Fall-2011

University of Alberta

IMPACTS OF ENCRYPTION ON STREAMING VIDEO

By

Harpreet Lotey

Project report submitted to:
Department of Computer Science and Department of Electrical and Computer Engineering

In Partial fulfillment of the requirements for the Degree of
Master of Science in Internetworking

Supervised By:
Dr. Mike MacGregor

Abstract

Internet based communication have become one of the fastest and easiest way of communication in different sectors of the world such as military, health care, educational or business sectors. Due to the privacy and security of the data VPN encryption is commonly used method to transfer the video but it also involves overhead and delays. These delays and overhead are caused by encryption at the VPN concentrator and decryption at the client side. This project studies about the inter-packet delays in encrypted data and comparing it with unencrypted data. To get a clear picture about the inter-packet delays three different kinds of videos are involved.

.

Acknowledgements

I would like to express my thanks to my supervisor, Dr. Mike MacGregor, for helping me in deciding the research topic and his invaluable guidance and support through the course of this work.

Finally, I would like to thank my husband for his love, support and motivation he has given me.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

IP	Internet Protocol
VPN	Virtual Private Network
PSK	Pre-Shared Key
IKE	Internet Key Exchange
HMAC	Hash-based Message Authentication Code
DH	Diffie-Hellman
ESP	Encapsulating Security Payload
AH	Authentication Header
IPSec	Internet Protocol Security

Chapter 1

Introduction

Today we have huge networks with lot of bandwidth available which has increased popularity of video based applications that are being used everywhere both at personal and professional levels. It is being used in health sector, monitoring city traffic, security systems for residential and commercial purposes, professional video conferencing, personal video chat and many other places. It has made world a small place where there is no need to travel long distance to conduct businesses. But there is a risk involved with it. The important data which has to be transferred between VPN client and VPN server is always vulnerable to unauthorized interception [4].
This raises concerns about security and confidentiality of data being transferred especially in health sector where these things are given utmost priority. Thankfully, there is a way to solve this problem. The video data that needs to be transferred can be transferred in encrypted form. The data gets encrypted at server side and then decrypted at client using certain protocol. But this data needs to be transferred in real time and if the data has to be encrypted it can cause major delays [1]. This project is focused on studying these delays, so, that we know approximation value of how much delay it can add.

1.1 VPN

If we need to transfer data to someone who is not in our network but in network which is very far away we need to use internet. But data packets transferred between two devices is not secure as it is vulnerable to attackers on the internet. So, to eliminate this problem we use Virtual Private Network (VPN). It is a security tool which allows secure communication of packets through internet as it is on some kind of a private leased line or network [2].

VPN eliminates the risk of unknowingly accepting data from attackers. VPN also encrypts the data packets. So, even if attacker is able to get a copy of encrypted data, he or she won't be able to read it [2].

VPN is of two types:

1) Access VPN: It securely connects small office or a home user with a remote PC.
2) Site to Site intranet VPN: It provides secure connection between two networks of an enterprise located far away from each other.

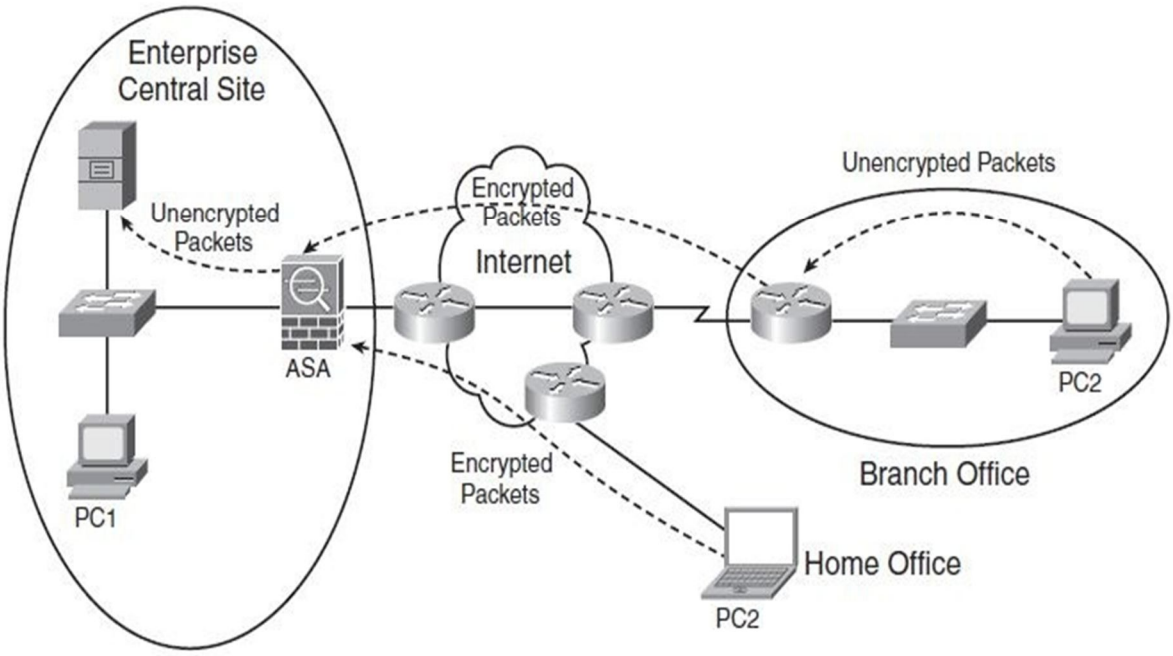

Figure 1: Virtual Private Network [2]

Lease lines provide some useful security features some of which are inherited by VPN and are as follows:

- Privacy: It doesn't allow anyone to ready the message in-between the transmission over the internet
- Authentication: The sender of the VPN packet is verified to be a genuine device rather than an invader
- Data Integrity: Packet is verified as not being changed during the transmission
- Antireplay: It prevents attacker to copy packets and resend them pretending to be a genuine user

1.2 IP Security (IPSec) VPNs

For any IP network IPSec is a framework for security services which defines a set of functions and rules like authentication and encryption [3]. In other words IpSec provides encryption for data packets to be sent from VPN client to VPN server over the internet.

1.2.1 IPSec Encryption

It uses a pair of encryption algorithms to encrypt data packets and decrypt it back to original data packets. While encrypting it uses math formulas to create encryption key also known as secret password or shared session key. This encryption key would be required by VPN client to decrypt data packet. Encryption is designed in such a way that it generates different encryption key for different packets. So, even if attacker is able to decrypt one of the packets he/she won't be able to decrypt other packets.

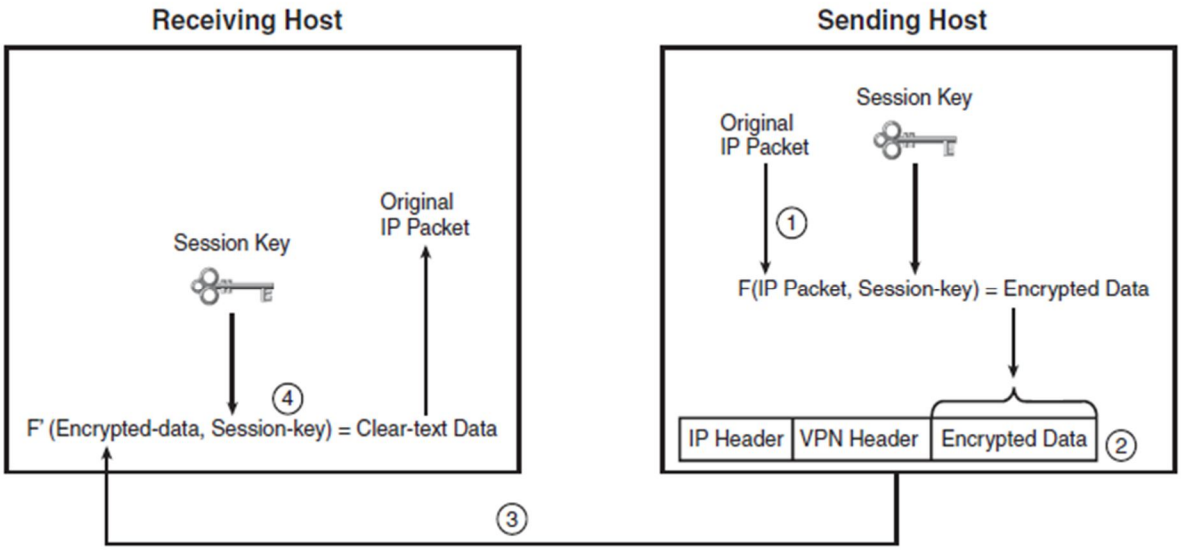

Figure 2: IPSec Encryption Process [3]

The process of IPSec Encryption takes place in four steps as illustrated by figure 2 which are explained as following:

1. The VPN server embeds the original data packet and the encryption key into the encryption formula.
2. The VPN server adds a new IP header and a VPN header and forms a new encrypted data packet.
3. The VPN server then transfers this new packet to VPN client.
4. The VPN client after receiving encrypted packet uses decryption formula and encryption key to decrypt the data [3].

