation is extended by investigating the trends of the performance metrics of a simultaneously operating multiple VPN setup. Finally, the work is extended to a geographically spanned multi-campus site-to-site VPN. The two sites are connected via an IPSec VPN tunnel, which is implemented over a public network infrastructure. Furthermore, the two VPN tunnel end-points are connected to a wireless mesh network and an IEEE 802.11b wireless ad hoc network. The performance measures for each of the above scenarios are comparatively analysed for defining acceptable performance and QoS levels for a wireless VPN.

1.6 Contribution

The results of this study can be used in defining acceptable performance and QoS levels for a wireless VPN configuration, under general enough conditions. By and large, this provides a guideline for predicting the behaviour of performance parameters, under such circumstances. Furthermore, these results can be used for estimating maximum possible throughput, percentage of packet loss, round-trip delay, and jitter for a specific data flow over a wireless VPN. Therefore, network operators and application developers can use these results to fine tune application parameters for achieving optimal QoS levels and reliability over such wireless VPNs.

1.7 Outline of the Thesis

The next chapter provides an in-depth discussion on the current and future trends in research in wireless network security. This discussion begins by introducing the IEEE 802.11 security standard to the reader, after which the security flaws of the existing standard and alternative
solutions are subsequently introduced. At this point the reader’s attention is drawn towards the benefits of using a VPN over a wireless infrastructure for securing communications. Chapter 2 concludes by establishing the need for QoS of a wireless VPN and presenting some of the current research trends in this area.

Once the purpose of the research is established, the stage is set for discussing the details of the experimentation. Chapter 3 contains a detailed description of the experimental platforms, setups and methodologies used for data collection. The objective behind the collection of such data is to obtain a comprehensive set of measurements for analysis and evaluation of the QoS measures of a wireless VPN.

Chapter 4 uses the previously collected performance results to perform a detailed analysis. The behavioural trends of each of the performance metrics are analysed individually. Chapter 5 uses these analysis results to identify the specific performance-limiting causes for each QoS metric considered under the study. Finally, this thesis concludes by drawing important conclusions based on the overall results of the research.
Chapter 2

Wireless LAN Security: Research Trends and Issues

This chapter provides a theoretical background and a literature review on the research trends in wireless LAN security. The first half of this section describes the basic security mechanisms introduced by the IEEE 802.11 standard and why it is incapable of providing a complete security solution to WLANs. The quest for alternate WLAN security solutions motivated researchers to develop new security standards and methods. The latter half of this chapter presents three such alternate security standards. Out of these three, the main focus is on the VPN solution, on which this research is based. It describes how VPNs can be deployed over wireless networks to secure communications between wireless clients and their conventional enterprise networks. This chapter concludes by discussing the current and future directions in research, and its importance.

2.1 The IEEE 802.11 Standard

The Institute of Electrical and Electronic Engineers (IEEE) formed the 802.11 Work Group in September 1990. The objective was to develop a standard for wireless LANs to operate on a low-power unlicensed frequency range. The selected frequency range was the Industrial, Scientific, and Medical (ISM) bands, either the 2.4 GHz band or 5 GHz band, set aside by the Federal Communications Commission (FCC). The first 802.11 standard was released in 1997 [2].

This standard addresses the Media Access Control (MAC) and Physical (PHY) standards separately. The original PHY standard provides data rates of 1-2 Mbps and three fundamentally different mechanisms of operation. They are namely: Infrared, 2.4 GHz Frequency Hopping Spread Spectrum (FHSS), and 2.4 GHz Direct Sequence Spread Spectrum (DSSS). The task assigned to the 802.11 MAC is to coordinate an access mechanism, which allows fair access to the medium. Since wireless stations do not have the capability of detecting collisions, 802.11 WLANs need an access method which makes every effort to avoid
collisions. This method is known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and will be discussed in more detail later.

In 1999 IEEE released a new PHY standard named 802.11b [7]. This new standard was capable of providing higher bit rates up to 11 Mbps using DSSS within the 2.4 GHz range. About the same time, IEEE released another PHY standard named 802.11a. It provided bit rates up to 54 Mbps and operated on the 5 GHz range [8]. However, instead of using DSSS as in the previous cases, 802.11a used a new modulation method called Orthogonal Frequency Division Multiplexing (OFDM). The most recent contribution to the family of 802.11 PHY standards is 802.11g, operating in the 2.4 GHz range and using OFDM [9]. At present, the IEEE 802.11g standard is capable of providing data rates up to 54 Mbps. Figure 2.1 shows the basic IEEE 802.11 structure and Table 2.1 summarises the IEEE 802.11 PHY specifications.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Max. Data Rate</th>
<th>Frequency</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2 Mbps</td>
<td>2.4 GHz and IR</td>
<td>FHSS and DSSS</td>
</tr>
<tr>
<td>802.11b</td>
<td>11 Mbps</td>
<td>2.4 GHz</td>
<td>DSSS</td>
</tr>
<tr>
<td>802.11a</td>
<td>54 Mbps</td>
<td>5 GHz</td>
<td>OFDM</td>
</tr>
<tr>
<td>802.11g</td>
<td>54 Mbps</td>
<td>2.4 GHz</td>
<td>OFDM</td>
</tr>
</tbody>
</table>

Table 2.1: IEEE 802.11 PHY Specifications

---

Figure 2.1: The IEEE 802.11 Standards Compared against the OSI Reference Model.
2.1.1 Wireless LAN Topologies

The WLAN station (STA) is the most basic component of the wireless network. A station may be a laptop PC, handheld device, or an Access Point (AP) that contains the functionality of the 802.11 protocol. The next important concept is the Basic Service Set (BSS). The BSS can be considered as the basic building block of an 802.11 wireless LAN. The BSS consists of a logical group of wireless stations, which may be a collection of a number of stations.

There are basically two types of BSS that correspond to two transmission methods supported by WLANs. They are namely,

- Peer-to-Peer (or Ad Hoc)
- Infrastructure.

![Figure 2.2: An Independent Basic Service Set (IBSS).](image)

Peer-to-peer or ad hoc networking consists of a group of computing devices equipped with wireless Network Interface Cards (NICs) directly communicating with one another. This setup does not use a wireless AP and is called an Independent Basic Service Set (IBSS), as illustrated by Figure 2.2. In an ad hoc wireless network, the Basic Service Set Identification (BSSID) is used as an identification method for all entities belonging to one BSS. The BSSID is a thirty-two character (maximum) alphanumeric key. For the wireless devices in one BSS to communicate with each other, all devices must share the same BSSID.

Infrastructure networking requires all wireless nodes to communicate via an AP. The AP is connected to the main wired networking infrastructure and acts as a relay between the wireless and wired LANs. This structure is referred to as an Infrastructure Basic Service Set, as shown by Figure 2.3. Due to loss of signal strength as a result of attenuation, an Infrastructure BSS has a finite limit.
An extension to such a setup will require additional APs to be set up, which will create further Infrastructure Basic Service Sets. The connection of two or more Infrastructure Basic Service Sets constitutes an Extended Service Set (ESS) (Figure 2.4). A fundamental issue arising from this setup is how to ensure stations communicate with the correct AP or the BSS that it belongs to. The solution is to have an Extended Service Set Identifier (ESSID) to distinctively identify each AP or BSS. Having the proper ESSID configured, wireless stations will be able to confine themselves to one BSS. To make sure that each station is communicating with the correct AP within its BSS, a special identifier called the Service Set ID (SSID) is employed. In most cases, this is used as an elementary password-based access mechanism for restricting unauthorised stations from accessing a wireless AP.
2.2 The IEEE 802.11 Security

This section discusses the basic security mechanisms addressed by the IEEE 802.11 standard. In order to provide a minimum amount of security in a WLAN, the IEEE 802.11 standard makes two recommendations [2]. The first is to have an authentication mechanism as a means to WLAN access control. The second is a means of providing privacy for the wireless data, which is fulfilled by introducing encryption. However, all authentication methods defined under the IEEE 802.11 standard rely on the privacy supported by the Wired Equivalent Privacy (WEP) algorithm. Neither mechanism alone is enough to secure a WLAN.

2.2.1 Authentication

Authentication is a process that verifies who can access what in a network. Under the IEEE 802.11 specification, any station that requires the use of the WLAN must be authenticated prior to being able to transfer data. It specifies two mechanisms for authentication of WLAN clients [2].

- **Open System Authentication**: This is the default authentication service that doesn’t have authentication

- **Shared Key Authentication**: This involves a shared key to authenticate the station to the AP.

2.2.1.1 Open System Authentication

Open system authentication is the simplest and default authentication algorithm for IEEE 802.11 networks. This is a null authentication process, which provides access to anyone who forwards a request. It involves a two-step process. The first is the identity declaration and request for authentication. The second is the authentication result. If the result is “successful,” the station will be mutually authenticated.

2.2.1.2 Shared-key Authentication

This method requires the client station and the AP to have the WEP privacy mechanism enabled. The required secret shared key is presumed to have been delivered to the participating stations via a secure channel. However, the IEEE 802.11 standards committee has not specifically addressed the key distribution or management mechanisms. This is left as an open
issue for the manufacturers and implementers. Figure 2.5 shows the shared-key authentication process.

![Diagram of shared key authentication process]

*Figure 2.5: Shared Key Authentication Process.*

**2.2.1.3. MAC Address Authentication**
Although this method is not specified in the IEEE 802.11 specification, it is supported by many vendors [10]. MAC address authentication simply verifies the station’s AC address against a locally configured list of addresses in an AP or an external authentication server. Therefore, an administrator can use this method to enhance the standard 802.11 authentication methods.

**2.2.2 The Wired Equivalent Privacy (WEP)**
The IEEE 802.11 standard has a feature to provide wireless LANs with an equivalent level of privacy commensurate with non-encrypted data flowing over a wired LAN infrastructure [2]. This technology is known as Wired Equivalent Privacy or WEP. The WEP protocol achieves three main security goals: confidentiality, access control and data integrity. Confidentiality prevents the data from casual eavesdropping. The second objective of WEP is to prevent unauthorised access to the wireless infrastructure. Finally, data integrity uses an integrity checksum to prevent tampering with transmitted messages.

WEP uses a shared-key mechanism with a symmetric cipher known as RC4 (designed by Ron Rivest in 1987). The standard specifies a secret key to be configured on all wireless stations and access points. This key is used to generate a pseudo-random number sequence,
Chapter 2 – Wireless LAN Security: Research Trends and Issues

which is used for encryption and decryption of data. The original key length specified in the
standard is 40 bits. However, most vendors managed to implement 104-bit keys for improved
security.

WEP combines a 40-bit WEP key with a 24-bit random number known as an
Initialisation Vector (IV) to encrypt the data. Some equipment manufacturers have also
implemented a 104-bit implementation. The sender XORs the stream cipher with the actual
data to produce ciphertext. The packet, combined with the IV (in clear text) with the ciphertext,
is sent to the receiver. The receiver decrypts the packet using the stored WEP key and the
attached IV.

2.3 Security Flaws of the IEEE 802.11 Standard

The IEEE 802.11 standard has only been capable of providing limited levels of security. Many
shortcomings of the authentication and privacy mechanisms of the above standard have been
reported by several researchers [3], [11], [12], [4]. This section discusses several serious
security flaws and the ensuing attacks.

2.3.1 Security Flaws of the IEEE 802.11 Authentication

Of the two standard authentication mechanisms specified, the first, open system authentication,
is a null authentication process. This simply provides access to anyone who forwards a request.
For secure authentication the second mechanism, which is the shared-key authentication, must
be used. It has been argued that the shared-key authentication protocol can be easily exploited
through a passive attack by eavesdropping on the mutual authentication [3]. In this case, the
fixed structure of the shared-key authentication protocol (discussed in section 2.2.1.2) and the
flaws of the WEP algorithm are identified as potential causes [3].

Despite the fact that it is not specified as a standard authentication protocol, MAC
address authentication has become a commonly addressed practice in the industry.
Unfortunately, due to the reasons identified below, MAC address authentication is incapable of
offering a reasonable standard of security [3]. Firstly, the MAC addresses are transmitted in
clear (even when encryption is enabled); they can be sniffed easily. Secondly, most wireless
network interface cards permit the changing of MAC addresses via different third-party software. Thus, an attacker can very easily gain access to a restricted network [13].

### 2.3.2 Security Flaws of the WEP

This section discusses some of the well-known design flaws of WEP and point out the attacks that result. It has been revealed that the flaws of WEP have given rise to many short-cut attacks, which can be successfully launched on the system irrespective of the WEP key size[14].

The stream cipher RC4 used for providing confidentiality operates on a secret key, which is expanded into an arbitrarily long “keystream” of pseudorandom bits. One of the fundamental requirements for a stream cipher is that the key stream must not be repeated. Thus, WEP creates a new key by combining its 40-bit secret key with a 24-bit random public IV. Each frame transmission uses a different key out of $2^{24}$ keys for data encryption. Since the WEP IV key space is far too small, the probability of IV duplication is quite high [4]. WEP is unable to avoid such IV collisions because its design does not address such a criterion. Thus an IV collision gives rise to a number of attacks.

For a potential intruder, finding such an IV collision is an effortless task due to the following reasons. Firstly, the IV field is transmitted in clear and duplicate IVs can be easily identified. Secondly, there is a very high probability for the same 24-bit IV to be generated in multiple messages. Therefore, if two messages are encrypted under the same IV and secret key, information about both messages can be revealed [11], [4]. Another such attack is, if one of the messages is known, the plaintext of the other the is immediately obtainable [11]. Therefore, it is impossible to achieve privacy with WEP by simply increasing the key size [4].

WEP uses a checksum to ensure the integrity of the data transmitted. The implemented checksum is CRC-32 and this is included as a part of the encrypted payload of the packet. Since CRC-32 is not a cryptographically secure message authentication code, it has been argued that they are not resilient against malicious attacks [11]. This problem becomes worse since the message payload is encrypted by a stream cipher. Most of the above analysis applies to any stream cipher in general. Nevertheless, it has been pointed out that RC4 also suffers from a few weaknesses, which makes the reliability of WEP more uncertain. The first of which is the identification of “weak” keys, which makes is far easier to cryptanalyze data encrypted
under these keys [4], [12]. The second issue is a related key vulnerability, which applies when part of the key is exposed to the attacker. It is proved that an attacker can relatively easily identify the secret part of the key by analysing various exposed values [12].

2.4 Alternative Solutions for Securing WLANs

This section introduces the three alternate standards used to secure wireless LANs. These are namely; the umbrella standard referred to as IEEE 802.1x, the new IEEE 802.11i specification, and the use of a Virtual Private Network (VPN).

2.4.1 The 802.1x Standard

A wireless environment needed a mechanism to restrict network connectivity (at the MAC layer) from unauthorized entities. Thus the IEEE standards group designed a new security architecture named the Robust Security Network (RSN). The communication framework of RSN revolves around the IEEE 802.1x standard. This section discusses about the IEEE 802.1x standard, which provides an enhanced a port based network access control mechanism [5]. It incorporates an architectural foundation for authentication, key exchange and access control for wireless LANs. The IEEE 802.1x standard is based the IETF’s Extensible Authentication Protocol (EAP), which was initially defined for wide area networking in RFC 2284 [15].

2.4.1.1 Extensible Authentication Protocol (EAP)

IEEE 802.1X standard is based on the Extensible Authentication Protocol [15], commonly known as EAP. EAP was a result of the Internet Engineering Task Force (IETF) in enabling a framework for a single point-to-point protocol to support a wide variety of authentication mechanisms. Figure 2.6 illustrates the EAP stack. This annotates how the basic EAP architecture is capable of operating over any link layer and supporting almost any kind of authentication schema.

![EAP Architecture](image)

*Figure 2.6: EAP Architecture*
2.3.1.2 IEEE 802.1X General architecture

The IEEE 802.1X general framework defines three major entities as illustrated by Figure 2.7. The first of which is the end user machine/client named the Supplicant. The second is a facility controlling access to the LAN via specific ports named the Authenticator. The above standard refers to the Supplicant and the Authenticator as Port Authentication Entities (PAEs) [5]. The third is the Authentication Server to which any incoming requests are logically forwarded by the Authenticator for actual processing. A form of EAP, either EAP over LANs (EAPoL) or EAP over wireless (EAPoW) may be used between the authenticator and supplicant for communication. On the back end between the Authenticator and the Authentication Server the protocol typically used is “EAP over RADIUS”.

![IEEE 802.1X Architecture](image)

Figure 2.7: IEEE 802.1X Architecture

It is worth mentioning that this is purely a framework, and the actual authentication mechanism is implemented by the authentication server. This mechanism enables to simply issue challenges and confirm or deny access. The authentication server that makes the judgment on the passed information is independent of the platform and configuration of the end user. The standard also gives flexibility to use any authentication server of choice without any changes at the supplicant.

2.4.1.3 IEEE 802.1X adaptation on an IEEE 802.11 network

The EAP is built around the challenge-response communication model. The main types of messages involved in the communication are EAP Request, EAP Response, EAP Success and EAP Failure. Figure 2.8 presents how 802.1X facilitates a framework for user authentication over wireless LANs.
The adaptation to the wireless environment, as illustrated in Figure 2.8, required the existence of a “network port” in the Authenticator. The solution was simple. IEEE defined the association between a wireless node and the access point to happen via a “logical” or “uncontrolled” port for the interpretation in the IEEE 802.1X standard [10]. Thus, first the IEEE 802.11 association takes place prior to the IEEE 802.1X negotiation begins. After successful association the IEEE 802.1X authentication process successfully proceeds via this so called uncontrolled port. Until such time the access point filters and blocks non IEEE 802.1X traffic. In the mean time, the authenticator (access point) facilitates full network access for previously authenticated ports through a second port called “controlled port.” Therefore, it is said that the IEEE 802.1X authenticator is designed with a “dual port authentication” model.

2.3.1.4 Identified Security Limitations
In spite of the fact that IEEE 802.1x framework was accepted by the industry over WEP, it had its own share of problems. A recent publication claims that the above standard is vulnerable of a man-in-the-middle attack and a possible session hijack [16]. The authors of the above
technical report argue that the nature of the one-way authentication algorithm of the IEEE 802.1x standard gives rise to a possible man-in-the-middle attack. It further demonstrates its susceptibility of a session hijack due to the lack of communication and loose cupping between the RSN state machines and the IEEE 802.1x state machines. It is proposed that such attacks may be eliminated by introducing per packet authenticating and integrity checking schema in the algorithm. Among other suggestions are the addition of an EAP authenticator attribute to EAPOL and an introduction of a possible peer-to-peer authentication model.

Nevertheless, it is important to mention that since the IEEE 802.1x was originally designed for stations that are permanently associated to a port, when applied to an 802.11 network, additional issues such as how to transfer the association and authentication information from one port to another had to be considered. Disappointingly, none of the previously mentioned has been addressed in the 802.1X standard.

2.4.2 The 802.11i Standard

The IEEE 802.11 Work Group instituted a Task Group i to incorporate a new generation of security for the 802.11 standard. As previously mentioned, the new IEEE 802.11i standard was designed around the IEEE 802.1x authentication and ratified on June 24, 2004 [6]. It defines a new type of a wireless network called Robust Security Network (RSN).

However, to be fully RSN-capable most wireless networking equipment requires to be replaced by special RSN-capable products. This was not very welcoming news for many wireless networking users. Thus IEEE 802.11i defined a transitional security network (TSN) in which both RSN and WEP systems could operate simultaneously. The idea behind this was to allow most users to up-grade their existing pre-RSN equipment over a period of time and to provide with a better security solution than WEP. Hence, the Wi-Fi Alliance developed the Temporal Key Integrity Protocol (TKIP) based on the RSN. This subset of RSN is called Wi-Fi Protected Access (WPA).

2.3.2.1 Wi-Fi Protected Access (WPA)

The aim of introducing WPA is to fix potential security gaps in legacy devices, mainly via driver and software upgrades. WPA incorporates TKIP, which addresses the deficiencies of
Chapter 2 – Wireless LAN Security: Research Trends and Issues

keys used with WEP. The TKIP includes a new key derivation and rotation algorithm to ensure higher security. A message integrity check (MIC) is also added to prevent packet forgeries. Despite all the advantages, some users may face difficulties since WPA is not fully backward compatible with some legacy devices and operating systems. Moreover, due to high resource consumption, WPA may degrade the performance of a WLAN device unless it has specific hardware that will run and accelerate the protocol.