1.2.2 IPSec Encryption Key Exchange

One of the important and very first step for secure transfer of data packets involve sharing of encryption key on both ends in a safe manner. Most of the time this process is done in two ways:

1. Pre-Shared Key (PSK) :
   This involves manually exchanging the encryption key on both VPN server and client. It may be a safe way to exchange key but it has a problem associated with it. It's in human nature that once the exchange key has been setup it won't be changed anytime soon. This compromises security of the whole system.

2. Dynamic Shared Key:
   It is also known as Internet key exchange (IKE) or Diffie-Hellman (DH) key exchange. It involves an algorithm which permits VPN server and client to exchange encryption keys securely. The length of DH keys depends upon the length of encryption keys. DH-1, DH-2 and DH-5 have a key length of 768, 1024 and 1536 bits respectively [3].

1.2.3 IPSec Message Integrity

IPSec authentication header (AH) protocol performs message integrity. It uses shared key hash function for encryption process known as Hash Message Authentication Code (HMAC). The ESP encryption doesn't use HMAC for data integration. The VPN server calculates the hash and adds it to a VPN header. The VPN client uses shared key to calculate hash and compares it to hash in header of received packet. If the hash value matches, then VPN client knows that data packet wasn't changed in transmission [3].

1.2.4 IPSec Authentication

This process uses public/private key which is shared between VPN server and client. The VPN client uses concept similar to the DH key exchange known as private key in this case and adds the value to VPN header. The VPN client uses public key to calculate private key and compares it to value it received in VPN header. If the value matches, client knows that it has received data packet from authentic source [3].

1.3 The ESP protocol and AH protocol

IPsec defines two security protocols to perform VPN functions. Both of them define their own header which gets added to original data packet. These protocols are:

1. The Encapsulating Security Protocol (ESP):
   The ESP protocol defines the rule to perform main four VPN functions of authentication, message integrity, encryption and antireplay.

2. The IP Authentication Header (AH):
   The IP AH protocol defines only authentication and message integrity. Either one of the features can be used or both of them can be used together.

1.4 Preferred Security Protocol

ESP performs all four major VPN functions of authentication, message integrity, encryption and antireplay. On the other hand AH has stronger Data authentication but doesn't perform major function of data encryption which is the major function required to transmit data in coded form. So, ESP is the preferred security protocol being used in this project.

Chapter 2

Project Implementation

2.1 Schematic of Implementation

The architecture used for implementation of project consists of following hardware and software:

- Cisco 3750 switch which helps in virtual routing and forwarding
- Cisco 2900 router
- Cisco 2800 router
- Vyatta VPN connector installed on Sunfire V20Z blade server helps in site-site VPN with Cisco router 2800
- VLC player is used on both server and client side to run three different videos
- Wireshark packet analyzer is used to capture the packets. It runs on one of the computer (sniffer) attached to switch 3750 to mirror the port G1/0/3

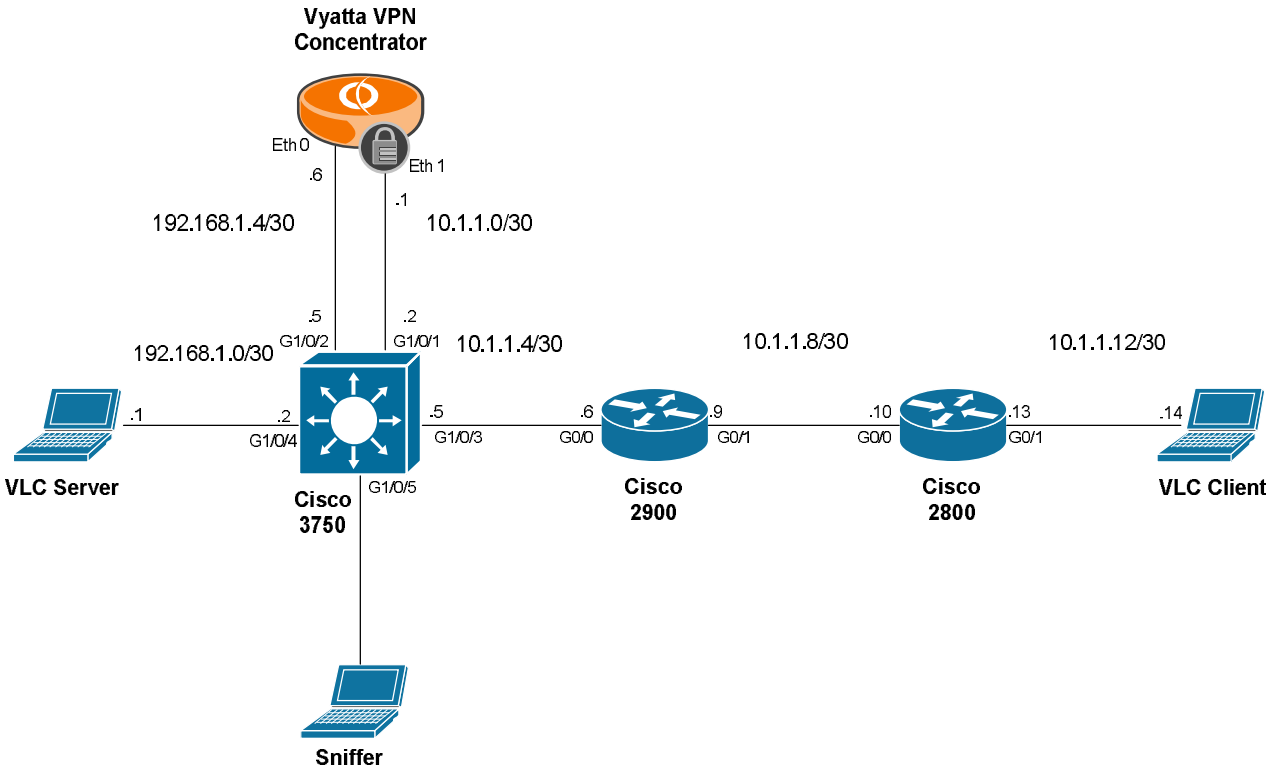

Figure 3: Schematic for Project Implementation

2.2 Implementation Scenarios

This schematic is used for various scenarios to evaluate inter-packet delay and overhead. The following scenarios have been implemented:

1. **Without encryption:**
   It involves capturing video packets between VLC server and client for unencrypted video.

2. **With encryption:**
   - It involves capturing video packets between VLC server and client for encrypted video.
   - IPsec encryption at the Vyatta VPN concentrator.

2.3 Policies used for testing

2.3.1 IKE Phase 1 negotiation criteria:

- Encryption algorithm: AES-256 (Health care standard)

- Hashing: SHA-1 (Md5 proven to be insecure)
- Authentication: pre-shared
- Key exchange: Diffie-Hellman Group 2
- Lifetime: 86,400 seconds

2.3.2 IPSec (IKE Phase 2) negotiation criteria:

- Encryption algorithm: esp-aes 256
- Authentication: esp-sha-hmac

2.3.3 Tunnel Parameter:

- Pre-shared key: letmein

2.4 Test Videos

Three videos were used for testing the scenarios both for unencrypted and encrypted scenarios. All three of them differ from each other in frames per second and mobility.

- A football video,
- In interview video, and
- A movie video.

Football has the highest mobility of characters in it where each frame is very different from other whereas interview video has the least where most of the frames remain same as there is no much movement of characters.

2.5 Inter Video-Packet Delay Measurement

Focus of the project is to calculate inter packet delay between video packets going from VPN server to VPN client. Port G1/0/3 of switch will be monitored for all outgoing and incoming data. But later on focus will be laid on video packets which will be filtered from rest of the packets using Wireshark.

Chapter 3

Implementation Results

VLC streaming was successfully run between server and client. Three different videos were played twice for approximate 2 minutes each, once for encrypted and another for unencrypted data capture. Sniffer was used to capture the data packets at port G1/0/3 of Cisco 3700 switch.

3.1 Summary of Encrypted and Unencrypted captured data

Table 1 gives the summary of Encrypted and Unencrypted captured data for the videos. It can be seen that for encrypted streams total numbers of packets as well as total number of bytes are more or almost double than for unencrypted ones.

Name of Video File	Total number of packets	Total Time B/W 1st & Last Packet(s)	Average Packets/Sec	Average Packet Size (Bytes)	Total Bytes
Football Unencrypted	8764	122.33	71.63	945.569	8286963
Football Encrypted	22562	122.98	183.45	1130.85	25514446
Interview Unencrypted	5393	125.2	43.07	820.47	4424819
Interview Encrypted	13849	125.69	110.181	991.629	13733065
Movie Unencrypted	7079	122.58	57.747	846.802	5994515
Movie Encrypted	18252	124.77	146.28	1030.43	18807446

Table1: Summary of Encrypted and Unencrypted captured data

3.2 Total number of bytes sent on the last hop to the receiver

Table 2 gives total number of bytes sent on the last hop to the receiver. The data was taken out by filtering ESP packet sent from 10.1.1.1 to 10.1.1.10 in encrypted videos. For unencrypted videos data was sent from 192.168.1.1 to 10.1.1.14. Total numbers of packets sent in encrypted videos are more than the unencrypted packets

Name of Video File	Total number of packets	Total Time B/W 1st & Last Packet(s)	Average Packets/Sec	Average Packet Size (Bytes)	Total Bytes
Football Unencrypted	6255	122.33	51.129	1300.60	8135266
Football Encrypted	13029	122.98	105.93	1307.31	17032990
Interview Unencrypted	3743	125.2	29.89	1155.31	4324347
Interview Encrypted	7992	125.69	63.63	1147.79	9173200
Movie Unencrypted	4943	122.58	40.32	1186.48	5864801
Movie Encrypted	10524	124.77	83.34	1193.46	12560008

Table 2: Total number of bytes sent on the last hop to the receiver

3.3 Payload Bytes

The payload packets for ESP packets in movie video sent from10.1.1.1 to 10.1.1.10 are most 1476 bytes and some of 372 bytes, 708 bytes, 868 bytes and 1380 bytes. The videos from 10.1.1.10 to 10.1.1.1 are 84 bytes. For unencrypted video most of the packets are 1460 bytes.

Similar kind of pattern is seen in football as well as interview videos are seen i.e 1476 bytes in ESP packets from 10.1.1.1 to 10.1.1.10. 84 bytes are sent from 10.1.1.10 to 10.1.1.1.

3.4 Total Number of bytes returned by receiver

Table 3 gives the total Number of bytes returned by receiver. In encrypted ESP packets sent from 10.1.1.10 to 10.1.1.1. For unencrypted the data sent from 10.1.1.14 to 192.168.1.1. Bytes returned by the receiver in encrypted videos are little more than unencrypted.

Name of Video File	Total number of Bytes returned by receiver
Football Unencrypted	2487
Football Encrypted	2954
Interview Unencrypted	1624
Interview Encrypted	1839
Movie Unencrypted	2105
Movie Encrypted	2440

Table 3: Total Number of bytes returned by receiver

1.5 Inter-video delays for video packets

First 20 packets were taken to measure inter-video delays in all three video clips for both encrypted and unencrypted data. This section explains it through a table and a histogram graph. The result shows VPN encrypted takes more time to travel from server to client than non-VPN encrypted videos.

3.5.1 Football Video

Following table and histograms represents inter video-packet delay for football video for first 20 samples

Encrypted			Unencrypted		
Packet #	Time	Inter Packet Delay	Packet #	Time	Inter Packet Delay
3	0.00023	0	1	0	0
4	0.000238	0.000008	2	0.000032	0.000032
6	0.000324	0.000086	4	0.09998	0.099948
8	0.000446	0.000122	5	0.100047	0.000067
10	0.000463	0.000017	7	0.100641	0.000594
11	0.000543	0.000080	8	0.199981	0.099340
13	0.000671	0.000128	9	0.20005	0.000069
14	0.000677	0.000006	11	0.339951	0.139901
15	0.000696	0.000019	12	0.340056	0.000105
16	0.000702	0.000006	14	0.399977	0.059921
17	0.000799	0.000097	15	0.400051	0.000074
18	0.000804	0.000005	17	0.500267	0.100216
24	0.100202	0.099398	18	0.500287	0.000020
25	0.10021	0.000008	20	0.500812	0.000525
27	0.100412	0.000202	22	0.601035	0.100223
29	0.100428	0.000016	23	0.601055	0.000020
31	0.100524	0.000096	25	0.681996	0.080941
32	0.100533	0.000009	26	0.682165	0.000169
34	0.100631	0.000098	27	0.682183	0.000018
35	0.100637	0.000006	29	0.802192	0.120009