2.3.2.2 Robust Security Network (RSN)
RSN is based on dynamic negotiation of authentication and encryption algorithms. The proposed authentication schema is based on IEEE 802.1x framework and Extensible Authentication Protocol (EAP). The key rotation of TKIP is replaced by a new encryption algorithm Advanced Encryption Standard (AES). Dynamic negotiation, IEEE 802.1x, EAP and AES make RSN a state of the art technology in securing wireless networks making it relatively stronger than WEP or WPA. However, RSN requires the wireless devices to be equipped with necessary hardware to accelerate the algorithms to provide acceptable levels of performance.

2.4.3 The VPN Security Solution
A Virtual Private Network (VPN) is a simple solution to achieve secure private communications over the use of a public network infrastructure such as the Internet [17]. It is also possible to similarly deploy VPNs on a wireless network infrastructure to secure transmission between wireless clients and their wired enterprise network. This method has been warmly accepted by the academia and industry as an alternative to securing WLANs. It involves in the creation of a VPN tunnel through the use of a tunneling protocol that encrypts traffic over the WLAN.

2.5 VPN Overview
In the recent years, the term Virtual Private Network (VPN) has become a famous “buzz word”. Amongst all the hype that surrounds this technology, its existence dates back to the early 80s with the development VPN services over X.25 [18]. As the technology migrated into an IP environment, many forms of VPN services and implementations came into effect. For all such VPN implementations, high scalability, flexibility and cost effectiveness are common
advantages. Interestingly, with the recent advancements and widespread global connectivity of the Internet and other WAN backbone networks VPN adaptations became easier and affordable than ever.

VPNs can be formally defined as a communication environment constructed by controlled segmentation of a shared communications infrastructure to emulate the characteristics of a private network [19]. More specifically explaining, a Virtual Private Network is a simple solution to achieve secure private communication over the use of a public network infrastructure such as the Internet [17]. It essentially provides interconnectivity among multiple entities and therefore known as a “Network”. The term “Private” emphasizes the capability of sharing the available network services and resources among an authorized group of users controlled by different levels of access control. It further indicates that the network traffic related to this network is private and independent of any external traffic flow-taking place in the public network infrastructure. Although the underlying network shares the resources of a public network, from the user perspective VPN looks private and consist of a independently administered virtual topology, hence “Virtual” [19].

By and large, the primary function of a VPN is to protect the data from disclosure during transmission over any given network path from point A to point B. Therefore the VPN must ensure sufficient mechanisms to guarantee confidentiality, authentication, integrity, non-repudiation and access control to the data traversing via public network segments. Amongst the above mentioned security features, a VPN must also be designed with features such as high scalability, performance, reliability, usability, ease of management, interoperability and multi protocol support [20].

2.5.1 Types of VPN Services

Deployment of the VPN technology in the correct manner can result in enhancing the organization to achieve its business goals while increasing opportunities and revenue. Some common uses of VPN technology are as follows [20]:

- Connecting branches within an organization, spanned over different physical locations, via a public network (such as the Internet).
- Enable branches of the same organization to securely interchange information over a shared corporate backbone.
• Connecting to business partners to enhance business opportunities.
• Efficient and cost effective remote access service for mobile employees via a public network infrastructure.
• Connection of confidential systems together to allow secure communications.

The above scenarios can be mainly categorized into three basic types. These three types are referred to as site-to-site intranet VPNs, extranet VPNs and remote access VPNs [21].

2.5.1.1 Site-to-Site Intranet VPNs
This VPN implementation helps to connect geographically distributed LANs over a shared network infrastructure. These distributed LANs may belong to the same company or a group of companies under one administration. Figure 2.9 shows such VPN implementation where VPN A connects location 1, 2, and 3; VPN B connects location 1 and 3. Both VPN A and B are implemented over a shared medium. However, virtually isolated and administered as two networks. This shared medium could be the Internet, which is most widely used. Alternatively, public networks such as ISDN, Frame Relay and ATM can carry mixed data types including voice, video and data [5].

Figure 2.9: Intranet VPN Services adopted from [19].
2.5.1.2 Extranet VPNs

This is a VPN Service provided to external vendor, suppliers or customers to connect and access specific areas of a company’s intranet over a shared network infrastructure.

![Diagram of Extranet VPN Services](image)

Figure 2.10: Extranet VPN Services adopted from [19].

Figure 2.10 shows such connection. The Authentication Server authenticates the user and if authenticated as an external entity, it will only be allowed to access the special area, Demilitarized Zone. However, if it is an internal user full access to the company intranet will be granted. Further, as shown in Figure 6 there may be remote access connections by mobile suppliers, etc. Having such extranet VPN connectivity to a company network opens doors to explore the possibilities of e-commerce, online inventory management and even Electronic Data Interchange (EDI).

2.5.1.3 Remote Access (Dial-up) VPNs

As shown in Figure 2.11, a Remote Access VPN facilitates mobile employees to connect to the company intranet from remote locations using mobile computing equipment such as a notebook computer or a pocket pc.
2.5.2 VPN Protocols

There are two basic types of VPN implementations, those that operate at layer 3 (network layer) and layer 2 (data link layer) of the OSI Reference Model. A typical example of a layer 2 VPN is a VPN established by configuring permanent virtual circuits (PVCs) over a public frame relay network. On the other hand, a layer 3 VPN operates on public TCP/IP networks, the Internet. In the modern age, layer 3 VPNs have become the most popular VPN implementation for obvious reasons. Therefore, the following discussion on VPN protocols primarily concentrates on VPN implementations related to the Internet Protocol and layer 3 networking.

As previously mentioned, a typical VPN implementation involves a massive amount of protocols dedicated for various tasks such as tunneling, connection establishment, encryption, authentication and access control, to name a few. Hence, in most cases it is a suit of protocols that work with each other that finally provide a full range of services of a secure VPN. Amongst all the above services, the protocol which implements the tunneling mechanism plays a vital role in the overall performance of the VPN. Tunneling is in fact a kind of encapsulation, i.e., a protocol (X) is encapsulated within another protocol (Y) when transporting, so the
protocol X is transparent to the public network [22]. The three common protocols used for IP
tunneling are the Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol
(L2TP) and IP Security (IPSec) [23]. The PPTP and L2TP are commonly deployed in
organizations for remote access. These tunneling protocols allow authorized clients to access
internal hosts via public networks such as the Internet. However, neither of these protocols are
capable of providing packet level protection to the tunneled information [22]. This requires
IPSec to be used in conjunction or as an alternative to PPTP or L2TP when data confidentiality
becomes a priority [20]. IPSec on the other hand, is the only tunneling protocol that allows the
user to establish an encrypted tunnel between two parties. IPSec in reality is a collection of
protocols and also the most widely deployed VPN standard for wired as well as wireless
networking infrastructures. This automatically makes IPSec the chosen VPN protocol of this
research.

2.5.2.1 IPSec
IPSec is a standard that has been established by the Internet Engineering Task Force (IETF) to
ensure the privacy and integrity of the IP packets being transferred in a public network [24].
IPSec is a suite of protocols that facilitates end-to-end security by providing confidentiality,
privacy, data integrity and authentication at the network layer [25]. These services are
independent of the protocols operating on the above layers, transport and application, and fully
transparent to end users.

The two main protocols defined in IPSec are Authentication Header (AH) [26] and
Encapsulating Security Payload (ESP) [27]. These define two special types of headers that are
added to the IP datagram, which carries cryptographically protected data. The AH ensures the
integrity and authenticity of the IP payload (even the entire IP datagram). However, it does not
provide confidentiality to the data. The ESP provides and ensures the confidentiality of the IP
payload (even the entire IP datagram) and may optionally provide authenticity and integrity.
Hence, ESP is used by IPSec for tunneling in VPNs.

As mentioned previously, tunneling hides the packets from the shared public network,
between the start and end points of the VPN. IPSec achieves this by hiding the original header
of the data packet and appending it with an additional IP header at the network layer as shown
in Figure 2.12. The destination address of this appended IP header is the terminating point of
the tunnel or the end point of the VPN. The modified packets are routed accordingly by the underlying public network to its new destination address. At the destination, which is the terminating point of the VPN, the additional header is stripped off and the original packet it recreated.

![Diagram](image)

*Figure 2.12: The concept of VPN tunneling*

There are some specific advantages of this mechanism of tunneling. It helps to route multiple protocols over a shared medium. Tunneling also lets the VPN have a totally different addressing mechanism from the shared public network. However it is worth noting that at the time of connection to the public network the addresses of the VPN packets may need to be translated.

The encryption algorithms used by ESP are Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Blowfish and RC5 [27]. It also provides facilities to adopt other similar symmetric key algorithms. IPSec also defines a protocol for session encryption key negotiation, exchange, and management as a part of its documentation called the Internet Key Exchange (IKE) [28]. IKE is the main protocol that facilitates this authentication process by preventing the user’s private key from being exposed. Once this step is successfully completed will the policy information be delivered to the user’s machine to set up the VPN tunnel.

IPSec support strong encryption to secure data which is tunneled. The encryption algorithms supported by ESP [8] are 168-bit triple Data Encryption Standard (3DES), International Data Encryption Algorithm (IDEA), triple IDEA, Blowfish and RC5. It also provides facilities to adopt other similar symmetric key algorithms.
2.5.2.2 IPSec Issues

The following issues regarding IPSec need to be taken into consideration [25]:

- Interoperability: Many implementations are currently incompatible mainly due to imprecise standards.
- Network Address Translation (NAT): When operating under transport mode, the NAT function fails. This is due to the authentication failure due to the changing of the IP header.
- Dynamic IP Address Negotiation: IPSec clients are unable to negotiate dynamic IP addresses.
- Legal and Regulatory Issues: Encryption may still be considered by some countries as munitions and some ISPs may block IPSec traffic as a policy.
- Quality of Service (QoS): With ESP encryption on the header and payload, the QoS classification may no longer be available for certain IP datagrams.

2.6 VPNs in a WLAN Environment

In comparing the three basic types of VPNs described under section 2.4.1, it is obvious that the remote access VPN would be the most appropriate method in securing wireless transmissions. This is mainly because the remote access VPN provides data protection from a client to the VPN server. Thus, a wireless client configured with a suitable VPN tunneling protocol can securely connect through the air to an access point and over the wired infrastructure to a VPN server. The setup requires the wireless access point to be configured with open access and no WEP encryption leaving the VPN to handle total security. The authentication and encryption over the wireless network are also provided by the VPN.

Mobile users can use wireless VPNs to securely access a corporate network from remote locations. It also ensures data privacy over an unsecured public network preventing a potential attacker from analyzing the wireless transmission. Furthermore, this approach enables centralized administration for network managers with less administrative overheads unlike MAC address filtering or WEP. Not to mention of its relatively high scalability. For organizations that already have VPN hardware products or software packages, it is a matter of extending the existing solution to the wireless network segment. Hence for some network
managers and administrators VPN became a single back end security technology implemented for protecting both wired and wireless communications.

Figure 2.13: VPN Security for IEEE 802.11 WLANs

As illustrated in Figure 2.13, VPN security is applied between pairs of end points, which are connected via untrusted (public) networks. The untrusted network can either be the Internet, an unsecured wireless network or a combination of both. In most cases, the VPN client is the device that initiates the connection to a VPN server or a gateway. A VPN client can be either an individual computer requesting remote access or a router requesting the services of another peer entity. Likewise, an individual computer or a router can act as a gateway depending on the configuration [29].
2.7 Current and Future Research Trends

In any wireless environment, maximum security requires both layer 2 and layer 3 of the OSI model to be secured. Despite the fact that a VPN plays an important role in providing end-to-end security, it may not be sufficient in fulfilling the total security requirement for a wireless networking environment under most circumstances. Layer 3 VPN solutions have an inherent security flaw when implemented in wireless networks. Since wireless networks operate a broadcast domain at Layer 2 of the OSI stack, access points and wireless bridges may be open to attack. Implementation of a port based access control mechanism based on the use of IEEE 802.1X framework may be able to eliminate such vulnerabilities of Layer 2 [30].

Another security vulnerability with such VPN-based wireless LAN deployments is what is referred to as the hidden wireless router vulnerability. There remains a possibility for wireless LAN enabled clients with dual two network interface cards to by pass the VPN by exploiting the features available in operating systems like Windows and Linux [31]. Research shows that this is becoming an increasing threat and techniques for detection and prevention must be in place.

Amongst other research issues relating to VPNs, remains the issue of privacy [32]. The issue of privacy is interpreted in two different ways when applied on VPNs. One way is to achieve confidentiality by using cryptographic techniques to obscure the content of the communication. The other way of achieving privacy is by reserving a dedicated communication channel over a publicly shared infrastructure. This indicates that many techniques must be looked into before constructing an appropriate VPN solution to a given scenario.

The quest for research into the enhancement of VPN security has resulted in reduced performance, high network overhead, and high administrative overheads. Therefore, much work is done with respect to performance enhancement and evaluation of wired and wireless VPNs. Due to the inherent weaknesses of the wireless media itself, high priority is given to wireless VPN implementations. Various amounts of research have taken place in the investigation and evaluation of performance in wired and wireless VPNs. This evaluation of performance involves in measuring and monitoring various Quality of Service (QoS) parameters. Throughput, packet loss, delay and jitter are some of the widely investigated QoS parameters. The behavior of these QoS parameters is investigated against varying conditions of
the transported data traffic (i.e., TCP, UDP, FTP, HTTP, etc...), VPN tunneling protocols (IPSec, L2TP, PPTP, etc...), and authentication and encryption algorithms (AH, ESP, etc...) over different hardware and software platforms.

One such research publication investigates the impact on a router’s throughput performance over a wired VPN when using various services and hash/encryption algorithms provided by IPSec on a vLinux kernel [33]. In this paper, the researchers compare the effects on throughput for AH and ESP using the same authentication algorithms. It also compares difference of the throughputs for HTTP and FTP traffic over an IPSec VPN. A similar publication investigates the effects of video and audio streaming on performances of a wired VPN implementation [34]. This investigation reports an analysis and evaluation on throughput, channel utilization, and gateway utilization of a wired VPN on two different platforms; Windows 2000 and Novell Netware. The authors have focused on issues related to QoS and delivery of multimedia data over an IPSec VPN. This paper concludes by emphasizing that network performance and other related issues are affected by the implementation of encryption tools (i.e., software or hardware) and various types of platforms (i.e., Windows 2000, Novell Netware, etc...).

As the VPNs implemented in software became an economic and accessible alternative to hardware VPNs, its impact on performance remained a question. The research publication on the performance evaluation of software VPNs claims that they may have a significant impact on throughput performance, producing high CPU usage and limiting network throughput [35]. The authors’ further state that an Ethernet link of 100 Mbps can degrade in more than 65% while the CPU usage can reach 97%, when software based strong encryption is enabled. Work has also been done in areas on how VPN performance can be improved. One such example is the research paper on how data compression can elevate the performance issue in a VPN implemented with the IPSec protocol [36].

As the VPN platform changes from wired to wireless, all the above mentioned issues remain the same. In fact, the impairments of the wireless channel further reduce the performance of a wireless VPN. The performance issues on a secure wireless LAN based on secure IPSec VPN tunneling protocol is analysed by [17]. This paper investigates the TCP and UDP performance to determine the effects of IPSec service on the wireless VPN. The experimental platform is based on Linux and FreeS/WAN and PGP certification is used to
provide secure public key management. The main performance parameters investigated are throughput and packet loss for TCP and UDP. A similar paper investigates the IPSec overhead in wireless networks for web and email applications [37]. This paper provides various test results for both wired and wireless links for combinations of AH and ESP protocols. The results mainly emphasize on how network load and transfer time vary against combinations of AH and ESP for email and web applications.

By and large, much contribution has been made to the field in identifying the overheads of different IPSec configurations in both wired and wireless environments. It also helps by providing a practical guideline for network designers and application developers to choose the optimal parameters for a given VPN setup. However, many parts of the puzzle are still missing. Amongst these are QoS parameter measurements such as CPU utilization, delay and jitter are yet to be established. Details on how the QoS parameters behave with varying payload data sizes, packet generation rates, increasing number of tunnels also need to be investigated. Other vital information include how the geographical distance, incorporation of a designated IPSec gateway for encryption and authentication, multi platform and subnet routes may effect the tunnel’s over all performance. The aim of this thesis is to make a contribution by investigating and analyzing such QoS measures for different types of wireless VPN setups. The next chapter describes the setting up of various experimental platforms and detailed procedures for data collection. Following which are the chapters on the analysis of these experimental data.
Chapter 3 – Research Methodology

Chapter 3

Research Methodology

This chapter presents a detailed description of the experimental platforms, setups and methodologies used for data collection. The objective behind the collection of such data is to obtain a comprehensive set of measurements for the analysis and evaluation of the performance of a Virtual Private Network (VPN) implementation over an IEEE 802.11b wireless infrastructure under various scenarios. The first section presents the basic performance metrics and measures considered for this study. Following this is a section providing a detailed description of all equipment, techniques and approaches used in the setup of these experimental platforms. The final section of this chapter takes the discussion further by stating the detailed procedures through which the specific experiments are performed. It also provides the collected data of various metrics and measures in a convenient tabular format.

3.1 Performance Metrics

A comprehensive set of performance measures and metrics relating to wireless VPNs is considered. These measures include the application throughput, packet loss, round-trip delay, jitter, and the CPU utilisation. A detailed description of these performance parameters is as follows:

Throughput: The measured total throughput is the average amount of data payload transmitted and received over a sampling period between two points. The throughput metric used is Mbps.

Packet Loss: This examines at the average per tunnel packet loss. Three different types of packet loss measures are taken at various instances. The first is the average per tunnel packet loss in transmission (outbound) and the next is the per tunnel packet loss in receiving (inbound). The final packet loss measure is the average per tunnel-round trip (total) packet loss. It may be obvious that with the first two the third can be easily constructed. However, having monitored the behaviour of these
three types of packet loss greatly helps in formulating various relationships at the analysis stage.

Round-trip Delay: The average time (delay) taken by a packet to complete one full trip from source to destination and back.

Jitter: This is the mean variation of delays on packets received. The delay considered for this measure is the round-trip delay. Thus, the measure jitter considered under this study specifically corresponds to the mean two-way variation.

CPU Utilisation: The study of this metric clearly shows the behaviour of the CPU as the numbers of simultaneously functioning IPSec VPN tunnels are increased. It also helps to understand the changes in the behaviour of the tunnel/s when the CPU reaches a maximum.

3.2 Experimental Setup

The basic experimental platform used for the research is primarily based on an IEEE 802.11b 2.4 GHz WLAN with networked clients operating in the Windows 2000 Professional operating system. The creation and administration of the VPN tunnels is facilitated by the use of the standard IPSec policy snap-in tool of the Windows 2000 Professional operating system.

3.2.1 Hardware

The first round of experiments involves the use of two desktop PCs. The relevant details of the hardware configurations of these two PCs are specified in Table 3.1. The selection of nodes is in line with current practical implementations. That is, a relatively slower CPU is assigned to the wireless client. As a convenient naming convention, these two nodes are referred to as wired client and wireless client throughout this thesis.

<table>
<thead>
<tr>
<th>Node Type</th>
<th>CPU</th>
<th>Memory</th>
<th>Adapter</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Client</td>
<td>AMD K6 (300MHz)</td>
<td>3D 128MB</td>
<td>Dlink AirPlus (11 Mbps)</td>
<td>Windows Professional 2000</td>
</tr>
<tr>
<td>Wired Client</td>
<td>AMD Athlon XP 2100+ (1.7GHz)</td>
<td>512MB</td>
<td>Intel[R] PRO_100 S (100 Mbps)</td>
<td>Windows Professional 2000</td>
</tr>
</tbody>
</table>

Table 3.1: Hardware Configuration
Chapter 3 – Research Methodology

![Diagram showing the basic hardware setup]

**Figure 3.1: The Basic Hardware Setup.**

Both *wireless* client and *wired* client are connected to the 137.154.148.0/24 School of Computing & IT (SCIT) subnet at the UWS Penrith Campus. The wired client is also connected to the above subnet via its 100 Mbps Fast Ethernet interface card. There also exists an IEEE 802.11b Access Point (AP), which is connected to the same subnet. The wireless client establishes an association with this AP via its IEEE 802.11b WLAN interface card forming an infrastructure Basic Service Set (BSS). Thus, the wireless client and wired client are nodes of a single subnet sharing the same IP address range. The distance between the AP
and the wireless client is around 3 metres. Figure 3.1 provides a detailed illustration of the abovementioned setup. At the time of the experimentation, extra care is taken to ensure no other WLANs are operating on the same channel within the vicinity of the setup.

### 3.2.2 Software

For the purpose of network traffic generation, capturing and recording, the fully licensed ZTI Telecom’s LanTraffic V2 is used. LanTraffic V2 is capable of generating a certain number of packets with a specified payload data size in either TCP or UDP to a designated destination. It is capable of handling up to 16 simultaneous outgoing or incoming connections at any given instance. Each connection can be specifically monitored by LanTraffic V2 by capturing and recording TCP or UDP traffic at a designated port number. LanTraffic V2 is installed on both wireless and wired clients. LanTraffic V2 on the wireless client is configured for outgoing traffic generation and monitoring. On the other hand, LanTraffic V2 on the wired client is configured for receiving and echoing back of the incoming traffic to the source (the wireless client). A detailed description on the configuration details of LanTraffic V2 will follow in the Experiment and Output Description section. Ethereal is used as the protocol analysing tool for the series of experiments.

Both wireless and wired clients are operating on Microsoft Windows 2000 Professional SP2, updated with the latest security patches and vendor-specific interface drivers. Apart from the third-party traffic generation and monitoring tools, wherever possible, standard tools provided by the operating system are used. The first of these is the IPSec policy snap-in tool that is used for the creation and administration of the VPN tunnels. IPSec client policies are configured for both wired and wireless clients. The Windows 2000 IP Security Monitor is used for monitoring the IPSec Security Associations. This tool helps to monitor the statistics of all IPSec sessions; such as the encrypted and authenticated traffic sent and received, bad Security Parameter Index (SPI) packets, packets not decrypted and not authenticated, the total number of key additions and ISAKMP/Oakley key exchange statistics. Finally, the Windows 2000 Performance Monitoring utility is used for measuring the CPU performance for the wireless client.
3.2.3 Case 1: Setup of a Single Wireless VPN

![Diagram of a Single Wireless VPN setup]

Figure 3.2: Setup of a Single Wireless VPN.

This section provides a detailed description of the very first experimental setup. It is also worth noting that this is the setup used in establishing the baseline measures. The basic hardware arrangement for Case 1 is illustrated by Figure 3.2. The construction of the single IPSec VPN tunnel, operating on transport mode, is carried out using the IPSec policy snap-in tool provided by the Windows 2000 Professional operating system. The two IPSec policies defined for the wired and wireless clients have pre-shared key authentication. The session key settings are set to generate a new key every 300 seconds. In the IPSec Filter List properties of the wireless client, a new outbound filter is created, specifying it as the source and the wired client’s IP address as the destination address. Then the automatic mirroring process is selected for configuring of the inbound filter. Thus the created inbound filter is essentially the mirror image of the previously defined outbound process. UDP is selected as the choice of protocol specifying the source port as “Any” and the destination port as 2001. Under the Filter Action Properties the IPSec Policy is configured to always Negotiate Security, not to accept any unsecured communication and to always respond using IP Security. It is further specified not to allow communications with non-IPSec-aware computers. Session key Perfect Forward Secrecy (PFS) is enabled to ensure the condition under which the compromise of a session key after a given session does not cause the compromise of any earlier session. The destination IPSec policy (that is, for the wired client) is configured similarly, except for the reversing of the UDP
source and destination port numbers. Table 3.2 summarises the specifications of the two IPSec policies.

<table>
<thead>
<tr>
<th>Tunnel End</th>
<th>IPSec Mode</th>
<th>Encryption Algorithm</th>
<th>Integrity Check Algorithm</th>
<th>Authentication Method</th>
<th>Session Key Generation</th>
<th>Filtered Protocols/Port Nos.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired Client</td>
<td>ESP-Transport Mode</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Pre-Shared Key</td>
<td>300 Sec</td>
<td>UDP/ SP: Any DP: 2001</td>
</tr>
<tr>
<td>Wireless Client</td>
<td>ESP-Transport Mode</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Pre-Shared Key</td>
<td>300 Sec</td>
<td>UDP SP: 2001 DP: Any</td>
</tr>
</tbody>
</table>

### 3.2.4 Case 2: Setup of Multiple Wireless VPNs

![Diagram showing setup of multiple wireless VPNs](image)

This section provides a detailed description of the second experimental setup. As illustrated by Figure 3.3, the basic hardware arrangement for Case 2 is very much the same as for the previous case. However, the difference remains in the number of IPSec VPN tunnels. The construction of these multiple IPSec VPNs, operating on transport mode, are carried out using
the IPSec policy snap-in tool provided by the Windows 2000 Professional operating system. In the IPSec Filter List properties of the wireless client, three outbound filters are created, specifying it as the source and the wired client’s IP address as the destination address. Then the automatic mirroring process is selected for configuring the three inbound filters. Thus the created inbound filters are essentially the mirror images of the previously defined outbound process. The three tunnels have UDP as their choice of protocol with the source ports for all three tunnels as “Any” and the destination ports as 2001, 2002 and 2003 respectively. All the remaining properties of the IPSec policy are similar to the specifications of case 1. The destination IPSec policy (that is, for the wired client) is configured similarly, except for the reversing of the UDP source and destination port numbers. Table 3.3 summarises the specifications of the IPSec policies.

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>Tunnel End</th>
<th>IPSec Mode</th>
<th>Encryption Algorithm</th>
<th>Integrity Check Algorithm</th>
<th>Authentication Method</th>
<th>Session Key Generation</th>
<th>Filtered Protocols/Port Nos.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel 1</td>
<td>Wired Client</td>
<td>ESP-Transport Mode</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Pre-Shared Key</td>
<td>300 Sec</td>
<td>UDP/SP: Any DP: 2001</td>
</tr>
<tr>
<td></td>
<td>Wireless Client</td>
<td>ESP-Transport Mode</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Pre-Shared Key</td>
<td>300 Sec</td>
<td>UDP SP: 2001 DP: Any</td>
</tr>
<tr>
<td>Tunnel 2</td>
<td>Wired Client</td>
<td>ESP-Transport Mode</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Pre-Shared Key</td>
<td>300 Sec</td>
<td>UDP/SP: Any DP: 2002</td>
</tr>
<tr>
<td></td>
<td>Wireless Client</td>
<td>ESP-Transport Mode</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Pre-Shared Key</td>
<td>300 Sec</td>
<td>UDP SP: 2002 DP: Any</td>
</tr>
<tr>
<td>Tunnel 3</td>
<td>Wired Client</td>
<td>ESP-Transport Mode</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Pre-Shared Key</td>
<td>300 Sec</td>
<td>UDP/SP: Any DP: 2003</td>
</tr>
<tr>
<td></td>
<td>Wireless Client</td>
<td>ESP-Transport Mode</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Pre-Shared Key</td>
<td>300 Sec</td>
<td>UDP SP: 2003 DP: Any</td>
</tr>
</tbody>
</table>
3.2.5 Case 3: Setup of a Site-to-Site VPN
This section provides a detailed description of the third and final experimental setup. The basic hardware arrangement for Case 3 is very much different from the previous cases. In fact, it can be conceptually categorised as a site-to-site VPN spanning over multiple subnets. This arrangement facilitates secure communications between two geographically distant private networks in a campus wide intranet. The two geographically distant locations selected for this experiment are located at the Penrith Campus and the Parramatta Campus.

![Diagram of Site-to-Site VPN Tunnel]

Figure 3.4: Setup of a Site-to-Site VPN Tunnel.

A detailed illustration of the hardware setup is presented in Figure 3.4. The actual IPSec VPN tunnel is operated between the two designated VPN gateways/routers sitting at the two campuses. The private network behind the Parramatta VPN gateway is an IEEE 802.11 WLAN
operating on Ad Hoc mode. The IP address space shared by this subnet is 192.168.10.0/24. Similarly, a wireless mesh network sits behind the Penrith VPN gateway, sharing the private subnet address space of 192.168.0.0/24. The traffic originating from private subnet 192.168.10.0/24 (say) to private subnet 192.168.0.0/24 (say) is tunnelled by the established IPSec VPN. Since routing to and from all private addresses is fully restricted by the UWS routers, the IPSec VPN must be specifically configured in tunnel mode.

The construction of the IPSec VPN tunnel between the two gateways is carried out using the IPSec policy snap-in tool provided by the Windows 2000 Professional operating system. In the IPSec Filter List properties of the Penrith VPN gateway, one outbound filter is created specifying the private subnet 192.168.0.0/24 as the source and the private subnet 192.168.10.0/24 as the destination address. In addition, the relevant tunnel end-point for this filter is 137.154.176.53. The inbound filter is created separately by reversing the source and destination subnet addresses and the corresponding tunnel end-point as 137.154.148.118. No restrictions on the type of traffic belonging to specific protocols or port numbers are made. All the remaining properties of the IPSec policy are similar to the specifications of Table 3.1. The IPSec policy for the Parramatta VPN gateway is configured similarly, except for the reversing of the source and destination subnets and tunnel end-points. Table 3.4 summarises the specifications of the IPSec policy settings.

Table 3.4: IPSec Policy Configuration for a Site-to-Site VPN

<table>
<thead>
<tr>
<th>VPN Gateway</th>
<th>IP Filter</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Tunnel endpoint</th>
<th>IPSec Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penrith</td>
<td>Outbound</td>
<td>192.168.0.0/24</td>
<td>192.168.10.0/24</td>
<td>137.154.176.53</td>
<td>ESP-Tunnel Mode</td>
</tr>
<tr>
<td></td>
<td>Inbound</td>
<td>192.168.10.0/24</td>
<td>192.168.0.0/24</td>
<td>137.154.148.118</td>
<td>ESP-Tunnel Mode</td>
</tr>
<tr>
<td>Parramatta</td>
<td>Outbound</td>
<td>192.168.10.0/24</td>
<td>192.168.0.0/24</td>
<td>137.154.148.118</td>
<td>ESP-Tunnel Mode</td>
</tr>
<tr>
<td></td>
<td>Inbound</td>
<td>192.168.0.0/24</td>
<td>192.168.10.0/24</td>
<td>137.154.176.53</td>
<td>ESP-Tunnel Mode</td>
</tr>
</tbody>
</table>
3.3 **Experimentation and Data Collection**

This section provides a detailed description on the experimentation performed on the previously described platforms.

3.3.1 **Establishment of Baseline Performance Measurements**

Establishment of a baseline performance measure is considered to be highly important. This task is accomplished over the setup described under section 3.2.3. LanTraffic V2 network traffic generator program on the *wireless* client (the source) is configured to generate a specific stream of UDP traffic (as specified in section 3.2.3) to the *wired* client (the destination). In the meantime, LanTraffic V2 at the *wired* client (the destination) is set to “start receiving traffic” mode for capturing this special incoming traffic transmitted from the *wireless* client (the source). LanTraffic V2 at the *wired* client (the destination) captures the incoming UDP packet flow and echoes them back to the source. Figure 3.2 shows the flow of the abovementioned UDP traffic from the source to the destination and back. A detailed description on how the traffic flow is controlled is as follows. At a given instance, the source generates 10000 packets of UDP traffic with a fixed repeating packet content of 5A Hex value and a fixed inter-packet delay of 1 ms. The starting UDP payload size is 50 bytes and the payload size is increased step-by-step up to a maximum of 1600 bytes to reach higher traffic levels. Next, the entire experiment is repeated for a relatively lower UDP flow with 5 ms inter-packet delay.

The data collection is facilitated via the automatic log file generation option of LanTraffic V2. Prior to the start of the UDP traffic flow, the automatic log file generation option in LanTraffic V2 is started at the source and destination. These auto-generated log files capture the total transmission throughput, the total UDP packets sent and received, jitter and the average round-trip delay encountered by a UDP datagram to complete a trip from source to destination and back. (Note: the throughput displayed by LanTraffic V2 corresponds to the UDP payload data on the sampling period (5 Sec by default); hence the obtained throughput value is “application” throughput.). Since LanTraffic V2 does not have a CPU Utilisation measuring facility, the Windows 2000 performance monitor is used to measure the percentage of CPU Utilisation at the *wireless* client at each UDP traffic level. Each reading is taken at least five times and the mean value of this sample is taken to increase the accuracy of the readings.
Hence note that all measures such as Throughput, CPU Utilisation, Packet Loss and Round-trip Delay correspond to an average value.

Table 3.5 and Table 3.6 provide the baseline readings obtained at the source, for UDP flows with 1 ms and 5 ms inter-packet generation gap respectively. The average total throughput (column 5) at the source is calculated by adding up the average transmission throughput (column 2) and the average receiving throughput (column 3). The two packet-loss measures taken by LanTraffic V2 at the source are the average packet loss in transmission (column 6) and the average total packet loss (column 7). The average packet loss in receiving (column 8) is computed by subtracting the total packet loss from the packet loss in transmission.

### Table 3.5: Baseline Readings for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>Kbps</td>
<td>Kbps</td>
<td>Kbps</td>
<td>Mbps</td>
<td>%</td>
<td>%</td>
<td>ms</td>
<td>ms</td>
<td>%</td>
</tr>
<tr>
<td>25</td>
<td>271.00</td>
<td>183.00</td>
<td>454.00</td>
<td>0.45</td>
<td>33</td>
<td>49</td>
<td>16</td>
<td>145</td>
<td>0</td>
</tr>
<tr>
<td>50</td>
<td>345.00</td>
<td>302.00</td>
<td>647.00</td>
<td>0.65</td>
<td>34</td>
<td>50</td>
<td>16</td>
<td>146</td>
<td>1</td>
</tr>
<tr>
<td>75</td>
<td>464.00</td>
<td>335.00</td>
<td>799.00</td>
<td>0.80</td>
<td>0</td>
<td>17</td>
<td>17</td>
<td>201</td>
<td>56</td>
</tr>
<tr>
<td>100</td>
<td>514.00</td>
<td>457.07</td>
<td>971.07</td>
<td>0.97</td>
<td>0</td>
<td>11</td>
<td>11</td>
<td>141</td>
<td>-60</td>
</tr>
<tr>
<td>125</td>
<td>575.00</td>
<td>573.00</td>
<td>1148.00</td>
<td>1.15</td>
<td>0</td>
<td>11</td>
<td>11</td>
<td>121</td>
<td>-20</td>
</tr>
<tr>
<td>150</td>
<td>680.00</td>
<td>678.00</td>
<td>1358.00</td>
<td>1.36</td>
<td>1</td>
<td>12</td>
<td>11</td>
<td>102</td>
<td>-19</td>
</tr>
<tr>
<td>175</td>
<td>775.00</td>
<td>772.00</td>
<td>1547.00</td>
<td>1.55</td>
<td>2</td>
<td>12</td>
<td>11</td>
<td>91</td>
<td>-11</td>
</tr>
<tr>
<td>200</td>
<td>912.13</td>
<td>818.31</td>
<td>1730.44</td>
<td>1.73</td>
<td>3</td>
<td>14</td>
<td>11</td>
<td>85</td>
<td>-6</td>
</tr>
<tr>
<td>400</td>
<td>1766.32</td>
<td>1240.62</td>
<td>3006.94</td>
<td>3.01</td>
<td>19</td>
<td>33</td>
<td>14</td>
<td>64</td>
<td>-21</td>
</tr>
<tr>
<td>600</td>
<td>2639.24</td>
<td>1300.77</td>
<td>3940.01</td>
<td>3.94</td>
<td>36</td>
<td>51</td>
<td>15</td>
<td>56</td>
<td>-8</td>
</tr>
<tr>
<td>800</td>
<td>3298.11</td>
<td>1215.38</td>
<td>4513.49</td>
<td>4.51</td>
<td>46</td>
<td>63</td>
<td>17</td>
<td>56</td>
<td>0</td>
</tr>
<tr>
<td>1000</td>
<td>3971.32</td>
<td>1178.88</td>
<td>5150.20</td>
<td>5.15</td>
<td>52</td>
<td>71</td>
<td>19</td>
<td>56</td>
<td>0</td>
</tr>
<tr>
<td>1200</td>
<td>4425.76</td>
<td>1172.66</td>
<td>5598.42</td>
<td>5.60</td>
<td>56</td>
<td>79</td>
<td>23</td>
<td>58</td>
<td>2</td>
</tr>
<tr>
<td>1400</td>
<td>4698.00</td>
<td>1174.00</td>
<td>5872.00</td>
<td>5.87</td>
<td>60</td>
<td>85</td>
<td>25</td>
<td>57</td>
<td>-1</td>
</tr>
<tr>
<td>1450</td>
<td>4795.00</td>
<td>1178.00</td>
<td>5973.00</td>
<td>5.97</td>
<td>61</td>
<td>86</td>
<td>25</td>
<td>59</td>
<td>2</td>
</tr>
<tr>
<td>1500</td>
<td>3313.00</td>
<td>912.00</td>
<td>4225.00</td>
<td>4.23</td>
<td>56</td>
<td>75</td>
<td>19</td>
<td>81</td>
<td>22</td>
</tr>
<tr>
<td>1550</td>
<td>3425.00</td>
<td>928.00</td>
<td>4353.00</td>
<td>4.35</td>
<td>56</td>
<td>76</td>
<td>20</td>
<td>85</td>
<td>4</td>
</tr>
<tr>
<td>1600</td>
<td>3533.00</td>
<td>940.00</td>
<td>4473.00</td>
<td>4.47</td>
<td>56</td>
<td>76</td>
<td>20</td>
<td>99</td>
<td>14</td>
</tr>
</tbody>
</table>
Table 3.6: Baseline Readings for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap

| Payload Size | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughput | Throughpoint## 3.3.2 Performance Measurement for a Single Wireless VPN

Once the baseline readings are recorded, the next stage is to activate a single IPSec VPN between the wireless and wired clients and repeat all readings. The construction of the wireless IPSec VPN, operating on transport mode, is done using the IPSec policy snap-in tool provided by the Windows 2000 Professional operating system. This is in accordance to the specifications provided in Section 3.2.3. The Windows 2000 IP Security Monitor (IPSecMon) utility is executed in the background to check the operational status of the IPSec session at both ends. This utility very clearly shows the confidential bytes sent and confidential bytes received fields. This field confirms if ESP is working. It also shows authenticated bytes sent and authenticated bytes received. Finally, it shows bad SPI packets, packets not decrypted and packets that are not authenticated fields.

The same experiment, as described in Section 3.3.1, is repeated for varying UDP payload size while ensuring all other parameters remains constant for a traffic flow with a 1 ms inter-packet generation gap. As mentioned earlier, each reading is taken at least five times and
the mean value of this sample is taken to increase the accuracy of the readings. The next step is to increase the inter-packet generation gap to 5 ms, repeat the same experiment and record the readings. Table 3.7 and Table 3.8 provide the readings obtained at the source, for UDP flows with 1 ms and 5 ms inter-packet generation gap respectively.