Table 4: Inter Video Packet Delays of football video

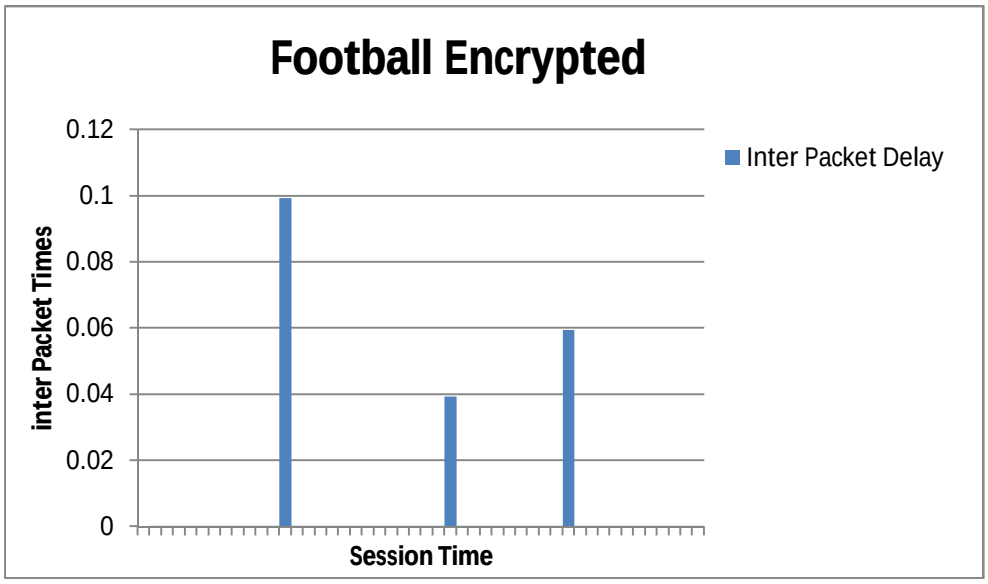

Figure 4: histogram for inter video-packet delays for encrypted football video

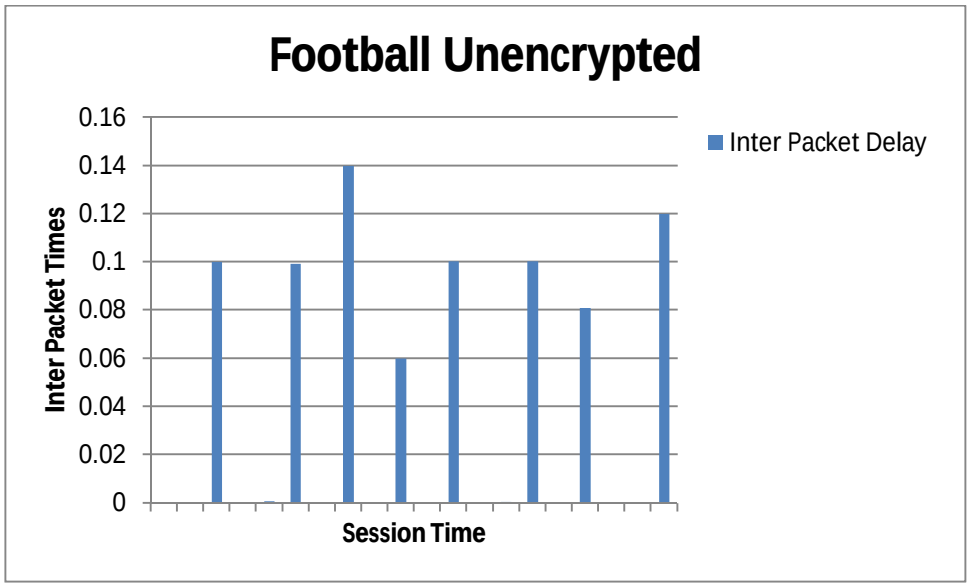

Figure 5: histogram for inter video-packet delays for unencrypted football video

3.5.2 Interview Video

Following table and histograms represents inter video-packet delay for interview video for first 20 samples

Encrypted			Unencrypted		
Packet #	Time	Inter Packet Delay	Packet #	Time	Inter Packet Delay
3	0.000202	0	1	0	0
4	0.00021	0.000008	2	0.000145	0.000145
5	0.000309	0.000099	3	0.000155	0.000010
6	0.000317	0.000008	6	0.039864	0.039709
10	0.100203	0.099886	7	0.120009	0.080145
11	0.100212	0.000009	8	0.120065	0.000056
12	0.100333	0.000121	10	0.120644	0.000579
13	0.100341	0.000008	12	0.219947	0.099303
17	0.180192	0.079851	13	0.22007	0.000123
18	0.180263	0.000071	14	0.220188	0.000118
19	0.180268	0.000005	17	0.319978	0.099790
20	0.180279	0.000011	18	0.320103	0.000125
23	0.185552	0.005273	19	0.320111	0.000008
24	0.185557	0.000005	21	0.320968	0.000857
27	0.300212	0.114655	23	0.420017	0.099049
28	0.300218	0.000006	24	0.420025	0.000008
29	0.300263	0.000045	26	0.420732	0.000707
30	0.300269	0.000006	27	0.520209	0.099477
34	0.340252	0.039983	28	0.520228	0.000019
35	0.340259	0.000007	30	0.5208	0.000572

Table 5: Inter Video Packet Delays of interview video

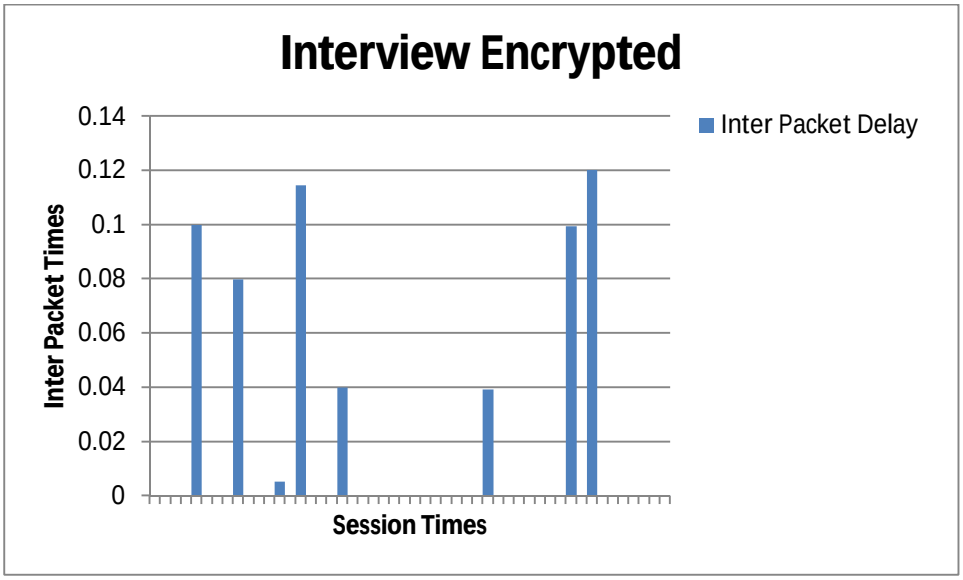

Figure 6: histogram for inter video-packet delays for encrypted interview video

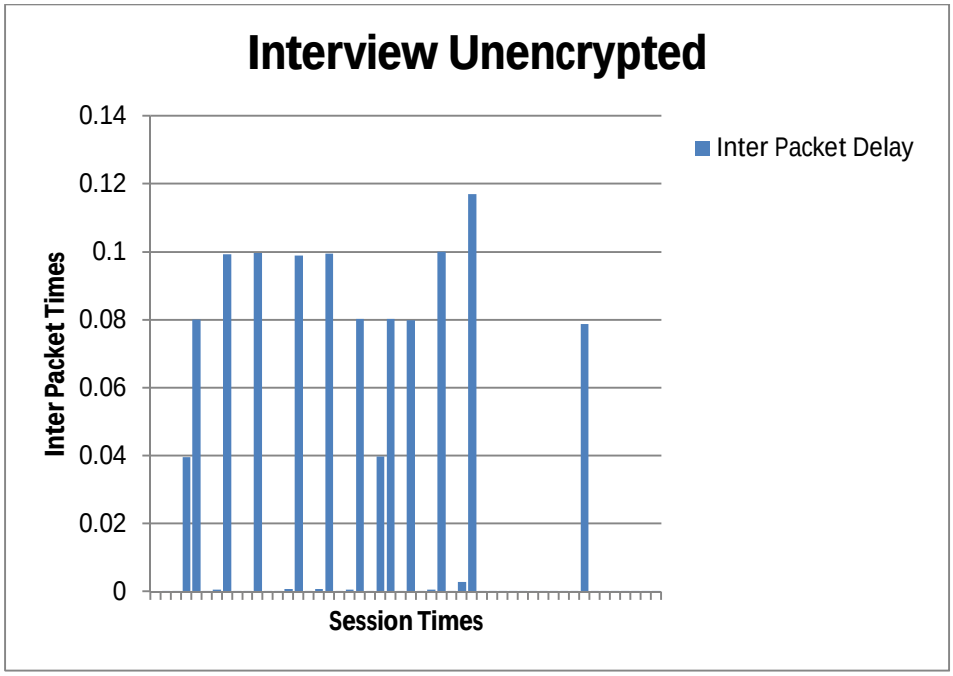

Figure 7: histogram for inter video-packet delays for unencrypted interview video

3.5.3 Movie Video

Following table and histograms represents inter video-packet delay for movie video for first 20 samples

Encrypted			Unencrypted		
Packet #	Time	Inter Packet Delay	Packet #	Time	Inter Packet Delay
3	0.00023	0	1	0	0
4	0.000238	0.000008	2	0.000059	0.000059
5	0.000245	0.000007	3	0.000153	0.000094
6	0.000252	0.000007	4	0.000259	0.000106
9	0.001729	0.001477	7	0.079581	0.079322
10	0.001737	0.000008	8	0.079658	0.000077
13	0.100265	0.098528	10	0.080301	0.000643
14	0.100271	0.000006	12	0.181568	0.101267
15	0.100277	0.000006	13	0.181712	0.000144
16	0.100283	0.000006	14	0.181719	0.000007
20	0.200253	0.099970	16	0.288616	0.106897
21	0.200261	0.000008	17	0.288697	0.000081
22	0.200368	0.000107	19	0.289306	0.000609
23	0.200376	0.000008	21	0.388628	0.099322
27	0.300216	0.099840	22	0.388636	0.000008
28	0.300294	0.000078	24	0.398747	0.010111
29	0.300299	0.000005	25	0.489693	0.090946
30	0.300305	0.000006	26	0.489832	0.000139
34	0.400374	0.100069	28	0.490397	0.000565
35	0.400382	0.000008	30	0.589808	0.099411