Table 3.7: Performance Readings of a Single Wireless IPSec VPN for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th>Payload Size (Bytes)</th>
<th>Av.Tx. Throughput (Kbps)</th>
<th>Av.Rx. Throughput (Kbps)</th>
<th>Av.Total Throughput (Kbps)</th>
<th>Av.Total Throughput (Mbps)</th>
<th>Av. Pkt. loss in Tx. %</th>
<th>Av. Pkt. loss in Rx. %</th>
<th>Av. Delay (ms)</th>
<th>Jitter (ms)</th>
<th>Av. CPU Utilisation %</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>200.00</td>
<td>171.00</td>
<td>371.00</td>
<td>0.37</td>
<td>15.0</td>
<td>36.0</td>
<td>21</td>
<td>178.0</td>
<td>0.0</td>
</tr>
<tr>
<td>50</td>
<td>318.83</td>
<td>261.10</td>
<td>579.93</td>
<td>0.58</td>
<td>12.0</td>
<td>32.0</td>
<td>20</td>
<td>172.0</td>
<td>-6.0</td>
</tr>
<tr>
<td>75</td>
<td>387.00</td>
<td>324.00</td>
<td>711.00</td>
<td>0.71</td>
<td>0.0</td>
<td>17.8</td>
<td>18</td>
<td>212.0</td>
<td>40.0</td>
</tr>
<tr>
<td>100</td>
<td>438.05</td>
<td>410.00</td>
<td>848.05</td>
<td>0.85</td>
<td>0.0</td>
<td>16.9</td>
<td>17</td>
<td>153.0</td>
<td>-59.0</td>
</tr>
<tr>
<td>125</td>
<td>506.00</td>
<td>501.00</td>
<td>1007.00</td>
<td>1.01</td>
<td>0.0</td>
<td>17.6</td>
<td>18</td>
<td>129.0</td>
<td>-24.0</td>
</tr>
<tr>
<td>150</td>
<td>595.00</td>
<td>586.00</td>
<td>1181.00</td>
<td>1.18</td>
<td>0.0</td>
<td>18.5</td>
<td>19</td>
<td>117.0</td>
<td>-12.0</td>
</tr>
<tr>
<td>175</td>
<td>672.00</td>
<td>669.00</td>
<td>1341.00</td>
<td>1.34</td>
<td>0.0</td>
<td>18.8</td>
<td>19</td>
<td>106.0</td>
<td>-11.0</td>
</tr>
<tr>
<td>200</td>
<td>762.30</td>
<td>750.00</td>
<td>1512.30</td>
<td>1.51</td>
<td>0.0</td>
<td>19.0</td>
<td>19</td>
<td>97.7</td>
<td>-8.3</td>
</tr>
<tr>
<td>400</td>
<td>1293.01</td>
<td>1280.97</td>
<td>2573.98</td>
<td>2.57</td>
<td>0.0</td>
<td>23.6</td>
<td>24</td>
<td>67.0</td>
<td>-30.7</td>
</tr>
<tr>
<td>600</td>
<td>1652.37</td>
<td>1655.55</td>
<td>3307.92</td>
<td>3.31</td>
<td>0.0</td>
<td>30.8</td>
<td>31</td>
<td>62.0</td>
<td>-5.0</td>
</tr>
<tr>
<td>800</td>
<td>1961.23</td>
<td>1958.18</td>
<td>3919.41</td>
<td>3.92</td>
<td>0.0</td>
<td>36.5</td>
<td>36</td>
<td>60.0</td>
<td>-2.0</td>
</tr>
<tr>
<td>1000</td>
<td>2209.05</td>
<td>2205.82</td>
<td>4414.87</td>
<td>4.41</td>
<td>0.0</td>
<td>41.5</td>
<td>42</td>
<td>60.0</td>
<td>0.0</td>
</tr>
<tr>
<td>1200</td>
<td>2385.72</td>
<td>2385.87</td>
<td>4771.59</td>
<td>4.77</td>
<td>0.0</td>
<td>47.9</td>
<td>48</td>
<td>61.0</td>
<td>1.0</td>
</tr>
<tr>
<td>1400</td>
<td>2472.00</td>
<td>2470.00</td>
<td>4942.00</td>
<td>4.94</td>
<td>0.0</td>
<td>54.0</td>
<td>54</td>
<td>63.0</td>
<td>2.0</td>
</tr>
<tr>
<td>1450</td>
<td>1857.00</td>
<td>1855.00</td>
<td>3712.00</td>
<td>3.71</td>
<td>0.0</td>
<td>45.0</td>
<td>45</td>
<td>73.0</td>
<td>10.0</td>
</tr>
<tr>
<td>1500</td>
<td>1925.00</td>
<td>1922.00</td>
<td>3847.00</td>
<td>3.85</td>
<td>0.0</td>
<td>47.5</td>
<td>48</td>
<td>73.0</td>
<td>0.0</td>
</tr>
<tr>
<td>1550</td>
<td>1985.00</td>
<td>1970.00</td>
<td>3955.00</td>
<td>3.96</td>
<td>0.0</td>
<td>49.0</td>
<td>49</td>
<td>77.0</td>
<td>4.0</td>
</tr>
<tr>
<td>1600</td>
<td>2022.00</td>
<td>2011.00</td>
<td>4033.00</td>
<td>4.03</td>
<td>0.0</td>
<td>51.0</td>
<td>51</td>
<td>81.0</td>
<td>4.0</td>
</tr>
</tbody>
</table>
Table 3.8: Performance Readings of a Single Wireless IPSec VPN for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th>Payload Size (Bytes)</th>
<th>Throughput Tx (Kbps)</th>
<th>Throughput Rx (Kbps)</th>
<th>Throughput Total (Kbps)</th>
<th>Throughput Avg. Total (Mbps)</th>
<th>Loss in Tx (%)</th>
<th>Loss in Rx (%)</th>
<th>Pkt. Loss Avg. (ms)</th>
<th>Rx Delay (ms)</th>
<th>Utilisation (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>59</td>
<td>59</td>
<td>118.00</td>
<td>0.12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3.0</td>
</tr>
<tr>
<td>50</td>
<td>98.00</td>
<td>99.00</td>
<td>197.00</td>
<td>0.20</td>
<td>0.00</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>3.0</td>
</tr>
<tr>
<td>75</td>
<td>173.00</td>
<td>174.00</td>
<td>346.00</td>
<td>0.35</td>
<td>0.00</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>4.0</td>
</tr>
<tr>
<td>100</td>
<td>174.00</td>
<td>174.00</td>
<td>348.00</td>
<td>0.35</td>
<td>0.00</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>5.0</td>
</tr>
<tr>
<td>125</td>
<td>211.00</td>
<td>211.00</td>
<td>422.00</td>
<td>0.42</td>
<td>0.00</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>5.0</td>
</tr>
<tr>
<td>150</td>
<td>248.00</td>
<td>247.00</td>
<td>495.00</td>
<td>0.50</td>
<td>0.00</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>5.0</td>
</tr>
<tr>
<td>175</td>
<td>286.00</td>
<td>286.00</td>
<td>572.00</td>
<td>0.57</td>
<td>0.00</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>5.0</td>
</tr>
<tr>
<td>200</td>
<td>324.00</td>
<td>325.00</td>
<td>649.00</td>
<td>0.65</td>
<td>0.00</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>5.0</td>
</tr>
<tr>
<td>400</td>
<td>617.00</td>
<td>617.00</td>
<td>1234.00</td>
<td>1.23</td>
<td>0.00</td>
<td>0.01</td>
<td>0.01</td>
<td>0.00</td>
<td>5.0</td>
</tr>
<tr>
<td>600</td>
<td>832.00</td>
<td>857.00</td>
<td>1689.00</td>
<td>1.69</td>
<td>0.00</td>
<td>0.02</td>
<td>0.02</td>
<td>0.00</td>
<td>6.0</td>
</tr>
<tr>
<td>800</td>
<td>999.00</td>
<td>999.00</td>
<td>1998.00</td>
<td>2.00</td>
<td>0.00</td>
<td>0.03</td>
<td>0.03</td>
<td>0.00</td>
<td>7.0</td>
</tr>
<tr>
<td>1000</td>
<td>1197.00</td>
<td>1193.00</td>
<td>2390.00</td>
<td>2.39</td>
<td>0.00</td>
<td>0.70</td>
<td>0.70</td>
<td>0.00</td>
<td>9.0</td>
</tr>
<tr>
<td>1200</td>
<td>1365.00</td>
<td>1363.00</td>
<td>2728.00</td>
<td>2.73</td>
<td>0.00</td>
<td>0.80</td>
<td>0.80</td>
<td>0.00</td>
<td>11.0</td>
</tr>
<tr>
<td>1400</td>
<td>1538.00</td>
<td>1536.00</td>
<td>3074.00</td>
<td>3.07</td>
<td>0.00</td>
<td>0.95</td>
<td>0.95</td>
<td>0.00</td>
<td>13.0</td>
</tr>
<tr>
<td>1600</td>
<td>1596.00</td>
<td>1585.00</td>
<td>3181.00</td>
<td>3.18</td>
<td>0.00</td>
<td>6.30</td>
<td>6.30</td>
<td>0.00</td>
<td>22.0</td>
</tr>
</tbody>
</table>

3.3.3 Performance Measurement of Multiple Wireless VPNs

This section involves performing an experiment that is very similar to Section 3.3.2, on a multiple wireless VPN setup. The multiple wireless VPN setup is in accordance with the specifications provided in Section 3.2.4. The IPSec policy snap-in tool, provided by the Windows 2000 Professional operating system, is used to set up the multiple IPSec VPNs. These VPNs are configured to operate on transport mode.

The aim of the experiment is to increase the number of wireless VPN tunnels between the wired client and the wireless client and record the performance measures. Since the performance measures for a single VPN are already recorded in Section 3.3.2, the experimentation and data collection can be started over two simultaneously operating VPNs.

The network traffic generator at the sender is configured to generate two streams of UDP traffic on two destination port addresses (port 2001 and port 2002). These two are the destination port numbers for VPN 1 and VPN 2 in the IPSec filter list (Table 3.3). This ensures that the traffic is securely transmitted via these two IPSec VPNs. In the meantime, LanTraffic V2 at the wired client (the destination) is set to “start receiving traffic” mode for capturing this
Chapter 3 – Research Methodology

special incoming traffic transmitted from the wireless client (the source) on UDP port 2001 and 2002. As previously stated, LanTraffic V2 at the wired client (the destination) captures these two incoming UDP packet flows and echoes them back to the source. The Windows 2000 IP Security Monitor (IPSecMon) utility is executed in the background at both sender and receiver to check the operational status of the two IPSec sessions. This utility very clearly shows that there are two active IPSec associations between two entities. It also provides the total numbers of confidential and authenticated bytes sent and received.

Apart from the two streams of UDP, the basic traffic generation procedure at the source remains the same as in Section 3.3.1. At a given instance, each generated data stream consists of 10000 packets of UDP traffic with a fixed repeating packet content of 5A Hex value and a fixed inter-packet generation gap of 1 ms. The starting UDP payload size is 50 bytes and the payload size is increased step-by-step up to a maximum of 1600 bytes to reach higher traffic levels. Next, the entire experiment is repeated for a relatively lower UDP flow with 5 ms inter-packet generation gap. Each reading is taken at least five times and the mean value of this sample is taken to increase the accuracy of the readings. Hence note that all measures such as Throughput, CPU Utilisation, Packet Loss and Round-trip Delay correspond to an average value.

The data collection is facilitated via the automatic log file generation option of LanTraffic V2. Prior to the start of the UDP traffic flow, the automatic log file generation option in LanTraffic V2 is started at the source and destination. These auto-generated log files are capable of capturing the total transmission throughput, the total UDP packets sent and received, jitter and the average round-trip delay for the two UDP data flows. Since LanTraffic V2 does not have a CPU Utilisation measuring facility, the Windows 2000 performance monitor is used to measure the percentage of CPU Utilisation at the wireless client at each UDP traffic level. Table 3.9 and Table 3.10 provide the readings obtained at the source, for UDP flows with 1 ms and 5 ms inter-packet generation gaps respectively.
## Chapter 3 – Research Methodology

### Table 3.9: Performance Readings for Two Simultaneous Wireless IPSec VPNs for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th>Payload</th>
<th>Av.Tx. Throughput</th>
<th>Av.Rx. Throughput</th>
<th>Av.Total Throughput</th>
<th>Av.Pkt. Throughput</th>
<th>Delay</th>
<th>Jitter</th>
<th>Av. CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Kbps</td>
<td>Kbps</td>
<td>Kbps</td>
<td>Mbps</td>
<td>ms</td>
<td>ms</td>
<td>%</td>
</tr>
<tr>
<td>Bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>392.00</td>
<td>123.00</td>
<td>515.00</td>
<td>0.52</td>
<td>50.5</td>
<td>67.2</td>
<td>17</td>
</tr>
<tr>
<td>50</td>
<td>630.00</td>
<td>180.00</td>
<td>810.00</td>
<td>0.81</td>
<td>47.7</td>
<td>70.3</td>
<td>23</td>
</tr>
<tr>
<td>75</td>
<td>730.00</td>
<td>250.00</td>
<td>980.00</td>
<td>0.98</td>
<td>39.5</td>
<td>56.7</td>
<td>17</td>
</tr>
<tr>
<td>100</td>
<td>720.00</td>
<td>440.00</td>
<td>1160.00</td>
<td>1.16</td>
<td>18.5</td>
<td>36.5</td>
<td>18</td>
</tr>
<tr>
<td>125</td>
<td>790.00</td>
<td>490.00</td>
<td>1280.00</td>
<td>1.28</td>
<td>4.7</td>
<td>32.0</td>
<td>27</td>
</tr>
<tr>
<td>150</td>
<td>850.00</td>
<td>530.00</td>
<td>1380.00</td>
<td>1.38</td>
<td>0.7</td>
<td>32.0</td>
<td>31</td>
</tr>
<tr>
<td>175</td>
<td>895.00</td>
<td>590.00</td>
<td>1485.00</td>
<td>1.49</td>
<td>0.0</td>
<td>35.2</td>
<td>35</td>
</tr>
<tr>
<td>200</td>
<td>940.00</td>
<td>610.00</td>
<td>1550.00</td>
<td>1.55</td>
<td>0.0</td>
<td>35.9</td>
<td>36</td>
</tr>
<tr>
<td>400</td>
<td>1510.00</td>
<td>850.00</td>
<td>2360.00</td>
<td>2.36</td>
<td>0.0</td>
<td>45.8</td>
<td>46</td>
</tr>
<tr>
<td>600</td>
<td>1950.00</td>
<td>950.00</td>
<td>2900.00</td>
<td>2.90</td>
<td>0.0</td>
<td>53.0</td>
<td>53</td>
</tr>
<tr>
<td>800</td>
<td>2300.00</td>
<td>1000.00</td>
<td>3300.00</td>
<td>3.30</td>
<td>0.0</td>
<td>57.8</td>
<td>58</td>
</tr>
<tr>
<td>1000</td>
<td>2550.00</td>
<td>1100.00</td>
<td>3650.00</td>
<td>3.65</td>
<td>0.0</td>
<td>62.5</td>
<td>63</td>
</tr>
<tr>
<td>1200</td>
<td>2800.00</td>
<td>1100.00</td>
<td>3900.00</td>
<td>3.90</td>
<td>0.0</td>
<td>68.0</td>
<td>68</td>
</tr>
<tr>
<td>1400</td>
<td>2950.00</td>
<td>1100.00</td>
<td>4050.00</td>
<td>4.05</td>
<td>0.0</td>
<td>72.0</td>
<td>72</td>
</tr>
<tr>
<td>1450</td>
<td>2200.00</td>
<td>1200.00</td>
<td>3400.00</td>
<td>3.40</td>
<td>0.0</td>
<td>44.3</td>
<td>44</td>
</tr>
<tr>
<td>1500</td>
<td>2230.00</td>
<td>1210.00</td>
<td>3440.00</td>
<td>3.44</td>
<td>0.0</td>
<td>45.0</td>
<td>45</td>
</tr>
<tr>
<td>1550</td>
<td>2380.00</td>
<td>1200.00</td>
<td>3580.00</td>
<td>3.58</td>
<td>0.0</td>
<td>47.0</td>
<td>47</td>
</tr>
<tr>
<td>1600</td>
<td>2300.00</td>
<td>1440.00</td>
<td>3740.00</td>
<td>3.74</td>
<td>0.0</td>
<td>50.0</td>
<td>50</td>
</tr>
</tbody>
</table>

### Table 3.10: Performance Readings for Two Simultaneous Wireless IPSec VPNs for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th>Payload</th>
<th>Av.Tx. Throughput</th>
<th>Av.Rx. Throughput</th>
<th>Av.Total Throughput</th>
<th>Av.Pkt. Throughput</th>
<th>Delay</th>
<th>Jitter</th>
<th>Av. CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Kbps</td>
<td>Kbps</td>
<td>Kbps</td>
<td>Mbps</td>
<td>ms</td>
<td>ms</td>
<td>%</td>
</tr>
<tr>
<td>Bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>122.00</td>
<td>122.00</td>
<td>244.00</td>
<td>0.24</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>50</td>
<td>197.00</td>
<td>194.00</td>
<td>391.00</td>
<td>0.39</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>75</td>
<td>270.00</td>
<td>270.00</td>
<td>540.00</td>
<td>0.54</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>100</td>
<td>344.00</td>
<td>344.00</td>
<td>688.00</td>
<td>0.69</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>125</td>
<td>418.00</td>
<td>418.00</td>
<td>836.00</td>
<td>0.84</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>150</td>
<td>490.00</td>
<td>490.00</td>
<td>980.00</td>
<td>0.98</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>175</td>
<td>555.00</td>
<td>555.00</td>
<td>1110.00</td>
<td>1.11</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>200</td>
<td>622.00</td>
<td>622.00</td>
<td>1244.00</td>
<td>1.24</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>400</td>
<td>1050.00</td>
<td>1050.00</td>
<td>2100.00</td>
<td>2.10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>600</td>
<td>1460.00</td>
<td>1460.00</td>
<td>2920.00</td>
<td>2.92</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>800</td>
<td>1830.00</td>
<td>1830.00</td>
<td>3660.00</td>
<td>3.66</td>
<td>0.3</td>
<td>0.3</td>
<td>0.3</td>
</tr>
<tr>
<td>1000</td>
<td>2150.00</td>
<td>2150.00</td>
<td>4300.00</td>
<td>4.30</td>
<td>0.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>1200</td>
<td>2400.00</td>
<td>2400.00</td>
<td>4800.00</td>
<td>4.80</td>
<td>0.0</td>
<td>1.3</td>
<td>1.3</td>
</tr>
<tr>
<td>1400</td>
<td>2600.00</td>
<td>2600.00</td>
<td>5200.00</td>
<td>5.20</td>
<td>0.0</td>
<td>1.9</td>
<td>1.9</td>
</tr>
<tr>
<td>1450</td>
<td>2200.00</td>
<td>2150.00</td>
<td>4350.00</td>
<td>4.35</td>
<td>0.0</td>
<td>4.2</td>
<td>4.2</td>
</tr>
<tr>
<td>1500</td>
<td>2250.00</td>
<td>2200.00</td>
<td>4450.00</td>
<td>4.45</td>
<td>0.0</td>
<td>4.7</td>
<td>4.7</td>
</tr>
<tr>
<td>1550</td>
<td>2280.00</td>
<td>2230.00</td>
<td>4510.00</td>
<td>4.51</td>
<td>0.0</td>
<td>5.0</td>
<td>5.0</td>
</tr>
<tr>
<td>1600</td>
<td>2350.00</td>
<td>2290.00</td>
<td>4640.00</td>
<td>4.64</td>
<td>0.0</td>
<td>5.1</td>
<td>5.1</td>
</tr>
</tbody>
</table>
The next phase is to increase the number of simultaneously operating IPSec VPN connections to three and repeat the same experiment. Hence, the network traffic generator at the sender is configured to generate three streams of UDP traffic on destination port addresses 2001, 2002 and 2003. These three correspond to the destination port numbers of VPN 1, VPN 2 and VPN 3 in the IPSec filter list presented in Table 3.3. The three VPN connections will securely transmit the encrypted traffic to the destination. In the meantime, LanTraffic V2 at the wired client (the destination) is set to “start receiving traffic” mode to capture the encrypted traffic transmitted from the wireless client (the source) on UDP ports 2001, 2002 and 2003. Once this special UDP traffic is captured, LanTraffic will then echo it back to the source via the same VPNs. Windows 2000 IP Security Monitor (IPSecMon) utility is executed in the background at both sender and receiver to check the operational status of the three IPSec sessions. If all IPSec sessions are successfully operating, this utility will clearly show three active IPSec associations between the two entities.

Apart from three streams of UDP, the basic traffic generation procedure at the source remains the same. At a given instance, three data streams that consist of 10000 packets of UDP traffic with a fixed repeating packet content of 5A Hex value and a fixed inter-packet generation gap of 1 ms are used. The starting UDP payload size is 50 bytes and the payload size is increased step-by-step up to a maximum of 1600 bytes to reach higher traffic levels. Next, the entire experiment is repeated for a relatively lower UDP flow with a 5 ms inter-packet generation gap. Each reading is taken at least five times and the mean value of this sample is taken to increase the accuracy of the readings. Hence note that all measures such as Throughput, CPU Utilisation, Packet Loss and Round-trip Delay correspond to an average value.

As in the previous case, the data collection is facilitated via the automatic log file generation option of LanTraffic V2. Since LanTraffic V2 does not have a CPU Utilisation measuring facility, the Windows 2000 performance monitor is used to measure the percentage of CPU Utilisation at the wireless client at each UDP traffic level. Table 3.11 and Table 3.12 provide the readings obtained at the source, for UDP flows with 1 ms and 5 ms inter-packet generation gaps respectively.
# Chapter 3 – Research Methodology

Table 3.11: Performance Readings for Three Simultaneous Wireless IPSec VPNs for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th>Payload Size</th>
<th>Av.Tx. Throughput (Kbps)</th>
<th>Av.Rx. Throughput (Kbps)</th>
<th>Av.Total Throughput (Kbps)</th>
<th>Av.Total Throughput (Mbps)</th>
<th>Av. Pkt. loss in Tx. %</th>
<th>Av.Total Pkt. loss %</th>
<th>Av.Pkt. loss in Rx. %</th>
<th>Delays (ms)</th>
<th>Av. Utilisation %</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>465.00</td>
<td>114.00</td>
<td>579.00</td>
<td>0.58</td>
<td>56.00</td>
<td>75.0</td>
<td>19</td>
<td>265.0</td>
<td>0.0</td>
</tr>
<tr>
<td>50</td>
<td>685.00</td>
<td>230.00</td>
<td>915.00</td>
<td>0.92</td>
<td>54.00</td>
<td>74.0</td>
<td>20</td>
<td>255.0</td>
<td>-10.0</td>
</tr>
<tr>
<td>75</td>
<td>945.00</td>
<td>245.00</td>
<td>1190.00</td>
<td>1.19</td>
<td>52.00</td>
<td>73.0</td>
<td>21</td>
<td>272.0</td>
<td>17.0</td>
</tr>
<tr>
<td>100</td>
<td>1080.00</td>
<td>345.00</td>
<td>1425.00</td>
<td>1.43</td>
<td>49.00</td>
<td>70.0</td>
<td>21</td>
<td>280.0</td>
<td>8.0</td>
</tr>
<tr>
<td>125</td>
<td>1250.00</td>
<td>352.00</td>
<td>1602.00</td>
<td>1.60</td>
<td>48.00</td>
<td>70.0</td>
<td>22</td>
<td>295.0</td>
<td>15.0</td>
</tr>
<tr>
<td>150</td>
<td>1210.00</td>
<td>480.00</td>
<td>1690.00</td>
<td>1.69</td>
<td>38.00</td>
<td>60.0</td>
<td>22</td>
<td>305.0</td>
<td>10.0</td>
</tr>
<tr>
<td>175</td>
<td>1160.00</td>
<td>580.00</td>
<td>1740.00</td>
<td>1.74</td>
<td>27.50</td>
<td>53.2</td>
<td>26</td>
<td>310.0</td>
<td>5.0</td>
</tr>
<tr>
<td>200</td>
<td>1120.00</td>
<td>550.00</td>
<td>1670.00</td>
<td>1.67</td>
<td>12.00</td>
<td>49.0</td>
<td>37</td>
<td>315.0</td>
<td>5.0</td>
</tr>
<tr>
<td>250</td>
<td>1510.00</td>
<td>770.00</td>
<td>2280.00</td>
<td>2.28</td>
<td>0.00</td>
<td>47.0</td>
<td>47</td>
<td>240.0</td>
<td>-75.0</td>
</tr>
<tr>
<td>300</td>
<td>1940.00</td>
<td>850.00</td>
<td>2790.00</td>
<td>2.79</td>
<td>0.00</td>
<td>54.0</td>
<td>54</td>
<td>210.0</td>
<td>-30.0</td>
</tr>
<tr>
<td>400</td>
<td>2300.00</td>
<td>900.00</td>
<td>3200.00</td>
<td>3.20</td>
<td>0.00</td>
<td>59.0</td>
<td>59</td>
<td>210.0</td>
<td>0.0</td>
</tr>
<tr>
<td>500</td>
<td>2580.00</td>
<td>970.00</td>
<td>3550.00</td>
<td>3.55</td>
<td>0.00</td>
<td>64.0</td>
<td>64</td>
<td>210.0</td>
<td>0.0</td>
</tr>
<tr>
<td>600</td>
<td>2800.00</td>
<td>998.00</td>
<td>3798.00</td>
<td>3.80</td>
<td>0.00</td>
<td>69.0</td>
<td>69</td>
<td>210.0</td>
<td>0.0</td>
</tr>
<tr>
<td>800</td>
<td>2980.00</td>
<td>950.00</td>
<td>3930.00</td>
<td>3.93</td>
<td>0.00</td>
<td>72.0</td>
<td>72</td>
<td>209.0</td>
<td>-1.0</td>
</tr>
<tr>
<td>1000</td>
<td>2180.00</td>
<td>1120.00</td>
<td>3300.00</td>
<td>3.30</td>
<td>0.00</td>
<td>40.0</td>
<td>40</td>
<td>183.0</td>
<td>-26.0</td>
</tr>
<tr>
<td>1200</td>
<td>2220.00</td>
<td>1260.00</td>
<td>3490.00</td>
<td>3.49</td>
<td>0.00</td>
<td>42.0</td>
<td>42</td>
<td>188.0</td>
<td>5.0</td>
</tr>
<tr>
<td>1600</td>
<td>2330.00</td>
<td>1590.00</td>
<td>3920.00</td>
<td>3.92</td>
<td>0.00</td>
<td>45.0</td>
<td>45</td>
<td>199.0</td>
<td>4.0</td>
</tr>
</tbody>
</table>

Table 3.12: Performance Readings for Three Simultaneous Wireless IPSec VPNs for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th>Payload Size</th>
<th>Av.Tx. Throughput (Kbps)</th>
<th>Av.Rx. Throughput (Kbps)</th>
<th>Av.Total Throughput (Kbps)</th>
<th>Av.Total Throughput (Mbps)</th>
<th>Av. Pkt. loss in Tx. %</th>
<th>Av.Total Pkt. loss %</th>
<th>Av.Pkt. loss in Rx. %</th>
<th>Delays (ms)</th>
<th>Av. Utilisation %</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>168.00</td>
<td>168.00</td>
<td>336.00</td>
<td>0.34</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>6.0</td>
<td>0.0</td>
</tr>
<tr>
<td>50</td>
<td>272.00</td>
<td>272.00</td>
<td>544.00</td>
<td>0.54</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>6.0</td>
<td>0.0</td>
</tr>
<tr>
<td>75</td>
<td>375.00</td>
<td>375.00</td>
<td>750.00</td>
<td>0.75</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>7.0</td>
<td>1.0</td>
</tr>
<tr>
<td>100</td>
<td>470.00</td>
<td>470.00</td>
<td>940.00</td>
<td>0.94</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>7.0</td>
<td>0.0</td>
</tr>
<tr>
<td>125</td>
<td>572.00</td>
<td>572.00</td>
<td>1144.00</td>
<td>1.14</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>8.0</td>
<td>1.0</td>
</tr>
<tr>
<td>150</td>
<td>645.00</td>
<td>645.00</td>
<td>1290.00</td>
<td>1.29</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>8.0</td>
<td>0.0</td>
</tr>
<tr>
<td>175</td>
<td>760.00</td>
<td>760.00</td>
<td>1520.00</td>
<td>1.52</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>9.0</td>
<td>1.0</td>
</tr>
<tr>
<td>200</td>
<td>853.00</td>
<td>853.00</td>
<td>1706.00</td>
<td>1.71</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>11.0</td>
<td>2.0</td>
</tr>
<tr>
<td>225</td>
<td>920.00</td>
<td>920.00</td>
<td>1840.00</td>
<td>1.92</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>13.0</td>
<td>4.0</td>
</tr>
<tr>
<td>250</td>
<td>960.00</td>
<td>960.00</td>
<td>1920.00</td>
<td>2.01</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.0</td>
<td>6.0</td>
</tr>
<tr>
<td>275</td>
<td>1030.00</td>
<td>1030.00</td>
<td>2063.00</td>
<td>2.14</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>17.0</td>
<td>8.0</td>
</tr>
<tr>
<td>300</td>
<td>1080.00</td>
<td>1080.00</td>
<td>2250.00</td>
<td>2.35</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>19.0</td>
<td>10.0</td>
</tr>
<tr>
<td>325</td>
<td>1120.00</td>
<td>1120.00</td>
<td>2440.00</td>
<td>2.51</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>21.0</td>
<td>12.0</td>
</tr>
<tr>
<td>350</td>
<td>1160.00</td>
<td>1160.00</td>
<td>2620.00</td>
<td>2.67</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>23.0</td>
<td>14.0</td>
</tr>
</tbody>
</table>

49
3.3.4 Performance Measurements for a Site-to-Site VPN Tunnel
The performance measurement and data collection for a site-to-site VPN is are carries out on the experimental setup described under Section 3.2.5. As described in Figure 3.4, the actual VPN tunnel is operated between the two designated VPN gateways/routers located at two geographically distant campuses. Once the IPSec Tunnel is activated at the two gateways, according to its policy configuration, any traffic originating from a source in subnet 192.168.10.0/24 to a destination in 192.168.0.0/24 (and vice-versa) is securely tunnelled. The Windows 2000 IP Security Monitor (IPSecMon) utility is executed at the two VPN gateways to check the operational status of the IPSec sessions at both ends. Ethereal, a network protocol analysing tool, is also used at the two gateways to ensure and monitor the tunnel mode ESP encapsulation process.

Two wireless nodes, which are acting as the source and destination of the above two subnets, have LanTraffic V2 installed. The LanTraffic V2 network traffic generator program on the source (any node of subnet 192.168.10.0) is configured to generate a specific stream of UDP traffic to the destination (any node of subnet 192.168.0.0). The gateway at the source encapsulates the outgoing UDP flow as ESP packets and tunnels them to the gateway of the destination. At the destination gateway the packets are demultiplexed by stripping off their ESP headers and the original UDP flow is forwarded to its actual wireless destination node. In the meantime, LanTraffic V2 at the destination is set to “start receiving traffic” mode for capturing this special incoming traffic transmitted from the source. Once this special UDP traffic is captured, LanTraffic will then echo it back to the source.

The traffic flow generated under this experimentation is similar to that used in the previous cases. At a given instance, the source generates 10000 packets of UDP traffic with a fixed repeating packet content of 5A Hex value and a fixed inter-packet delay of 1 ms. The starting UDP payload size is 50 bytes and the payload size is increased step-by-step up to a maximum of 1600 bytes to reach higher traffic levels. Next, the entire experiment is repeated for a relatively lower UDP flow with a 5 ms inter-packet delay.

The data collection is facilitated via the automatic log-file generation option of LanTraffic V2. Prior to the start of the UDP traffic flow, the automatic log-file generation option in LanTraffic V2 is started at the source and destination. As in the previous cases, these auto-generated log files capture the total transmission throughput, the total UDP packets sent
and received, jitter and the average round-trip delay encountered by a UDP datagram to complete a trip from source to destination and back. However, unlike the previous cases, the CPU utilisation is measured at the VPN gateways, as this is where the IPSec encryption and tunnelling takes place. Since LanTraffic V2 does not have a CPU Utilization measuring facility, Windows 2000 performance monitor is used to measure the percentage of CPU Utilisation at the two VPN gateways. Each reading is taken at least five times and the mean value of this sample is taken to increase the accuracy of the readings. Hence note that all measures such as Throughput, CPU Utilization, Packet Loss and Round-trip Delay correspond to an average value. Table 3.13 and Table 3.14 provide the readings obtained at the source, for UDP flows with 1 ms and 5 ms inter-packet generation gaps respectively.

Table 3.13: Performance Readings for a Site-to-Site IPSec VPN Tunnel for UDP Traffic Generated with a 1 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>Kbps</td>
<td>Kbps</td>
<td>Kbps</td>
<td>Mbps</td>
<td>%</td>
<td>%</td>
<td>ms</td>
<td>ms</td>
</tr>
<tr>
<td>25</td>
<td>179.00</td>
<td>174.00</td>
<td>353.00</td>
<td>0.35</td>
<td>16.0</td>
<td>23.0</td>
<td>7</td>
<td>342.0</td>
</tr>
<tr>
<td>50</td>
<td>331.00</td>
<td>300.00</td>
<td>631.00</td>
<td>0.63</td>
<td>15.0</td>
<td>22.0</td>
<td>7</td>
<td>332.0</td>
</tr>
<tr>
<td>75</td>
<td>495.00</td>
<td>382.00</td>
<td>877.00</td>
<td>0.88</td>
<td>14.0</td>
<td>20.0</td>
<td>6</td>
<td>340.0</td>
</tr>
<tr>
<td>100</td>
<td>656.00</td>
<td>424.00</td>
<td>1080.00</td>
<td>1.08</td>
<td>19.0</td>
<td>25.0</td>
<td>6</td>
<td>345.0</td>
</tr>
<tr>
<td>125</td>
<td>759.00</td>
<td>463.00</td>
<td>1222.00</td>
<td>1.22</td>
<td>28.0</td>
<td>33.0</td>
<td>5</td>
<td>353.0</td>
</tr>
<tr>
<td>150</td>
<td>983.00</td>
<td>530.00</td>
<td>1513.00</td>
<td>1.51</td>
<td>38.0</td>
<td>43.0</td>
<td>5</td>
<td>365.0</td>
</tr>
<tr>
<td>175</td>
<td>1050.00</td>
<td>569.00</td>
<td>1619.00</td>
<td>1.62</td>
<td>40.0</td>
<td>45.0</td>
<td>5</td>
<td>369.0</td>
</tr>
<tr>
<td>200</td>
<td>1200.00</td>
<td>607.00</td>
<td>1807.00</td>
<td>1.81</td>
<td>42.0</td>
<td>47.0</td>
<td>5</td>
<td>364.0</td>
</tr>
<tr>
<td>400</td>
<td>2180.00</td>
<td>726.00</td>
<td>2906.00</td>
<td>2.91</td>
<td>62.0</td>
<td>68.0</td>
<td>6</td>
<td>301.0</td>
</tr>
<tr>
<td>600</td>
<td>3090.00</td>
<td>714.00</td>
<td>3804.00</td>
<td>3.80</td>
<td>69.0</td>
<td>75.0</td>
<td>6</td>
<td>280.0</td>
</tr>
<tr>
<td>800</td>
<td>3730.00</td>
<td>742.00</td>
<td>4472.00</td>
<td>4.47</td>
<td>74.0</td>
<td>81.0</td>
<td>7</td>
<td>276.0</td>
</tr>
<tr>
<td>1000</td>
<td>4190.00</td>
<td>868.00</td>
<td>5058.00</td>
<td>5.06</td>
<td>76.0</td>
<td>83.0</td>
<td>7</td>
<td>274.0</td>
</tr>
<tr>
<td>1200</td>
<td>4690.00</td>
<td>860.00</td>
<td>5550.00</td>
<td>5.55</td>
<td>78.0</td>
<td>85.0</td>
<td>7</td>
<td>274.0</td>
</tr>
<tr>
<td>1400</td>
<td>4850.00</td>
<td>915.00</td>
<td>5765.00</td>
<td>5.77</td>
<td>82.0</td>
<td>90.0</td>
<td>8</td>
<td>268.0</td>
</tr>
<tr>
<td>1450</td>
<td>4890.00</td>
<td>769.00</td>
<td>5659.00</td>
<td>5.66</td>
<td>74.0</td>
<td>78.0</td>
<td>4</td>
<td>238.0</td>
</tr>
<tr>
<td>1500</td>
<td>3690.00</td>
<td>546.00</td>
<td>4236.00</td>
<td>4.24</td>
<td>76.0</td>
<td>81.0</td>
<td>5</td>
<td>242.0</td>
</tr>
<tr>
<td>1550</td>
<td>3740.00</td>
<td>516.00</td>
<td>4256.00</td>
<td>4.26</td>
<td>80.0</td>
<td>85.0</td>
<td>5</td>
<td>254.0</td>
</tr>
<tr>
<td>1600</td>
<td>3870.00</td>
<td>487.00</td>
<td>4357.00</td>
<td>4.36</td>
<td>83.0</td>
<td>89.0</td>
<td>6</td>
<td>265.0</td>
</tr>
</tbody>
</table>
Table 3.14: Performance Readings for a Site-to-Site IPSec VPN Tunnel for UDP Traffic Generated with a 5 ms Inter-packet Generation Gap

<table>
<thead>
<tr>
<th>Payload Size (Bytes)</th>
<th>Throughput (Kbps)</th>
<th>Throughput (Kbps)</th>
<th>Throughput (Mbps)</th>
<th>% Loss in Tx.</th>
<th>% Pkt. Loss</th>
<th>% Loss in Rx.</th>
<th>Delay (ms)</th>
<th>Jitter (ms)</th>
<th>AV. CPU (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>60.50</td>
<td>60.50</td>
<td>121.00</td>
<td>0.12</td>
<td>0.00</td>
<td>0.00</td>
<td>11.5</td>
<td>0.0</td>
<td>17.0</td>
</tr>
<tr>
<td>50</td>
<td>99.90</td>
<td>99.90</td>
<td>199.80</td>
<td>0.20</td>
<td>0.00</td>
<td>0.00</td>
<td>12.5</td>
<td>1.0</td>
<td>17.0</td>
</tr>
<tr>
<td>75</td>
<td>138.00</td>
<td>138.00</td>
<td>276.00</td>
<td>0.28</td>
<td>0.00</td>
<td>0.00</td>
<td>13.5</td>
<td>1.0</td>
<td>17.0</td>
</tr>
<tr>
<td>100</td>
<td>176.00</td>
<td>176.00</td>
<td>352.00</td>
<td>0.35</td>
<td>0.00</td>
<td>0.00</td>
<td>14.0</td>
<td>0.5</td>
<td>18.0</td>
</tr>
<tr>
<td>125</td>
<td>212.00</td>
<td>212.00</td>
<td>424.00</td>
<td>0.42</td>
<td>0.00</td>
<td>0.00</td>
<td>15.0</td>
<td>1.0</td>
<td>18.0</td>
</tr>
<tr>
<td>150</td>
<td>253.00</td>
<td>253.00</td>
<td>506.00</td>
<td>0.51</td>
<td>0.00</td>
<td>0.00</td>
<td>16.0</td>
<td>1.0</td>
<td>18.0</td>
</tr>
<tr>
<td>175</td>
<td>292.00</td>
<td>292.00</td>
<td>584.00</td>
<td>0.58</td>
<td>0.00</td>
<td>0.00</td>
<td>17.5</td>
<td>1.5</td>
<td>19.0</td>
</tr>
<tr>
<td>200</td>
<td>331.00</td>
<td>331.00</td>
<td>662.00</td>
<td>0.66</td>
<td>0.00</td>
<td>0.00</td>
<td>19.0</td>
<td>1.5</td>
<td>19.0</td>
</tr>
<tr>
<td>400</td>
<td>615.00</td>
<td>615.00</td>
<td>1230.00</td>
<td>1.23</td>
<td>0.00</td>
<td>0.00</td>
<td>21.5</td>
<td>2.5</td>
<td>23.0</td>
</tr>
<tr>
<td>600</td>
<td>924.00</td>
<td>902.00</td>
<td>1826.00</td>
<td>1.83</td>
<td>0.00</td>
<td>0.00</td>
<td>25.0</td>
<td>3.5</td>
<td>25.0</td>
</tr>
<tr>
<td>800</td>
<td>1210.00</td>
<td>1190.00</td>
<td>2400.00</td>
<td>2.40</td>
<td>0.00</td>
<td>0.00</td>
<td>29.0</td>
<td>4.0</td>
<td>35.0</td>
</tr>
<tr>
<td>1000</td>
<td>1510.00</td>
<td>1495.00</td>
<td>3005.00</td>
<td>3.01</td>
<td>0.00</td>
<td>0.00</td>
<td>32.5</td>
<td>3.5</td>
<td>37.0</td>
</tr>
<tr>
<td>1200</td>
<td>1810.00</td>
<td>1795.00</td>
<td>3605.00</td>
<td>3.61</td>
<td>0.20</td>
<td>0.25</td>
<td>36.0</td>
<td>3.5</td>
<td>40.0</td>
</tr>
<tr>
<td>1400</td>
<td>2065.00</td>
<td>2030.00</td>
<td>4085.00</td>
<td>4.09</td>
<td>0.70</td>
<td>0.95</td>
<td>40.0</td>
<td>4.0</td>
<td>48.0</td>
</tr>
<tr>
<td>1450</td>
<td>2118.00</td>
<td>1910.00</td>
<td>4028.00</td>
<td>4.03</td>
<td>0.90</td>
<td>1.75</td>
<td>45.0</td>
<td>5.0</td>
<td>55.0</td>
</tr>
<tr>
<td>1500</td>
<td>1995.00</td>
<td>1960.00</td>
<td>3955.00</td>
<td>3.96</td>
<td>4.44</td>
<td>5.35</td>
<td>48.0</td>
<td>3.0</td>
<td>57.0</td>
</tr>
<tr>
<td>1550</td>
<td>2060.00</td>
<td>2015.00</td>
<td>4065.00</td>
<td>4.07</td>
<td>5.68</td>
<td>6.75</td>
<td>49.0</td>
<td>1.0</td>
<td>58.0</td>
</tr>
<tr>
<td>1600</td>
<td>2110.00</td>
<td>2090.00</td>
<td>4200.00</td>
<td>4.20</td>
<td>6.20</td>
<td>7.30</td>
<td>50.0</td>
<td>1.0</td>
<td>58.0</td>
</tr>
</tbody>
</table>

An in-depth analysis of the collected performance results is presented in the next chapter. It individually investigates the behaviour of each performance parameter by plotting these results in graphs and by comparing it with the most recent works in the field.
Chapter 4

Analysis of Performance Results

In this chapter a detailed analysis of the performance results from the experimentation described in the previous chapter is presented. Here, the behaviour of each performance metric is analysed individually. In most cases, the performance results are plotted, as graphs provide for easy comparisons and quick references. For each performance metric three basic scenarios are considered. The first scenario compares the performance of a single wireless IPSec VPN with that of a baseline measurement. Once the levels of the overheads for a single wireless IPSec VPN are documented, the next scenario investigates the variation in performance as the number of simultaneously operating VPNs is increased, under a similar environment. Finally, the setup is expanded to a site-to-site, geographically spanned, VPN implementation over an internetworked multi-platform infrastructure. A comparative analysis of the performance is then carried out to investigate the effects of the changed environment on a single wireless IPSec VPN.