Table 6: Inter Video Packet Delays of movie video

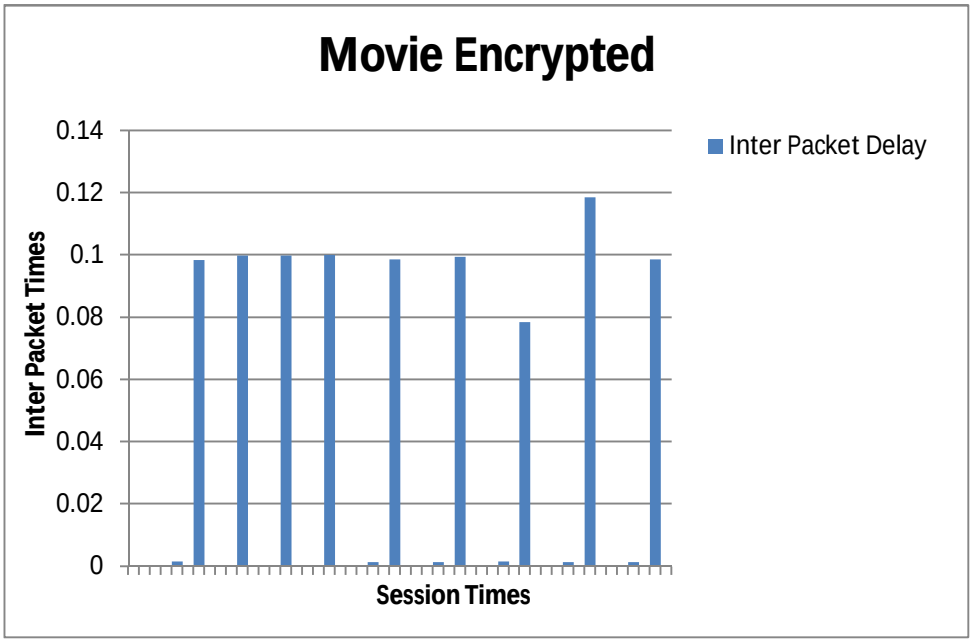

Figure 8: histogram for inter video-packet delays for encrypted movie video

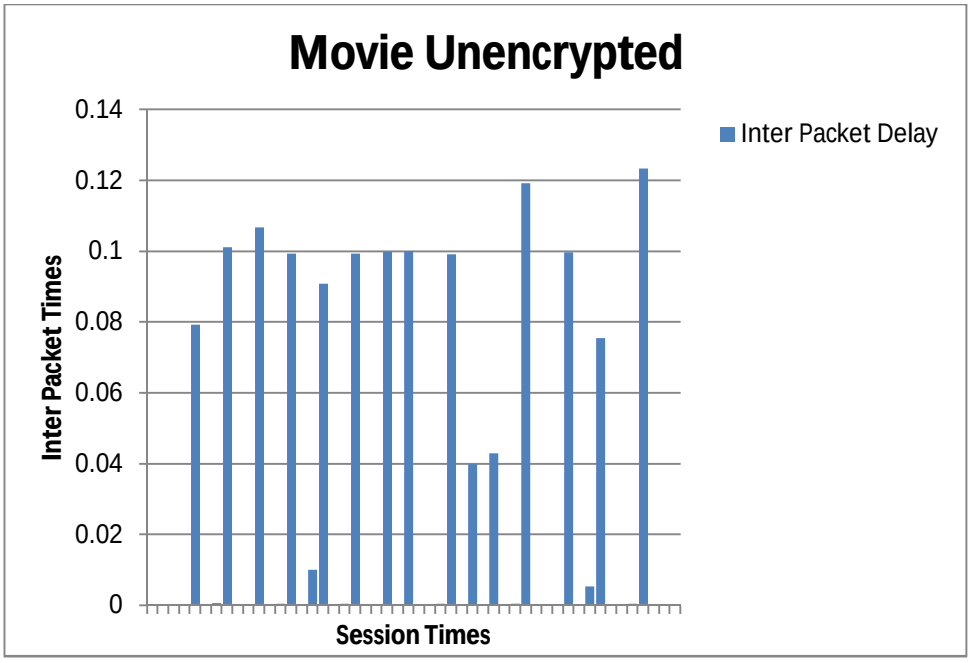

Figure 9: histogram for inter video-packet delays for unencrypted movie video

1.6 Average and Standard Deviation Graphs

3.6.1 Football

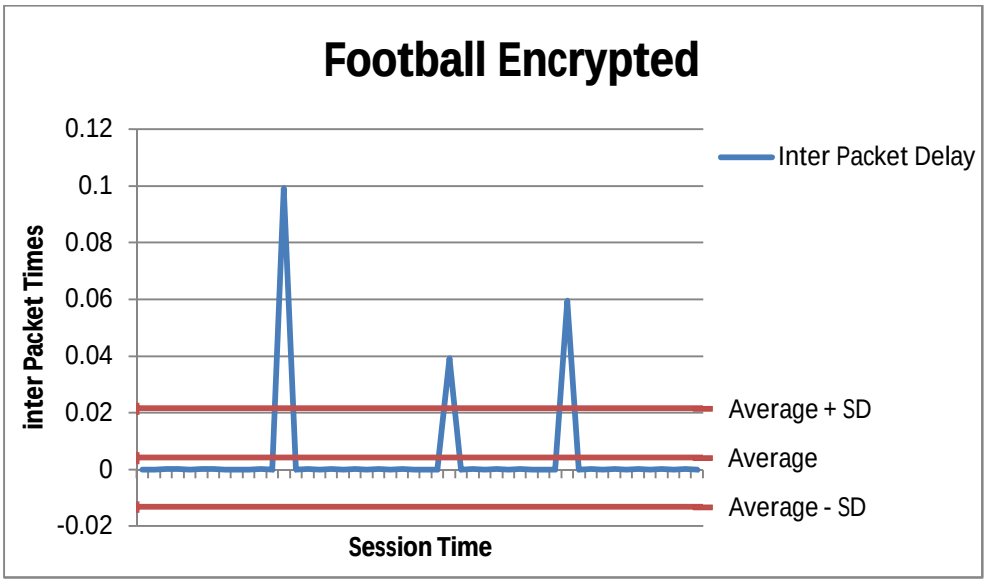

Figure 10: Average and Standard Deviation for football encrypted

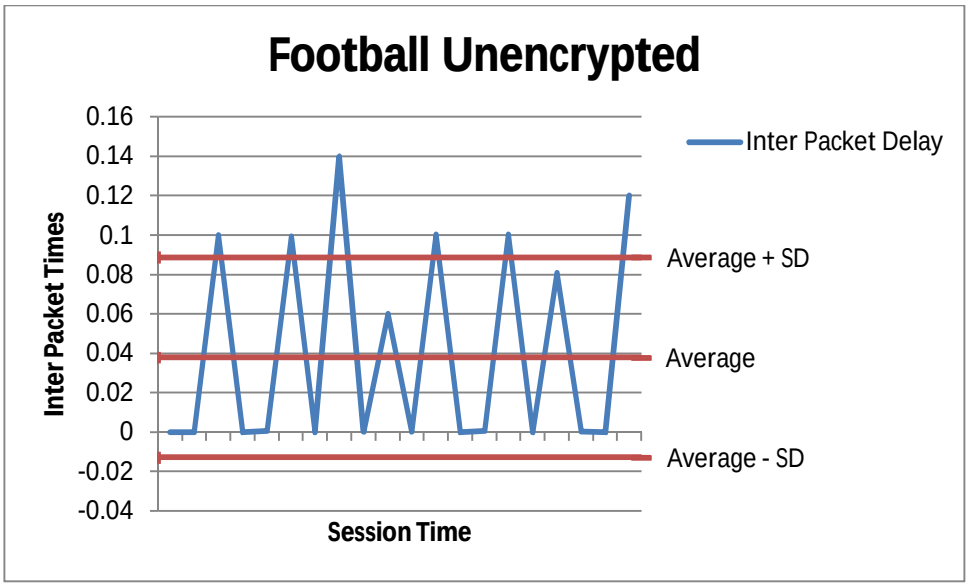

Figure 11: Average and Standard Deviation for football unencrypted

3.6.2 Interview

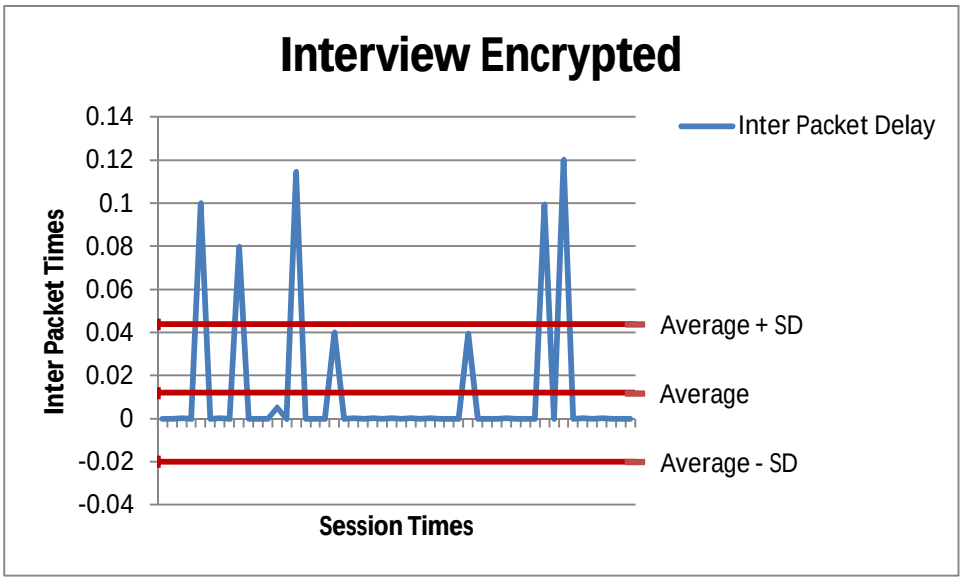

Figure 12: Average and Standard Deviation for interview encrypted

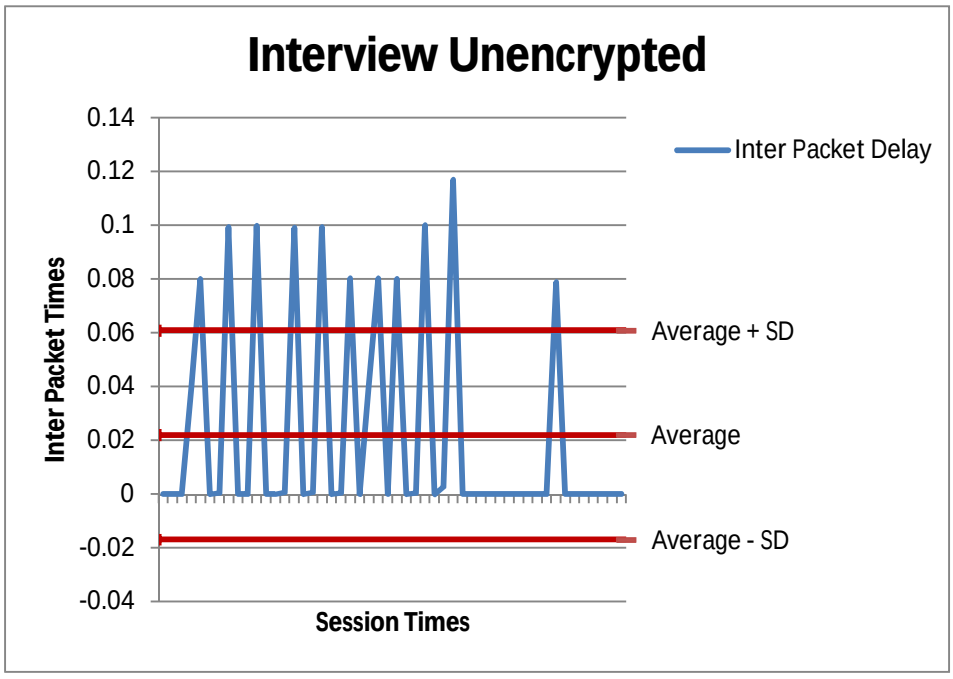

Figure 13: Average and Standard Deviation for interview unencrypted

3.6.3 Movie Video

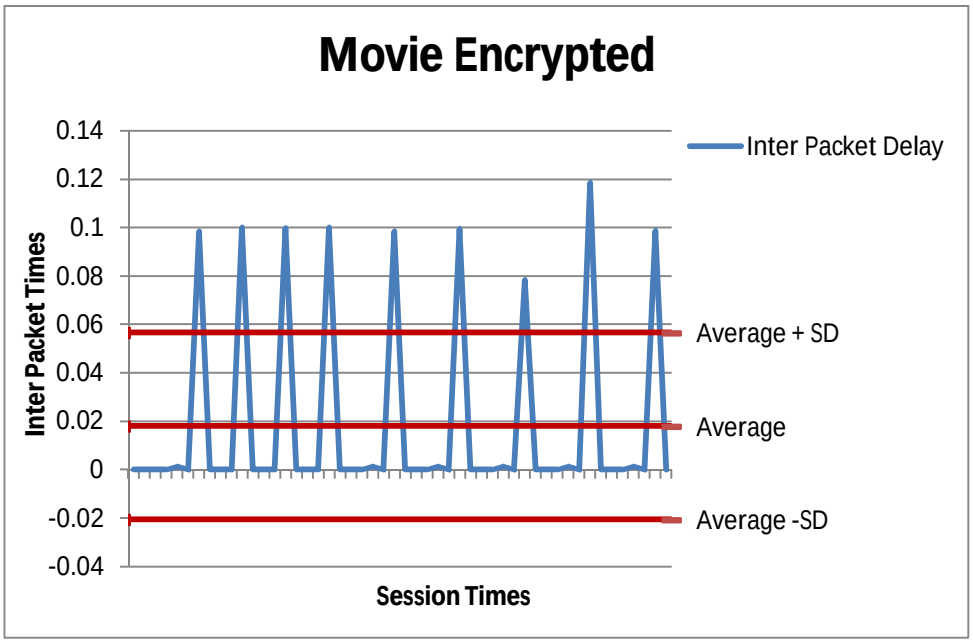

Figure 14: Average and Standard Deviation for movie encrypted

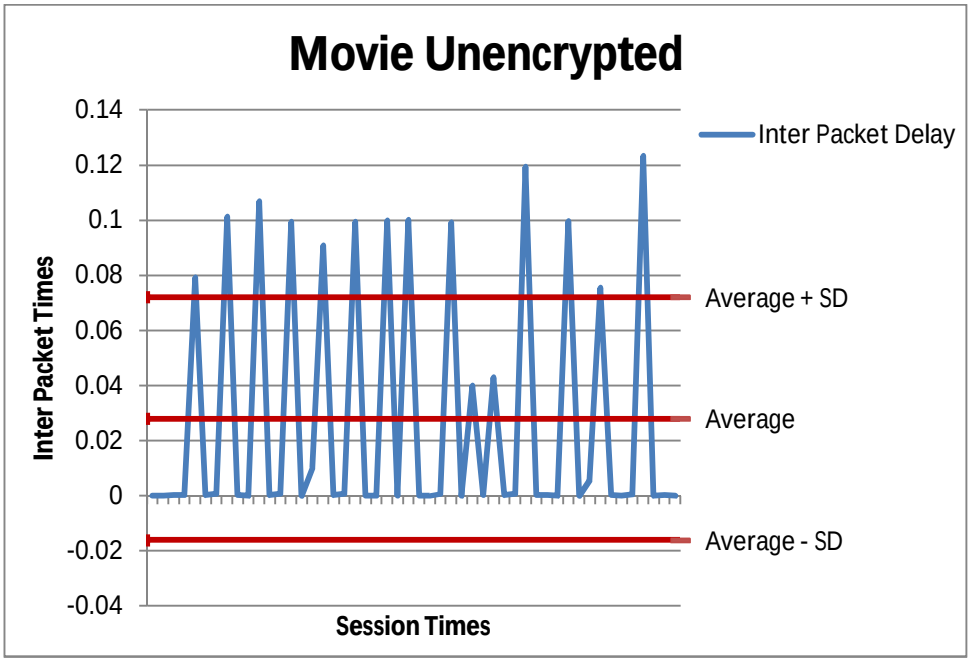

Figure 15: Average and Standard Deviation for movie unencrypted

1.7 Propagation Time for video packets

Propagation time for encrypted video time packets are almost double than unencrypted video. It may be due to the IPSec encryption taking place at VPN concentrator at Vyatta.