2.1 Throughput

Throughput is one of the most important parameters used to evaluate the performance of wired as well as wireless data networks. The measured total throughput can be defined as the average amount of data payload transmitted and received over a sampling period between two points in the same service area [38]. The throughput metric used is Mbps.

4.1.1 Throughput Analysis for a Single Wireless VPN

Figures 4.1 and 4.2 represent the average throughput graphs for UDP traffic generated at 1 ms and 5 ms inter-packet generation gaps respectively. The results presented in Figure 4.1 indicate that the baseline value for maximum achievable throughput for UDP, under the given conditions, is 5.97 Mbps. Although the effective net throughput depends on the bit rate at which the wireless station communicates with the AP, the result indicates that the achievable throughput has somehow compensated as a consequence of various overheads. The overheads of the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) medium access
Figure 4.1: The Average Throughput Graphs for Traffic Generated with a 1ms Inter-packet Generation Gap.

Figure 4.2: The Average Throughput Graphs for Traffic Generated with a 5ms Inter-packet Generation Gap.
schema, of the IEEE 802.11 standard, can be pointed out as the primary cause for such a poor performance in throughput. Other overheads that may affect throughput are the preambles of the transmitted frames, MAC headers, ACK frames, transmission protocol overheads, processing delays in stations, forwarding delays around the APs and the random back-off periods [39], [40].

Furthermore, it is interesting to see that the observation of the baseline result is in line with some of the previously published results [41], [39]. Figure 4.1 also shows that, when IPSec VPN is active, the resultant tunnel overheads drop the throughput to 4.94 Mbps. It is evident from the above results that the effective net average throughput greatly depends on the bit rate at which the packets are generated. This behaviour has been attributed to the fact that more payload data is being transferred in shorter transfer times, resulting in relatively high net throughput values [42].

It can also be noted that the throughput graphs in Figures 4.1 and 4.2 show a general trend. That is, they show that there is generally an enhancement in throughput with the increasing UDP payload sizes. This can be explained by noting the relative reduction of UDP/IP and MAC overheads with the increasing payload (per UDP packet) [43]. The graphs representing the throughput for the baseline and the IPSec VPN indicate a behaviour very much closer for payloads up to 200 bytes, then the gap between the two graphs tends to widen as the payload increases. This is caused by the excessive overheads of the IPSec VPN connection [17]. As a result, for a payload size of 1400 bytes, the average throughput achieved by the VPN is approximately 15% less than its baseline value.

The graphs show that when the throughput reaches a maximum point a sudden (but temporary) drop can be noted. This can be related to the fragmentation of the IP datagrams. This phenomenon can be expected when the payload increases beyond 1472 bytes (that is, 1500 bytes for Ethernet frame – 20 bytes for IP header – 8 bytes for UDP header) for the baseline curve. Payloads larger than 1472 bytes become fragmented into more than one datagram, reducing the net throughput rapidly [44]. A similar behaviour can be noticed for the average throughput graph of the IPSec VPN. However, this happens somewhat earlier when the payload increases beyond 1438 bytes. This is due to the additional headers introduced by the ESP encapsulation.
4.1.2 Throughput Analysis for a Multiple Wireless VPNs

Figures 4.3 and 4.5 represent the average throughput graphs for multiple IPSec VPNs. These are plotted for UDP traffic flows generated with 1 ms and 5 ms inter-packet generation gaps respectively. It is worth noting that the graphs corresponding to the baseline and the single IPSec VPN relate to Figures 4.1 and 4.2. For comparative analysis all throughput results are plotted in a single plane.

As the number of simultaneously operating VPNs is increased, a considerable reduction in the total average throughput can be noticed. This is evident from Figure 4.3. For instance, when 2 simultaneous IPSec VPNs are operating, the total highest average throughput achieved by both VPNs in Figure 4.3, is 4.05 Mbps. In other words, the maximum per tunnel average throughput is approximately 2 Mbps. This is almost a 60% drop compared to the average throughput achieved by the single IPSec VPN (4.97 Mbps). Figure 4.3 also shows that, when the number of simultaneously operating VPNs is increased to three, the highest per VPN average throughput drops further to 1.3 Mbps. Figure 4.5 shows that, when the packet generation rate is reduced, multiple VPNs achieve higher throughput levels. For instance, the maximum per VPN average throughput for two simultaneously operating IPSec VPNs in Figure 4.5 is 2.6 Mbps. This is very much close to the maximum average throughput of 2.9 Mbps achieved by a single IPSec VPN under similar conditions.

The graphs in Figure 4.3 indicate that there may be a possibility for reduction in the per VPN average throughput as the total number of simultaneously operating VPNs is increased. However, Figure 4.4 illustrates that this is not always true. In fact, Figure 4.4 shows that for UDP flow with payload sizes up to 150 bytes, the throughput graphs may behave in the opposite manner. The highest total average throughput value in Figure 4.5 is recorded for the setup of 3 simultaneously operating IPSec VPNs. The second-highest total average throughput value corresponds to the setup of 2 simultaneously operating IPSec VPNs. The baseline and the single VPN show the lowest throughput values in Figure 4.4.

Furthermore, the throughput graphs in the region of 1000 bytes and lower, in Figure 4.5, closely resemble the graphs in Figure 4.4. Both of these show how the peak performing multiple VPN setup increasingly suffers reductions in the rate of change (increase) in throughput. Refer to the graphs in Figure 4.5; this effect is experienced by UDP traffic with
payloads of 600 bytes and over. Figures 4.4 and 4.3 also indicate that a similar effect is being experienced, at a much earlier stage. From these two cases; it is clear that the packet generation rate and the packet payload size are the two dominant factors affecting the performance of simultaneously operating multiple VPN setups. The maximum throughput limit achievable between two end-systems from such a configuration varies significantly, depending on the values of these two parameters. In summary, to achieve the highest performance levels from multiple VPN setups, relatively slower packet generation rates and shorter payload data sizes must be used.

In all the above cases, as the throughput values reach a maximum point, a sudden (but temporary) drop is experienced. This is related to the fragmentation of the IP datagrams, as explained in detail in Section 4.1.1.

![Figure 4.3: The Average Throughput Graphs for Traffic Generated with a 1ms Inter-packet Generation Gap.](image-url)
Figure 4.4: Expanded Section of Figure 4.3; the Average Throughput Graph for Payload Data Sizes of 25 to 200 Bytes.

Figure 4.5: The Average Throughput Graphs for Traffic Generated with a 5ms Inter-packet Generation Gap.
4.1.3 Throughput Analysis for a Site-to-Site VPN

This section analyses the throughput results of a site-to-site IPSec VPN with encryption and tunnelling between two geographically distant locations (subnets). Figures 4.6 and 4.7 represent the average throughput graphs for UDP traffic generated at 1 ms and 5 ms inter-packet generation gaps respectively. The results in Figure 4.6 indicate that the value for maximum achievable throughput for such an IPSec VPN implementation, under the given conditions, is 5.77 Mbps. This result is very much closer to the maximum achievable baseline throughput result in Section 4.1.1.

For easy and convenient comparison, the two throughput graphs (baseline and wireless IPSec VPN with encryption) of Figure 4.1 are incorporated in Figure 4.6. The graphs clearly show how the throughput results of the site-to-site VPN coincide with the baseline throughput results. It also shows how much this deviates from the throughput results achieved by a simple wireless VPN with encryption. Thus the throughput results reveal that by deploying a designated VPN gateway for IPSec encryption and tunnel maintenance, a given node can achieve higher throughput levels. Similar observations can be made for the behaviour of throughput for traffic generated with higher inter-packet generation gaps (that is, 5 ms) by analysing graphs in Figures 4.7 and 4.2.

As explained in Section 4.1.1, the throughput results obtained for the site-to-site VPN setup are still affected by the same overheads which influenced the baseline throughput results. The overheads of the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) medium access schema, of the IEEE 802.11 standard can be pointed out as the primary cause for such poor performance in throughput. Other overheads that may affect throughput are preambles of the transmitted frames, MAC headers, ACK frames, transmission protocol overheads, processing delays in stations, forwarding delays around the APs and the random back-off periods [39], [40]. However, the transmitting node is not affected by the overheads of the IPSec VPN tunnel maintenance or encryption.
Figure 4.6: The Average Throughput Graphs for Traffic Generated with 1 ms Inter-packet Generation Gap.

Figure 4.7: The Average Throughput Graphs for Traffic Generated with 5 ms Inter-packet Generation Gap.
As per the previous observations, the throughput graphs show a sudden (but temporary) drop as the fragmentation of the IP datagrams takes place. This phenomenon can be noticed when the payload increases beyond 1472 bytes (that is, 1500 bytes for Ethernet frames – which include 20 bytes for the IP header and 8 bytes for the UDP header) for the baseline curve. Payloads larger than 1472 bytes become fragmented into more than one datagram, reducing the net throughput rapidly [44]. A similar behaviour is noticed for the two IPSec VPN graphs. However, in both cases, this happens somewhat earlier when the payload increases beyond 1438 bytes. This is due to the additional headers introduced by the ESP encapsulation. Unlike the rest of the throughput curves, the throughput of a site-to-site IPSec VPN does not show a steep drop at 1438 bytes. The site-to-site IPSec VPN shows a noticeable drop at 1472 bytes, behaving very similarly to the baseline results. This again shows that the fragmentation of ESP packets taking place at an off-site IPSec VPN gateway has a minimal affect on the end-to-end throughput.

### 2.2 Packet Loss

Packet loss is another important parameter used to evaluate the performance of data networks. Two different types of packet loss measures are taken at various instances. The first is the average per tunnel packet loss in transmission (outbound traffic) and the second is the per tunnel packet loss in receiving (inbound traffic). The analysis presented in this section discusses its behaviour under various scenarios.

#### 4.2.1 Packet Loss Analysis for a Single Wireless VPN

The series of experimental data collected shows two types of packet loss. The first is the percentage of average packet loss in transmission (that is, outbound) from source to destination. The second is the percentage of average packet loss in receiving the inbound echoed traffic from the destination to source. The former is represented as packet loss in transmitting by the graphs in Figures 4.8 and 4.10, whereas the latter is better labelled as packet loss in receiving by the graphs in Figures 4.9 and 4.11.

These graphs clearly illustrate that the faster the UDP packet generation, the higher the packet loss. This phenomenon applies to all packet loss observations. Furthermore, as the UDP payload size is increased, the packet loss ratio increases for both baseline and IPSec VPNs.
This is again in line with previous works in the field [42]. The overall average round-trip (transmission and receive combined) packet loss reached a maximum of 85% for the baseline, and for the IPSec VPN this value is 54%.

As it is clear from Figures 4.8 and 4.9 there is a high packet loss (up to approximately 35% in transmission and 20% in receiving) experienced for UDP datagrams with light payloads (that is, 25 to 50 bytes), generated at 1 ms intervals. Similar trends in packet loss have already been identified and published [42], [45], [46]. One such argument is that the buffer shortages at the UDP level, due to the very fast generation rate of short packets, may cause datagrams to be dropped [42]. In spite of this, such a condition is most likely to arise for bursty traffic. Hence, for the type of UDP flow used in this experiment, UDP buffer overflow cannot be the primary cause for such packet loss. A second explanation for the cause of such high packet loss points towards the behaviour of the lower network layers, data link layer or physical layer [45], [46]. These researchers argue that, when a wireless interface card deals with frames having such short payload sizes, the overheads occupy most of the frame. The bidirectional traffic arriving continuously causes increases in the total traffic and contention. When such frames arrive continuously at the wireless interface, the processing ability of the interface card is decelerated and the packets eventually get dropped off. This leads to a bottleneck situation and once the above point is reached, a significant loss of UDP frames can be experienced.

For higher packet generation rates (that is, 1ms), as the UDP payload gradually increases from 100 to 1,400 bytes, the packet loss trend increases. The cause is again a similar bottleneck situation forming at the wireless interface as per the following explanation. When the payload of the UDP packets increases, the transmission delay at the interface increases. As a result, at high packet generation rates (that is, 1ms), relatively larger packets may experience increasing queuing delays. Consequently, a bottleneck situation forms at the wireless interface. As we know, when a UDP datagram is delayed due to queuing up to the maximum delay limit, it is not useful anymore, will not be transmitted and will be dropped by the sender [43]. Alternatively, the output buffer may simply overflow beyond a point, contributing to the dropping of UDP packets [40]. Hence an exponential growth in the packet loss at the source is experienced. The direct effect of this can be seen in Figure 4.8. If you observe closely, the baseline graph in Figures 4.8 and 4.9 further reveals that the bulk of the packets is lost
Chapter 1 – Analysis of Performance Results

Figure 4.8: Packet Loss in Transmitting Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.9: Packet Loss in Receiving Traffic Generated at 1 ms Inter-packet Delay
Chapter 1 – Analysis of Performance Results

Figure 4.10: Packet Loss in Transmitting Traffic Generated at 5 ms Inter-packet Delay.

Figure 4.11: Packet Loss in Receiving Traffic Generated at 5 ms Inter-packet Delay.
in transmission and the average packet loss in receiving the echoed traffic is relatively less. Section 4.2.2 can be referred to for a logical explanation for such behaviour.

Despite the high packet generation rate, it is interesting to note that the IPSec VPN graph in Figure 4.8 experiences a minimal packet loss. The explanation is that at the network layer, a UDP datagram spends a comparatively longer time for the IPSec encryption process. This causes each UDP packet to slow down automatically, acting as a kind of a natural flow control mechanism. This prevents or, if not, reduces queuing at the interface. As a result, the packet losses are relatively less for an IPSec VPN, even at higher packet generation rates. A similar explanation holds true for low packet losses experienced by the graphs in Figures 4.10 and 4.11. When the inter-packet delay is increased to 5 ms, queuing at the interface is virtually inexistent. Hence, there is a very low level of packet loss.

Finally, the graphs in Figures 4.8 and 4.9 show a sudden but temporary drop at the point of fragmentation similar to the graphs in Figures 4.2 and 4.3. The most likely reason for this is the delay component introduced at the Network Layer as a result of fragmentation. This helps to reasonably slow down the UDP flow, acting as a natural flow control mechanism. Hence a temporary drop in the packet loss at this point is displayed. This explanation only applies for high packet generation rates (that is, 1 ms). When the inter-packet delay is increased to 5 ms, as mentioned previously, queuing at the interface becomes virtually nonexistent. It can be noted from Figures 4.10 and 4.11 that there is an increase in packet loss rate as fragmentation happens. This is due to the overheads introduced by the fragmentation process.

### 4.2.2 Packet Loss Analysis for a Multiple Wireless VPNs

As in the previous case, the packet loss metric specifically investigates the average per tunnel packet loss percentage in the transmission (outbound) and receiving (inbound) processes. These relate to the wireless client for UDP traffic generated at two different rates. These results are represented in Figures 4.12 to 4.15.

As is clear from the graphs in Figure 4.12, there is a relatively high packet loss experienced by UDP datagrams with light payloads (that is, 25 to 50 bytes), generated at 1 ms intervals. The argument and explanation provided in Section 4.2.1 holds true despite the fact
that the numbers of multiple VPNs are increased. According to this argument, as the number of simultaneously operating VPNs is increased, it is obvious that this situation becomes worse. Thus, Figure 4.12 indicates higher percentages of packet losses in transmission for UDP traffic with light payload sizes (that is, 200 bytes and less).

Comparing the results in Figures 4.12 and 4.13 against those in Figures 4.14 and 4.15 indicates that, for traffic with smaller inter-packet generation gaps, packet loss is higher. Furthermore, as the UDP payload size is gradually increased, the packet loss also increases for baseline as well as for IPSec VPN setups. This is also confirmed by previously published works in the field [42]. The cause can yet again be related to a similar bottleneck situation forming at the wireless interface, as explained in Section 4.2.1.

Despite the high packet generation rate, the packet loss graphs in Figure 4.12 show that IPSec VPNs achieve relatively low packet losses compared to their baseline situation. This condition only applies to UDP traffic with payloads of 400 bytes and over. This is due to the delay taking place at the network layer as a result of the increased overheads of the IPSec VPN as the UDP payload size increases. A detailed explanation of this phenomenon is produced in Section 4.2.1.

![Packet Loss in Transmitting Traffic Generated at 1 ms Inter-packet Delay](image)

*Figure 4.12: Packet Loss in Transmitting Traffic Generated at 1 ms Inter-packet Delay.*
Chapter 1 – Analysis of Performance Results

Figure 4.13: Packet Loss in Receiving Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.14: Packet Loss in Transmitting Traffic Generated at 5 ms Inter-packet Delay.
Chapter 1 – Analysis of Performance Results

Figure 4.15: Packet Loss in Receiving Traffic Generated at 5 ms Inter-packet Delay.

The above discussions have mainly concentrated on one aspect of packet loss, that is, the packet loss during transmission of the data from the wireless client to the wired client, as shown by the graphs in Figures 4.12 and 4.14. The second aspect of packet loss is shown by Figures 4.13 and 4.15. This relates to the loss in receiving the inbound echoed packets, from the wired client to the wireless client. The analysis of inbound traffic leads to some interesting results. Based on the results for the baseline situation, shown in Figure 4.13, it can be assumed that without any VPNs the interface is capable of processing inbound traffic with a minimal loss.