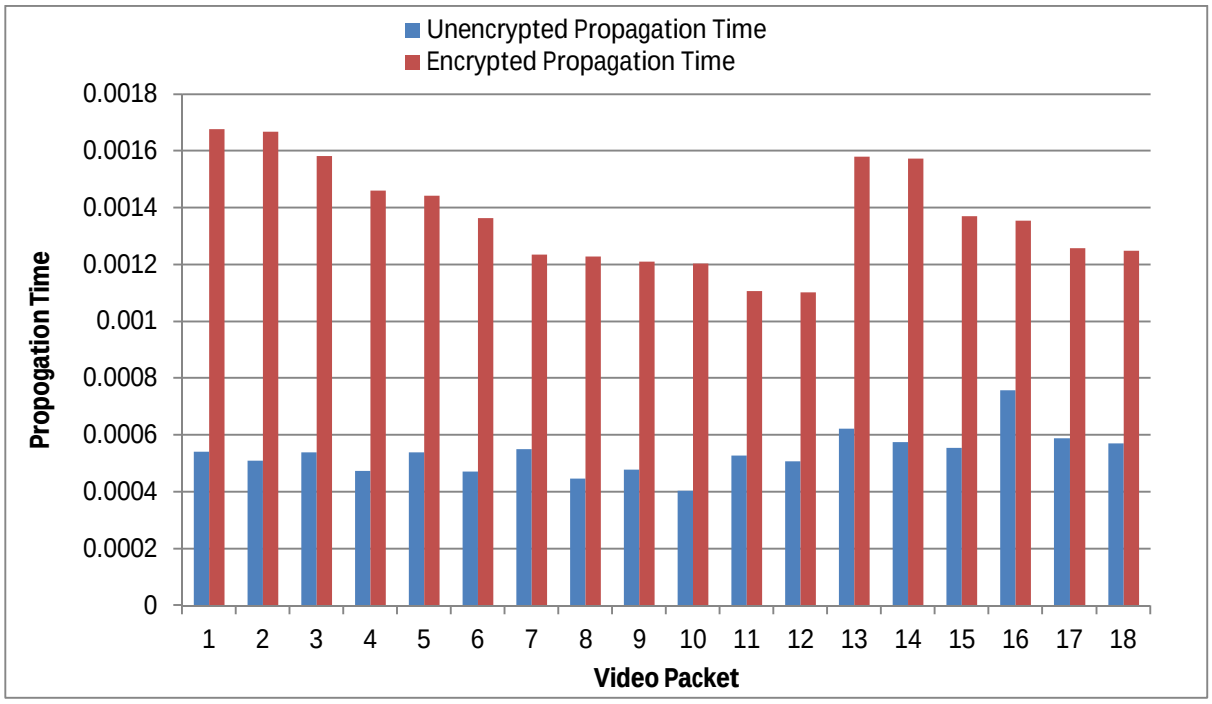

Figure 16: Propagation time of football video

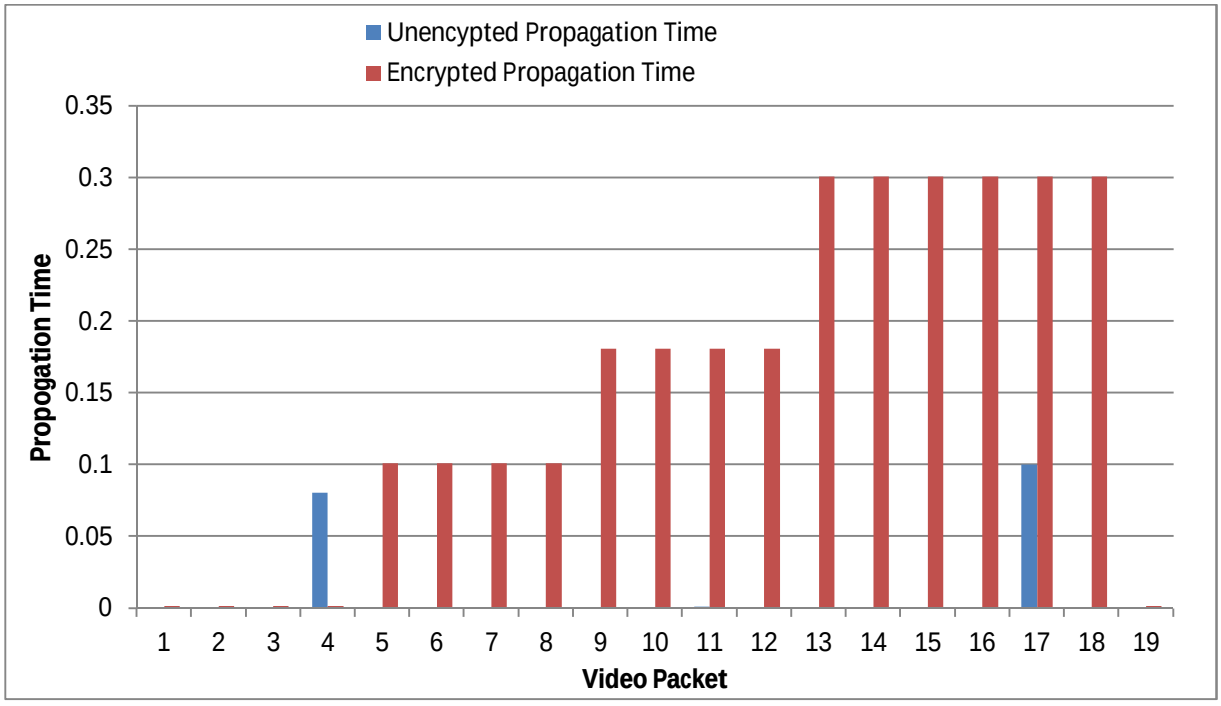

Figure 17: Propagation time of Interview video

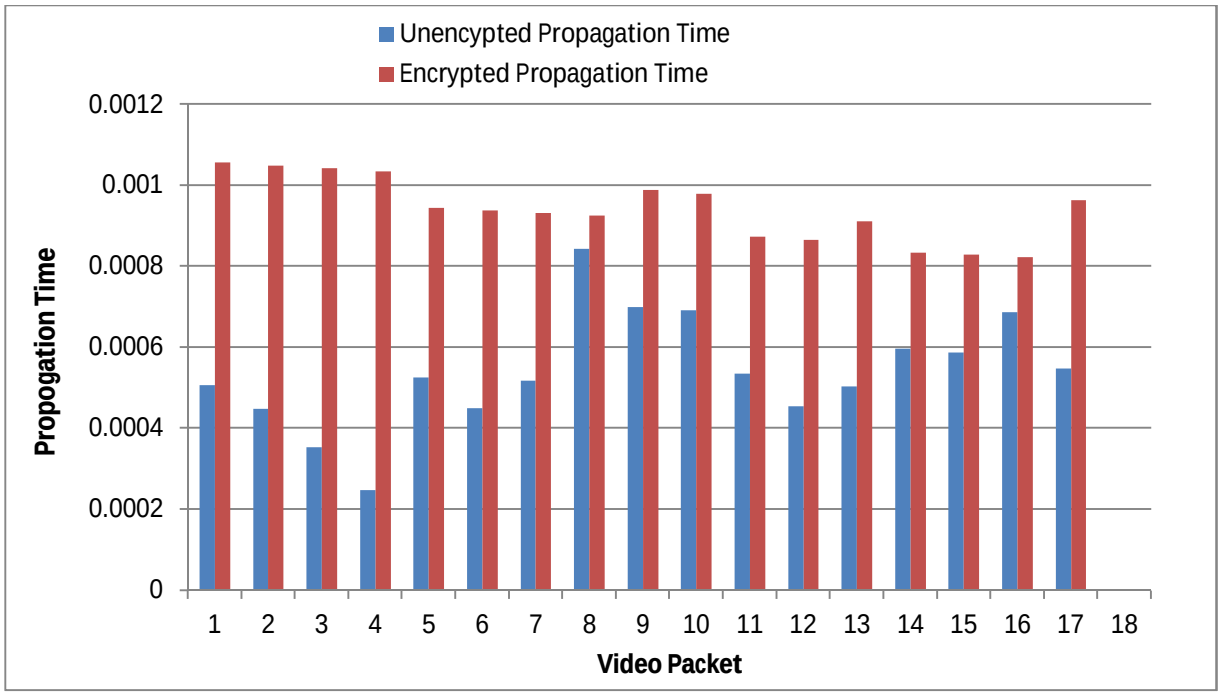

Figure 18: Propagation time of movie video

1.8 Performance Evaluation

From the results obtained from capturing data we come to know interesting things.

- It can be seen that encrypted transmission produces more packets than the unencrypted ones.
- Inter video-packet delay in encrypted video is less than unencrypted ones for all the sample videos as encrypted one has more packets which implies that delta would be less.
- Propagation time for video packets is more in encrypted run than the unencrypted one.
- In simple words encrypted packets take longer to travel through network whereas on other hand unencrypted packets travel faster comparatively.
- In a real scenario encrypted transmission can add real time delays because of more propagation time but these delays can be reduced if better data compression techniques are used while streaming videos.

Chapter 4

Conclusion

Impacts of encryption on streaming video are studied in this project. It was done by inserting encryption at Vyatta VPN concentrator which adds overhead and delay for a video to reach a client sent by server. After capturing the data it was observed that time taken by encrypted data to travel from source to destination is more than unencrypted. The AES-256 encryption algorithm which is expected to be standardized by most of the health care organizations is also used in this project

4.1 Future Work

For future work this schematic can be tested on following scenarios:

1. More complex network can be used by adding more devices in between server and client.

2. A remote Server and client scenario could be used with the help of internet to create real-time environment.

3. Different software could also be used such as real time video chat instead of VLC player which may provide us with different results for delay and quality of user experience.

List of References

[1] Park, Shihyon; Matthews, Bradley; D'Amours, Danny; McIver Jr., William J., " Characterizing the Impacts of VPN Security Models on Streaming Video", Communication Networks and Services Research Conference (CNSR), 2010 Eighth Annual , page(s): 152 – 159, 11-14 May 2010

[2] CCNET/2
Official Exam Certification Guide, Second Edition by Wendell Odom CCIE No. 1624

[3] CCNET/3
Official Exam Certification Guide, Second Edition by Wendell Odom CCIE No. 1624

[4] http://technet.microsoft.com/en-us/library/cc778013(WS.10).aspx

Appendix A

Vyatta Device

Configuration mode:
set interfaces ethernet eth0 address 192.168.1.6/29
set interfaces ethernet eth0 address 10.1.1.1/29
!
set protocols static route 192.168.1.0/30 next-hop 192.168.1.5
set protocols static route 10.1.1.4/30 next-hop 10.1.1.2
set protocols static route 10.1.1.8/30 next-hop 10.1.1.2
set protocols static route 10.1.1.12/30 next-hop 10.1.1.2
!
commit
save
!
set vpn ipsec ipsec-interfaces interface eth1
edit vpn ipsec ike-group IKE1
set lifetime 86400
edit proposal 1
set encryption aes256
set hash sha1