This can be taken as an indication that the interface is also able to process all the outbound traffic. If that is the case, the high level of packet loss depicted in Figure 4.12 needs to be investigated. However, this may be qualitatively explained as follows. As a result of the dropping of UDP packets due to congestion and buffer overflows before reaching the interface, the interface may eventually end up processing less outbound data than what was originally generated. A side observation from this is that the interface is not performing at its peak when processing the outbound traffic. In fact, this was also verified by analysing some dump files captured using the Windump (the Windows version of TCP Dump) utility.

As discussed previously, Figure 4.14 shows a minimal outbound packet loss during transmission. However, in the case of inbound traffic, Figure 4.15 indicates that one of the
Chapter 1 – Analysis of Performance Results

VPN implementations is experiencing a significant growth in packet loss. This happens to be the implementation of three simultaneous IPSec VPNs. For payload data over 600 bytes, these VPNs experienced increasing packet losses. Furthermore, referring back to Figure 4.5, it can be noted that for payload sizes over 600 bytes, the same VPN setup experienced a reduction in the rate of change (increase) in throughput. Therefore, as per the argument presented in Section 4.1.2, it can be assumed that the above VPN setup has reached its performance limits.

Finally, all packet loss results shown in Figures 4.12 to 4.15 indicate sudden, but temporary, changes at the point of fragmentation, similar to the results in Figures 4.3 and 4.5. This can be attributed to the delay and overheads introduced at the network layer as a result of fragmentation. This will reasonably slow down the UDP flow, resulting in a temporary drop in the packet loss.

4.2.3 Packet Loss Analysis for a Site-to-Site VPN

This section provides a comparative analysis for the behaviour of packet loss in a site-to-site IPSec VPN, with encryption and tunnelling between two geographically distant locations (subnets). Similar to the previous two sections, the series of experimental data collected signifies two types of packet loss. The first is the percentage of average packet loss in transmission and the second is the percentage of average packet loss in receiving. The former is represented by the graphs in Figures 4.16 and 4.18 and the latter corresponds to the graphs in Figures 4.17 and 4.19. For ease and convenience in comparison, the packet loss graphs in Section 4.2.1 (that is, Figures 4.8 to 4.11) are incorporated into Figures 4.16 and 4.19.

It can be very clearly seen how the packet loss trends represented by these new graphs, for a site-to-site VPN, are approximately close to the baseline graphs of Section 4.2.1. The overall average round-trip (transmission and receiving combined) packet loss reaches a maximum of 90%, which is slightly higher than the corresponding baseline result (85%) of Section 4.2.1. We can further investigate how the geographical distance and the deployment of an external gateway may affect packet loss by analysing graphs in Figures 4.16 and 4.17. Figure 4.16 indicates that a site-to-site VPN has a relatively higher packet loss in transmission at high inter-packet generation rates. Since there is no IPSec encryption taking place, the configuration and behaviour of the source is similar to the time of obtaining the baseline reading (Section 4.2.1). Therefore, the primary causes for such high packet loss can be directly
related to the reasons stated for the packet loss of the baseline reading in Figure 4.8, in Section 4.2.1. The geographical distance between the two campuses, routing and the performance of the microwave link can be pointed out as additional contributors to the packet loss. As the inter-packet generation gap is increased to 5 ms, as mentioned in the previous sections, queuing at the interface becomes minimal. As a result, Figures 4.18 and 4.19 show minimal packet loss.

Another interesting observation can be noted by closely looking at the graphs of site-to-site VPN in Figures 4.16 and 4.17. It is noted that the bulk of the packets are lost in transmission (as discussed above) and the average packet loss in receiving (Figure 4.17) of the echoed traffic is relatively less. This phenomenon has also been observed in the baseline packet loss graphs of Sections 4.2.1 and 4.2.2. Section 4.2.2 presents a reasonable explanation for such behaviour.

As discussed previously, at the point of fragmentation all packet loss graphs in Figures 4.16 and 4.17 show temporary drops. Although the packet loss graphs for the site-to-site VPN show the trend of the baseline graph, the fragmentation coordinates coincide with the wireless IPSec VPN graph. However, due to the increase in overheads of fragmentation, Figures 4.18 and 4.19 show a notable increase in packet loss.

![Packet Loss Graph](image)

*Figure 4.16: Packet Loss in Transmitting Traffic Generated at 1 ms Inter-packet Delay.*
Chapter 1 – Analysis of Performance Results

Figure 4.17: Packet Loss in Receiving Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.18: Packet Loss in Transmitting Traffic Generated at 5 ms Inter-packet Delay.
Figure 4.19: Packet Loss in Receiving Traffic Generated at 5 ms Inter-packet Delay.

2.3 CPU Utilisation

It is a common belief that the impact of the CPU is insignificant on the performance of a data network. However, the study of this metric proves otherwise and helps to understand how it may affect the performance of an IPSec VPN. It helps especially to understand the behaviour of the CPU as the numbers of simultaneously functioning IPSec VPNs are increased. It also helps to understand the changes in behaviour of the VPN/s as the CPU reaches its limits. Finally, results are shown on how the performance metrics may vary as an external VPN gateway is deployed.

4.3.1 CPU Utilisation Analysis for a Single Wireless VPN

The CPU utilisation for various UDP payloads is represented in Figures 4.20 and 4.21. From these graphs, it is evident that considerable numbers of CPU cycles are necessary for the functioning of a single IPSec VPN. For instance, as evident from Figure 4.20, with a low inter-packet generation gap (that is, 1 ms), the IPSec VPN (approximately) enforces an extra 50% load on the CPU. On the other hand, as the inter-packet generation gap increases (that is, to 5 ms), this difference gradually reduces down to around 35%, as shown in Figure 4.21.
Chapter 1 – Analysis of Performance Results

The analysis shows that there is a direct relationship between the average throughput and the CPU utilisation. Obviously, the higher throughput values require packets generated at higher bit rates with payload data transmitted in shorter transfer times. The additional CPU cycles for these tasks can explain why the IPSec VPN graph in Figure 4.20 shows an (approximately) extra 15% load on the CPU in comparison to that in Figure 4.21. Therefore, we can assume that a considerably high CPU utilisation rate is required to maintain an IPSec VPN at its peak performance. However, the converse does not hold true, that is, by simply upgrading the CPUs at the VPN end-points higher throughput rates cannot be achieved beyond a certain ceiling limit. Then again, the reasons for such limitations have already been discussed in Section 4.1.1. If the CPU reaches its saturation point, an immediate negative effect on the average throughput may be experienced. Nevertheless, the CPUs used for this experiment did not demonstrate such extreme behaviour for a single IPSec VPN over a wireless media for conditions under study.

The graphs in Figures 4.20 and 4.21 also show relatively high CPU utilisation rates for lighter UDP payloads. The bottleneck situation discussed in Section 4.2.1 can be pointed out as the primary cause. It is clear from the above graphs that when the UDP payload increases, the CPU utilisation also increases. In spite of this, at the point of fragmentation the CPU utilisation graph for the IPSec VPN in Figure 4.20 shows a momentary drop. As discussed in Section 4.2.1, fragmentation and the extra overheads of the IPSec VPN at the network layer help to relatively slow down the UDP flow, acting as a natural flow control mechanism. This temporarily decelerates queuing at the interface and, as a result, the CPU utilisation reduces. Thus, a momentary drop in the CPU utilisation is noted. However, when the inter-packet generation gap increases to 5 ms, we know that the queuing at the interface becomes virtually inexistent. That is, beyond the point of fragmentation, a higher number of CPU cycles are required to process the fragmented datagrams with the overheads of the IPSec VPN. Consequently, an increase in CPU utilisation can be noted, as in Figure 4.21.
Chapter 1 – Analysis of Performance Results

Figure 4.20: The CPU Utilisation Graphs for Traffic Generated with a 1 ms Inter-packet Generation Gap.

Figure 4.21: The CPU Utilisation Graphs for Traffic Generated with a 5 ms Inter-packet Generation Gap.
4.3.2 CPU Utilisation Analysis for a Multiple Wireless VPNs

The results of average CPU utilisation at the wireless client for various UDP payloads are shown in Figures 4.22 and 4.23. It is clearly evident that a considerable number of CPU cycles are necessary for the functioning and implementation of single as well as multiple IPSec VPN setups.

As the number of simultaneous VPN implementations is increased, the CPU utilisation increases further. The highest average CPU utilisation rate shown in Figure 4.22 is 99.2%. However, Figure 4.23 shows 100% CPU utilisation for payloads of 1200 and 1400 bytes when three VPNs operate simultaneously. It also shows an average CPU utilisation of 98% and over for all UDP traffic with payloads of more than 600 bytes. From this point onwards, the graph indicates that the CPU is in full utilisation. This can be classified as the CPU having reached a saturation point as predicted in [47]. The behaviour shown by the graphs for three simultaneous VPNs in Figures 4.5 and 4.15 clearly illustrate the overall VPN performance degradation, as a result of the CPU reaching its processing limits. This phenomenon of a relatively slower CPU acting as a bottleneck by affecting the QoS of an IPSec VPN is in agreement with other publications in the field [48].

The graphs in Figures 4.22 and 4.23 also show relatively high CPU utilisation rates for lighter UDP payloads. The bottleneck situation discussed in Section 4.2.2 can be regarded as the primary cause for this situation. Yet again, at the point of fragmentation, the CPU utilisation for the IPSec VPNs in Figures 4.22 and 4.23 (except for the baseline and single VPN graphs in Figure 4.23) shows a momentary drop. As discussed in Section 4.2.4, fragmentation and the extra overheads of the IPSec VPN at the network layer help to relatively slow down the UDP flow. This temporarily reduces the queuing at the interface and, as a result, the average CPU utilisation reduces.
Chapter 1 – Analysis of Performance Results

Figure 4.22: CPU Utilisation for Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.23: CPU Utilisation for Traffic Generated at 5 ms Inter-packet Delay.
4.3.3. CPU Utilisation Analysis for a Site-to-Site VPN

The analysis presented in this section shows the extent of CPU utilisation that an external IPSec VPN gateway is subjected to in a site-to-site VPN implementation. The CPU utilisation at the IPSec VPN gateway is represented in Figures 4.24 and 4.25. For convenient comparison, the CPU utilisation graphs in Section 4.3.1 (that is, Figures 4.20 and 4.21) are incorporated into Figures 4.24 and 4.25.

Despite the fact that there is no packet generation taking place, the graphs clearly indicate how encryption and tunnelling at a remote VPN gateway can still consume a very high number of CPU cycles. As illustrated in Figure 4.24, the comparison of these CPU utilisation results with the CPU utilisation results of a wireless IPSec VPN (where both transmission and encryption are perform at the host), reveal similar trends. The most prominent of these relates to how the gap between the two graphs narrows down as the UDP payload size increases. The graphs on Figure 4.25 further confirm that, irrespective of the traffic generation rate of the data flow, this trend is followed.

Another interesting observation from Figures 4.24 and 4.25 is that the CPU utilisation graph of a remote VPN gateway not showing relatively high CPU utilisation rates for lighter UDP payloads (that is, 25 to 50 bytes). However, this can be seen in the rest of the CPU utilisation graphs (that is, for the baseline and wireless IPSec VPN) in Figures 4.24 and 4.25. This is an indication that the bottleneck situation discussed in Section 4.2.1 is not taking place at the VPN gateway. Unlike the setup considered in Section 4.2.1, the VPN gateway forwards its outbound traffic to a wired IEEE 802.3 Ethernet interface. This can be seen as a possible reason for such bottleneck situations to not arise.

As seen before, all CPU utilisation graphs in Figures 4.24 and 4.25 show a momentary change at the time of fragmentation. The effect of the IPSec VPN on the UDP flow, as discussed in Section 4.3.1, can be pointed out as a possible cause for such variations.
Chapter 1 – Analysis of Performance Results

Figure 4.24: CPU Utilisation for Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.25: CPU Utilisation for Traffic Generated at 5 ms Inter-packet Delay.
2.2 Round-trip Delay

This is the average time (delay) taken by a packet to complete one full trip from source to destination and back. This section further describes how approximate speculations can be made on the regions where queues are formed, by analysing this metric. Such information may also point to various bottlenecks in the VPN.

4.4.1 Round-trip Delay Analysis for a Single Wireless VPN

In our experiments, the round-trip delay measure for a UDP datagram is considered as the average time taken to complete one full trip from source to destination and back. This measure is vital for checking queuing delays. Figures 4.26 and 4.27 represent the round trip delay curves for UDP traffic with inter-packet delays of 1 ms and 5 ms respectively.

The graphs in Figures 4.26 and 4.27 show that, at faster packet generation rates, the average time taken for a UDP datagram to complete a round trip is relatively longer. This result is contradictory to what would normally be expected. In Section 4.2.1, it was mentioned that at faster packet generation rates, there is a relatively larger queue forming at the interface. Therefore, an average packet experiences a higher amount of queuing delay until it is actually transmitted by the interface. Thus, relatively high round-trip delays can be noted in Figure 4.26 in comparison to Figure 4.27.

The graphs in Figure 4.26 also show a sudden increase in the round-trip delay for UDP packets with light payloads. This is related to the bottleneck situation described in Section 4.2.1. The round-trip delay graphs in Figure 4.27 do not display such behaviour for light payloads. Hence, this confirms that when the inter-packet generation gap is increased, the effects of this bottleneck are not as predominant as they were in the past. Lastly, in both Figures 4.26 and 4.27, there are significant jumps in the round-trip delay graphs to be noted at the point of fragmentation. This is primarily due to the sudden overheads of fragmentation. Further, Figure 4.26 helps us to reach a general conclusion that the majority of packet losses are due to queuing delays, in comparison with delays caused by other errors attributable to the wireless channel.
Figure 4.26: The Round-trip Delay Graphs for Traffic Generated with a 1 ms Inter-packet Generation Gap.

Figure 4.27: The Round-trip Delay Graphs for Traffic Generated with a 5 ms Inter-packet Generation Gap.
4.4.2 Round-trip Delay Analysis for a Multiple Wireless VPN

As mentioned previously, the round-trip delay measure is vital for observing queuing delays. Figures 4.28 and 4.29 represent the round-trip delay curves for UDP traffic with inter-packet delays of 1 ms and 5 ms respectively. The graphs in Figures 4.28 and 4.29 show that, at faster packet generation rates, the average time for a given UDP datagram to complete one full round trip is relatively longer. This applies to the baseline as well as all VPN implementations. As mentioned in Section 4.2.2, at faster packet generation rates, there is a relatively larger queue forming at the interface. Therefore, an average packet usually experiences a higher amount of queuing delay before it is actually transmitted by the interface. Thus, relatively high round-trip delays can be noted for VPNS represented by the graphs in Figure 4.28 in comparison to those shown in Figure 4.29.

Figure 4.28 also shows a sudden increase in the round trip delay for UDP packets with light payloads at higher packet generation rates. This is related to the bottleneck situation described in Section 4.2.2. The round trip delay graphs in Figure 4.29 do not indicate such behaviour for light payloads at lower packet generation rates. Figure 4.29 shows significant jumps in the round-trip delay graphs beyond the point of fragmentation. This is mainly due to

![Figure 4.28: Round-trip Delay for Traffic Generated at 1ms Inter-packet Delay.](image)
the increased queue lengths as a result of the overheads of fragmentation. However, the corresponding graphs for multiple VPNs in Figure 4.28 behave differently. As discussed in Section 4.3.2, for high packet generation rates, the IPSec VPN may contribute to a temporary reduction in queuing, as a result of fragmentation. Hence, Figure 4.29 shows a reduction in the round-trip delay when multiple VPNs are in operation.

4.4.3 Round-trip Delay Analysis for a Site-to-Site VPN

As discussed in Sections 4.4.1 and 4.4.2, the round-trip delay measure for a UDP datagram is considered as the average time taken to complete one full trip from source to destination and back. Figures 4.30 and 4.31 represent the round-trip delay curves for UDP traffic with inter-packet delays of 1 ms and 5 ms respectively. For analysis and evaluation, the round-trip delay graphs in Section 4.4.1 (that is, Figures 4.26 and 4.27) are incorporated into Figures 4.30 and 4.31.

As expected, the graphs in Figure 4.30 and 4.31 show that the average time taken for a UDP datagram to complete a round trip in a site-to-site VPN implementation is relatively longer. The geographical distance between the two campuses, routing and the performance of the microwave link can be pointed out as possible contributors to relatively longer delays. When UDP packets are queued up to such long delays, as described in Section 4.2.1, a high
packet loss rate can also be expected (as shown by Figures 4.16 and 4.17). Therefore, this graph confirms that the majority of packet losses are due to queuing delays, in comparison with delays caused by other errors attributable to the wireless channel.

When the round trip delay graphs for the site-to-site IPSec VPN are compared with the round-trip delay graphs in Section 4.4.1, it can easily be noted that the basic trends in the behaviour of the delay metric have not been subjected to considerable changes. Therefore, the sudden increase in the round-trip delay for UDP packets with light payloads and the significant jump in delay at the fragmentation point are expected for a site-to-site VPN.

![Round-trip Delay Graph](image)

*Figure 4.30: Round-trip Delay for Traffic Generated at 1 ms Inter-packet Delay.*
2.5 Jitter

Jitter is the mean variation of delays on packets received. The delay metric considered in computing jitter is the round-trip delay measured and analysed in Section 4.4. Therefore, the measured jitter under this study can also be interpreted as the mean two-way variation in delay. This section provides a comprehensive analysis of jitter and its behaviour in various VPN implementations.

4.5.1 Jitter Analysis for a Single Wireless VPN

In our experiments, the jitter measure for a UDP datagram is considered as the mean variation of time taken to complete one full trip from source to destination and back. This is a vital QoS measure for checking the performance of a wireless VPN. Figures 4.32 and 4.33 represent the jitter graphs for UDP traffic with inter-packet delays of 1 ms and 5 ms respectively.

The graphs in Figures 4.32 and 4.33 show that, at faster packet generation rates, the jitter for a UDP flow is relatively higher. In Section 4.2.1, it was mentioned that at faster packet generation rates, a relatively higher congestion and queuing forms at the interface. Due
to such congestion and improper queuing at the interface, the outbound UDP stream becomes lumpy with varying inter-packet intervals. Therefore, an average packet experiences a varied delay until it is actually transmitted by the interface. Therefore, relatively higher jitter is noted in Figure 4.32. On the other hand, for a relatively slower packet generation rate, such congestion does not build up. Hence Figure 4.33 shows minimal levels of jitter.

The graphs in Figure 4.26 indicate a sudden increase in the round-trip delay for UDP packets with light payloads. Figure 4.32 shows that this results in a sudden increase in jitter for data payload sizes from 25-75 bytes. The jitter graphs in Figure 4.33 do not display such behaviour for light payloads. Lastly, in both Figures 4.32 and 4.33, there are significant jumps in the jitter graphs to be noted at the point of fragmentation. This is primarily due to the sudden overheads of fragmentation. Further, Figure 4.32 indicates that the variation of the queuing delay or jitter may also have contributed to the dropping of UDP packets. In contrast, Figure 4.33 shows minimal amounts of jitter for a UDP flow with a relatively higher inter-packet generation rate.

![Graph showing comparison of baseline and IPSec VPN delay and jitter across different UDP payload sizes](image)

*Figure 4.32: The Jitter Graphs for Traffic Generated with a 1 ms Inter-packet Generation Gap.*
Chapter 1 – Analysis of Performance Results

Figure 4.33: The Jitter Graphs for Traffic Generated with a 5 ms Inter-packet Generation Gap.

4.5.2 Jitter Analysis for a Multiple Wireless VPN

As mentioned previously, jitter is a measure which is vital for measuring performance in wireless networks. Figures 4.34 and 4.35 represent the jitter graphs for UDP traffic with inter-packet delays of 1 ms and 5 ms respectively. The graphs in Figures 4.34 and 4.35 show that, at faster packet generation rates, the average variation of delay for a UDP datagram to complete one full round trip is relatively longer. Section 4.5.1 showed that this applies to the baseline as well as to a single VPN. This section shows that it also applies to multiple VPN implementations. As mentioned in Sections 4.2.2 and 4.3.2, at faster packet generation rates, there are relatively larger queues and delays forming at the interface in multiple VPN setups. This delay also seems to increase with the increasing number of VPNs. Therefore, an average packet usually experiences a higher amount of queuing delay before it is actually transmitted by the interface. Thus, relatively high jitter can be noted for VPNs in Figure 4.34, in comparison to those shown in Figure 4.35.
Chapter 1 – Analysis of Performance Results

Figure 4.34: The Jitter Graphs for Traffic Generated at 1ms Inter-packet Delay.

Figure 4.35: The Jitter Graphs for Traffic Generated at 5 ms Inter-packet Delay.
Figure 4.34 also shows a sudden increase in jitter for UDP packets with light payloads at higher packet generation rates. This is related to the bottleneck situation described in Section 4.2.2. The round-trip delay graphs in Figure 4.35 do not indicate such behaviour for light payloads at lower packet generation rates. Nevertheless, Figure 4.35 shows significant jumps in the jitter graphs beyond point of fragmentation.

This is mainly due to the increased queuing delays as a result of the overheads of fragmentation. Despite the low jitter mentioned for a UDP flow with relatively high inter-packet delay, Figure 4.35 shows an interesting rise in jitter for payload data sizes from 400 to 600 bytes. Close observation shows that such a rise is only noted in the case of three simultaneous VPN implementations. The corresponding CPU utilisation graphs in Section 4.3.2 also shows that at this point the average CPU utilisation was approaching 100%. This proves that CPU exhaustion may also contribute to the jitter of a data flow.

4.5.3. Jitter Analysis for a Site-to-Site VPN
As discussed in Sections 4.5.1 and 4.5.2, the jitter measure for a UDP datagram is considered as the mean variation of time taken to complete one full trip from source to destination and back. Figures 4.36 and 4.37 represent the round-trip delay curves for UDP traffic with inter-packet delays of 1 ms and 5 ms respectively. For analysis and evaluation, the jitter graphs in Section 4.5.1 (that is, Figures 4.32 and 4.33) are incorporated into Figures 4.36 and 4.37.

As expected, the graphs in Figures 4.36 and 4.37 show that the average variation of delay for a UDP flow completing a round trip in a site-to-site VPN implementation is relatively higher. The network congestion and improper queuing taking place between the two geographically distant nodes located in the two campuses can be pointed out as the main contributors to jitter. Amongst other contributors to delay and jitter are routing, performance of the VPN gateways/tunnel end-points, and the performance of the microwave link.
Chapter 1 – Analysis of Performance Results

Figure 4.36: The Jitter Graphs for Traffic Generated at 1 ms Inter-packet Delay.

Figure 4.37: The Jitter Graphs for Traffic Generated at 5 ms Inter-packet Delay.
When the jitter graphs for the site-to-site IPSec VPN are compared with the jitter graphs in Section 4.5.1, it can easily be noted that the basic trends of the curve have not been subjected to considerable changes. The sudden increase in jitter for UDP packets with light payloads and the significant jump at the fragmentation point can be noticed in the new curve as well. Additionally the new graph has a trend in showing higher levels in the variation of delay.

The analysis of the performance data collected on throughput, packet loss, CPU utilisation, round-trip delay and jitter points out many trends in behaviour. Interestingly enough, many QoS parameters indicated that they had multiple effects on the behaviour of each other. It further shows that optimal QoS levels may be achieved by regulating various external parameters. The next chapter combines and summarises the above two facts by providing a comprehensive analysis of the behaviour of many QoS metrics under various circumstances.
Chapter 5 – Performance Limitations and Causes

Chapter 5

Performance Limitations and Causes

The previous chapter provided a comprehensive analysis of the behaviour of many QoS metrics under various circumstances. This chapter identifies the specific performance-limiting causes for each QoS metric. The first section discusses the specific causes that affect the throughput of a wireless VPN. Packet loss and round-trip delay are investigated subsequently and highlight how the optimal QoS levels can be achieved.

5.1 Throughput: Limitations and Causes

This section investigates some of the performance-limiting factors affecting the throughput of a wireless IPSec VPN. From all the performance-limiting factors outlined in the throughput analysis sections of Chapter 4, two types of causes can be determined. The first category relates to the protocol design of the IEEE 802.11 standard and the IPSec protocol. The medium-access schema (CSMA/CD), preambles of the transmitted frames, MAC headers, ACK frames, transmission protocol overheads, processing delays in stations, forwarding delays around the APs and the random back-off periods are amongst such overheads that may affect throughput. The second category relates to external causes such as the packet generation rate, payload data size, number of simultaneously operating VPNs and CPU processing power.

Figures 4.1 and 4.2 of Section 4.1.1, clearly establish the fact that the effective net throughput depends on the transmitter’s packet generation rate. The faster the packet generation rate, the higher the amount of payload data transferred in a unit of time, and thus, the higher the net throughput. These results also show that the throughput increases with the payload data size and the maximum achievable throughput is reached prior to fragmentation.

As discussed in Section 4.1.2, when simultaneously operating multiple VPNs are increased beyond a certain point, the rate of increase in throughput against the payload data size drops gradually. The analysis of the CPU utilisation in Section 4.3.2 (Figure 4.5) also shows that the CPU is fully exhausted at this stage. This also indicates that the current hardware configuration may not be able to fully handle any further simultaneous VPN
connections. Figure 5.1 illustrates the effect of CPU on the throughput of simultaneously operating IPSec VPNs. The 3D mesh graph represents the three throughput curves: a single, two and three simultaneous IPSec VPNs respectively. As the CPU approaches full utilisation (that is, close to 100%), the rate of increase in throughput shows a noticeable reduction. Furthermore, this phenomenon can only be noticed for relatively large payload sizes (that is, 600 bytes and above). Therefore, it is clear that the CPU is a major contributing factor to the throughput performance of an IPSec VPN.

![Figure 5.1: Variation of Throughput and CPU Utilisation against Payload Data Size.](image)

The above graph also indicates that as the number of simultaneously operating tunnels are increased, the per tunnel throughput performance degrades. Section 4.1.2 provides a detailed analysis on the per tunnel throughput levels for multiple IPSec VPN implementations. Last but not least, Figures 4.6 and 4.7 shows that the geographical distance between nodes was not proven to affect the throughput performance at the transmitter. It also suggests that by off-
loading the IPSec encryption and tunnel maintenance to a designated VPN gateway, higher throughput performance levels can be achieved. Furthermore, it shows that routing and link quality have a minimal effect on throughput.

5.2 Packet Loss: Limitations and Causes

This section outlines the limitations and causes of packet loss based on the analysis performed in Section 4.2. Some of the standard causes are the inherent behaviours of the operating system (causing UDP buffer limitations), the operational nature of the IEEE 802.11 standard and the performance of the network interface card. Although the analysis points out how these may effect the overall packet loss, the objective of this study is not to identify the flaws in the existing standards.

Interestingly enough, these experimental results reveal vital information as to how external parameters can be controlled to achieve best performance levels. For instance, the analysis shows that the payload data size and the inter-packet generation rate of a data flow may contribute to the degree of packet loss. The packet loss graphs in Section 4.2 show that the faster the packet generation rate, the higher the packet loss. It also shows that the larger the payload data size, the higher the packet loss (irrespective of the inter-packet generation rate). This section also points out that relatively lighter UDP payload data sizes (25-50 bytes) result in high packet losses for data flows with higher inter-packet generation rates. Hence there remains a region where minimal packet loss is recorded. Therefore, irrespective of the networking infrastructure, by regulating the payload data size and inter-packet generation rate to its optimal levels, minimal packet loss may be achieved.

Another interesting observation from the graphs in Section 4.2 (Figures 4.8 and 4.12) is that there are some instances where the data flow of an IPSec VPN experiences less packet loss in comparison to its baseline readings. This phenomenon can only be observed for data flows with higher packet generation rates. As the inter-packet generation gap of the data flow is increased, the above phenomenon is not to be seen. Therefore, it can be concluded that due to the encryption and tunnelling overheads of the IPSec VPN tunnel the data flow may experience a reduction in its flow. The reduction in the data flow results in a lower packet loss.
The investigations into the contributions of simultaneously operating VPNs and the CPU utilisation reveal another potential cause for packet loss. The packet loss graphs in Figure 4.15 shows a sudden increase in packet loss for the curve representing three IPSec VPNs. Such an exceptionally high level of packet loss is not observed for the rest of the curves. An investigation into the CPU utilisation graph (Figure 4.23) shows that the CPU is fully exhausted at this point. Thus, due to the overheads of the increasing numbers of VPNs the CPU becomes over-exhausted, resulting in a sudden increase in packet loss. Figure 5.2 illustrates the effect of the CPU on packet loss of simultaneously operating IPSec VPNs. The 3D mesh graph represents the three packet loss curves: a single, two and three simultaneous IPSec VPNs respectively. As the CPU approaches full utilisation (that is, close to 100%), the packet loss shows a noticeable increase. Furthermore, this phenomenon can only be noticed for relatively large payload sizes (that is, 600 bytes and above). Therefore, it is clear that the CPU is a major limiting factor for the performance of an IPSec VPN.

![Figure 5.2: Variation of Packet Loss and CPU Utilisation against Payload Data Size.](image-url)
Another interesting point to note is how the packet loss of simultaneously operating IPSec VPNs increases with increasing throughput, illustrated by Figure 5.3. As the throughput performance approaches its peak (that is, close to 6 Mbps), the packet loss shows a noticeable increase. As in the case in Figure 5.2, this trend can also be noticed for relatively large payload sizes (that is, 600 bytes and above). This also indicates that extreme throughput performance levels may result in higher packet loss rates under multiple VPN tunnel implementations.

![Figure 5.3: Variation of Packet Loss and Throughput against Payload Data Size.](image)

Lastly, as indicated by Figures 4.16 and 4.17 in Section 4.2.3, it is clear that the geographical distance between the VPN tunnel end-points contributes to the packet loss. One of the main reasons behind such high UDP packet loss with increasing geographical distance is the increase in delay, as per the explanations provided in Section 4.4. The other major contributor to this high packet loss is the performance impairments of the microwave link connecting the two campuses. The impact of the performance of the routers on the packet loss can be considered to be minimal.
5.3 Round-trip Delay: Limitations and Causes

This section outlines the limitations and causes for round-trip delay, based on the analysis performed in Section 4.4. As mentioned in the above sections, some of the standard causes for delay are the operational nature of the IEEE 802.11 standard (medium-access schema, preambles of transmitted frames, MAC headers and ACK frames, random back-off periods, etc.), processing delays in stations and access points, and the performance of the network interface cards. Apart from the abovementioned causes, the analysis in Section 4.4 points out that external causes such as packet generation rate, payload data size, CPU processing power, number of simultaneously operating VPNs, transmission impairments of links and geographical placement of the VPN gateways also have a considerable effect on delay. The analysis presented in Section 4.4.1 clarifies that the above causes lead to queuing at the interface, which somehow contributes to the overall increase in round-trip delay.

The round-trip delay graphs (Figures 4.26 and 4.27) in Section 4.4.1 show that the faster packet generation rate, the higher the round-trip delay. As the analysis explains, for relatively higher packet generation rates, larger queues form at the interface, causing longer round-trip delays. The analysis also points out a sudden increase in the round-trip delay for UDP packets with light payload sizes (25–75 bytes). It indicates the bottleneck situation described under Section 4.2.1 as the cause of such behaviour. The round-trip delay noticed for these low payload sizes can also be noticed for multiple VPN implementations as well as VPN tunnels over multiple platforms (Figures 4.28 and 4.30). Unlike the case of packet loss, there is no considerable increase in the round-trip delay for higher payload data sizes up to the point of fragmentation. By careful analysis a region that has been subjected to minimal round-trip delay can be identified. Therefore, minimal round-trip delay can be achieved for a given link by regulating the payload data size and inter-packet generation rate to its optimal levels.

Another noteworthy point is the sudden increase in round-trip delay in the setup of three simultaneous VPN implementations (Figure 4.29). Such an exceptionally high level of round-trip delay cannot be noted for the remaining graphs of Figure 4.29. The analysis and investigation of this phenomenon led to the identification of another potential cause for round-trip delay; the CPU processing power. An investigation into the CPU utilisation graph (Figure 4.23) shows that the CPU is fully exhausted at this point. The overheads of the increasing
numbers of VPNs led the CPU to such exhaustion. This also caused a sudden increase in packet loss for three simultaneous IPSec VPN implementations, as discussed in Section 5.2. Figure 5.4 illustrates the effect of the CPU on the round-trip delay of simultaneously operating IPSec VPNs. The 3D mesh graph represents four round-trip delay curves. They correspond to the baseline, a single, two and three IPSec VPN connections respectively. As the CPU approaches full utilisation (that is, close to 100%), the round-trip delay shows a noticeable increase. Moreover, this phenomenon can only be noticed for relatively large payload sizes (that is, 600 bytes and above). Hence it is clear that the CPU can act as a major limiting factor on the round-trip delay of an IPSec VPN.

![Graph showing variation of round-trip delay and CPU utilisation against payload data size.](image)

**Figure 5.4: Variation of Round-trip Delay and CPU Utilisation against Payload Data Size.**

The graphs in Figures 4.30 and 4.31 point out that the geographical distance between the VPN tunnel end-points and the quality of the microwave link connecting the two campuses also affect the round-trip delay metric. The increase in delay also gives rise to the packet loss discussed in Section 5.2.
5.4 Jitter: Limitations and Causes

Jitter is defined as the variation in delay of the received packets. The analysis in Section 4.5 points out various trends and behaviour of jitter in wireless VPN implementations. This section discusses the limitations and causes for jitter, based on the analysis performed in Section 4.5. As mentioned previously, some of the standard causes for delay and jitter are the processing delays and congestion taking place at stations, access points, switches, routers, and the network interface cards. Apart from the abovementioned causes, the analysis in Section 4.5 also highlights that packet generation rate, payload data size, CPU processing power, number of simultaneously operating VPNs, transmission impairments of links and geographical placement of the VPN gateways may also impose a considerable effect on jitter. The analysis presented in Section 4.5.1 also explains how congestion and improper queuing at the interface may result as jitter in the data flow.

The round-trip delay graphs (Figures 4.32 and 4.33) in Section 4.5.1 point out that the faster the packet generation rate, the higher the jitter. As the analysis explains, for relatively higher packet generation rates a relatively higher congestion and queuing forms at the interface. The analysis also points out a sudden increase in jitter for UDP packets with light payload sizes (that is, 25-75 bytes). The jitter noticed for these low payload sizes can also be noticed for multiple VPN implementations as well as VPN tunnels over multiple platforms (Figures 4.34 and 4.36).

The round-trip delay does not show a considerable increase for UDP flows with increasing payload data sizes up to the point of fragmentation. Thus all graphs show a minimal jitter in this region. Hence a range in UDP payload data size that is subject to minimal delay can be identified. Therefore, minimal jitter levels can be achieved for a given link by regulating the payload data size and inter-packet generation rate within its optimal levels.

Another interesting point is the sudden rise in jitter in the setup of three simultaneous VPN implementations (Figure 4.35). Such a trend in jitter cannot be noted for the remaining graphs of Figure 4.35. Figure 4.29 also confirms that this sudden rise in jitter corresponds with the sudden rise in round-trip delay for the setup of three simultaneous VPN implementations. As described in Section 5.3, an investigation into the CPU utilisation graph (Figure 4.23) shows that the CPU is overwhelmed and exhausted by this point. The high overheads of the increasing numbers of VPNs are the contributors to the CPU’s exhaustion. This also caused a
Chapter 5 – Performance Limitations and Causes

sudden increase in packet loss and an increase in round-trip delay for the three simultaneous IPSec VPN implementations. Therefore, as the CPU approaches its full utilisation (that is, close to 100%), the variation in delay or jitter shows a noticeable increase. Furthermore, this phenomenon can only be noticed for relatively large payload sizes (that is, 600 bytes and above). Hence it is clear that the CPU may act as an external factor contributing to the jitter of the data flow of an IPSec VPN.
Chapter 6

Summary, Conclusions and Future Work

The aim of this thesis is to evaluate and establish the performance and QoS levels of a virtual private network operating over a wireless infrastructure. The main focus of the research is to identify the major performance limitations and their underlying causes for wireless VPN implementations under various practical scenarios.

The experimentation and data collection spans over a number of platforms to suit a range of practical VPN implementations over a wireless medium. Firstly, a series of experiments are conducted to analyse the QoS behaviour of a single IPSec VPN operating over an IEEE 802.11b wireless infrastructure. Vital measures of various QoS parameters of the VPN link are observed and recorded for each experiment and scenario. Such parameters include the application throughput, packet loss, round-trip delay and jitter. The experimental results are then compared against the baseline performance results of a wireless link. Subsequently this experimentation and data collection is extended to a platform of simultaneously operating multiple VPN setups. This aims at studying the behaviour of QoS metrics and measures in a multiple VPN setup over a wireless link. The last stage of the experiment is to construct a site-to-site VPN by deploying two specific VPN gateways across multiple subnets, platforms and geographical locations. Finally, the performance results of the site-to-site VPN are compared against the results of the previously performed experiments, based on the wireless VPN. The analysis illustrates how the QoS measures of a wireless VPN may vary from a typical site-to-site VPN implementation, their limitations and causes.

The substance of the derived results can be summarised as follows. The payload data size, inter-packet generation rate, number of simultaneously operating VPN connections, the geographical distance, and CPU processing power can be identified as major contributing factors towards the quality of service of a wireless VPN. The results of the analysis reflect that the throughput, packet loss and delay show an increasing trend as the payload data size and the inter-packet generation rate of the data flow increases. The analysis explains how a data flow with a relatively shorter inter-packet generation gap may give rise to a potential bottleneck at the interface, which will eventually contribute to the packet loss and delay.
Another interesting phenomena revealed from this research is that significantly high packet loss, delay and jitter are experienced by UDP datagrams with light payloads (that is, 25-50 bytes), generated at reasonably faster packet generation rates. The analysis indicates that when a wireless interface card is bombarded with a bi-directional flow of datagrams having relatively larger overheads than its actual payload data size, total traffic and contention can increase rapidly. Thus, under such circumstances a rapid decrease in the QoS of the link can be witnessed. The results and analysis also signify that there are substantial variations in the trends of the above QoS parameters as fragmentation of datagrams takes place.

The investigation into finding the causes of performance limitations for simultaneously operating multiple VPNs identifies the processing power of the CPU as a major contributor for the conditions under study. The performance results also indicate that as the numbers of simultaneously operating VPNs are increased, the QoS of each link rapidly deteriorates as a result of the CPU reaching its processing limits. Thus the selection and configuration of an appropriate hardware platform may sometimes help to overcome certain performance barriers.

The benefits of off loading the encryption and tunnelling, by deploying a designated VPN gateway, to the overall tunnel performance are also investigated. The improvement in the tunnel throughput is clearly one such benefit. The geographical distance between the two gateways does not seem to impose a substantial effect on the tunnel throughput. However, its effect on packet loss, delay and jitter is rather significant. In fact, the analysis indicates that the geographical distance between two VPN gateways may considerably reduce performance levels of such QoS parameters.

The results of this study can be used in defining acceptable performance and QoS levels for a wireless VPN configuration, under general enough conditions. By and large, this provides a guideline for predicting the behaviour of performance parameters, under such circumstances. Furthermore, these results can be used for estimating maximum possible throughput, percentage of packet loss, round-trip delay, and jitter for a specific data flow over a wireless VPN. Therefore, network operators and application developers can use these results to fine-tune application parameters for achieving optimal QoS levels and reliability over such wireless VPNs.

There is also the possibility of using these experimental data for advanced mathematical simulation and modelling. One such area is to implement queuing theory to analyse the
Chapter 6 – Summary, Conclusions and Future Work

statistical behaviour of queue length at the wireless interface to provide qualitative predictions of average packet delay. Another area is the application of the concept of Artificial Neural Networks (ANN). An ANN is a distributed parallel computing system which has the ability to extract patterns and detect trends from complicated or imprecise data. A trained ANN, using the collected data from the above experiments, can be used to provide projections, given new situations of interest, and answer “what if” questions.
References


References


References

References


References