set dh-group 2
top
!
edit vpn ipsec esp-group IKE2
set lifetime 86400
edit proposal 1
set encryption aes256
set hash sha1
top
!
edit vpn ipsec site-to-site peer 10.1.1.10
set authentication pre-shared-secret letmein
set ike-group IKE1
set local-ip 10.1.1.1
!
edit tunnel 1
set local-subnet 192.168.1.0/29
set remote-subnet 10.1.1.12/30
set esp-group IKE2
!
commit
save

Switch (Cisco 3750)

```
Switch#
Switch#sh run
Building configuration...

Current configuration : 2457 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
switch 1 provision ws-c3750g-24ps
system mtu routing 1500
ip subnet-zero
ip routing
!
!
ip vrf LAN
!
ip vrf WAN
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
interface GigabitEthernet1/0/1
 no switchport
 ip vrf forwarding WAN
 ip address 10.1.1.2 255.255.255.252
!
```

```
interface GigabitEthernet1/0/2
 no switchport
 ip vrf forwarding LAN
 ip address 192.168.1.5 255.255.255.252
!
interface GigabitEthernet1/0/3
 no switchport
 ip vrf forwarding LAN
 ip address 10.1.1.5 255.255.255.252
!
interface GigabitEthernet1/0/4
 no switchport
 ip vrf forwarding LAN
 ip address 192.168.1.2 255.255.255.252
!
interface GigabitEthernet1/0/5
 switchport mode access
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
```

```
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface Vlan1
 no ip address
!
ip classless
ip route vrf LAN 10.1.1.0 255.255.255.252 192.168.1.6
ip route vrf LAN 10.1.1.4 255.255.255.252 192.168.1.6
ip route vrf LAN 10.1.1.8 255.255.255.252 192.168.1.6
ip route vrf LAN 10.1.1.12 255.255.255.252 10.1.1.6
ip route vrf WAN 10.1.1.8 255.255.255.252 10.1.1.6
ip route vrf WAN 10.1.1.12 255.255.255.252 10.1.1.6
ip route vrf WAN 192.168.1.0 255.255.255.252 10.1.1.1
ip route vrf WAN 192.168.1.4 255.255.255.252 10.1.1.1
ip http server
!
!
!
!
control-plane
!
!
line con 0
line vty 5 15
!
!
monitor session 2 source interface Gi1/0/1 , Gi1/0/3 rx
monitor session 2 source interface Gi1/0/2 tx
monitor session 2 destination interface Gi1/0/5
end
```

Cisco 2900

```
hostname 2900
!
interface GigabitEthernet0/0
ip address 10.1.1.6 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.1.1.9 255.255.255.252
duplex auto
speed auto
!
ip route 10.1.1.0 255.255.255.252 10.1.1.5
ip route 10.1.1.12 255.255.255.252 10.1.1.10
ip route 192.168.1.0 255.255.255.252 10.1.1.5
ip route 192.168.1.4 255.255.255.252 10.1.1.5
```

Cisco 2800

```
hostname 2800
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
group 2
crypto isakmp key letmein address 10.1.1.1
!
crypto ipsec transform-set NRC esp-aes 256 esp-sha-hmac
!
crypto map S2S-VPN 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set NRC
 match address S2S-VPN-TRAFFIC
!
interface GigabitEthernet0/0
 ip address 10.1.1.10 255.255.255.252
duplex auto
 speed auto
 crypto map S2S-VPN
!

interface GigabitEthernet0/1
 ip address 10.1.1.13 255.255.255.252
 duplex auto
 speed auto
!
```

```
ip route 10.1.1.0 255.255.255.252 10.1.1.9
ip route 10.1.1.4 255.255.255.252 10.1.1.9
ip route 192.168.1.0 255.255.255.252 10.1.1.9
ip route 192.168.1.4 255.255.255.252 10.1.1.9
!
ip access-list extended S2S-VPN-TRAFFIC
permit ip 10.1.1.12 0.0.0.3 192.168.1.0 0.0.0.7
```