INT J COMPUT COMMUN, ISSN 1841-9836
8(1):136-145, February, 2013.

Efficiency Consideration for Data Packets Encryption within Wireless VPN Tunneling for Video Streaming

D. Simion, M.F. Ursuleanu, A. Graur, A.D. Potorac, A. Lavric

Daniel Simion, Mihai Florentin Ursuleanu
Adrian Graur, Alin Dan Potorac, Alexandru Lavric
"Stefan cel Mare" University of Suceava
Universitatii Street, No.13, RO-720229, Suceava, Romania
E-mail: dasimion@eed.usv.ro, mursuleanu@stud.usv.r
adriang@eed.usv.ro, alinp@eed.usv.ro, lavric@eed.usv.ro

Abstract:
With the help of the Internet today we can communicate with anyone from anyplace to access all types of data with a high level of QoS. This mobility is available for legitimate users, as well as for illegitimate ones, for this reason we need extra data security. A solution for QoS and data confidentiality is Virtual Private Network (VPN); ways, in which we can reduce operational costs, grow productivity, simplify network topology and extend the area of connectivity. Video data packets must arrive with a constant and low delay at the same rate in order to have e real time transmission. This paper presents an analysis of different protocols used and the way that video data packets are encapsulated and encrypted for a high level of QoS in a VPN connection.
Keywords: encryption, IPSec, L2TP, VPN, videostreaming, wireless tunneling.

1 Introduction

Sending video streams in IP networks is not a trivial problem even more so if we do it on a wireless network. In the wireless standard 802.11 for each carried data packet, timing intervals and additional overheads are mandatory. Often attacks of this sort compromise the network availability of the application. Data integrity and confidentiality can be compromised by unauthorized external access, for example hackers who can modify data content and data bases.

The following research is a part of a bigger project that aims the optimization of data communication. The main focuses of the research are towards technologies like video streaming, VoD, VoIP, and IPTV.

Virtual Private Network (VPN) is used to avoid DoS (Denial of Service) attacks, eavesdropping, masquerade and traffic analysis; to reduce operational costs and to increase productivity; to simplify network topology and extend the geographical connectivity area without adding other costs.

VPN security solution offers two major advantages: network scalability and a low implementation cost. The client doesn't have to rent other networks to cover all of the company's locations; he can connect them through a local connection to any licensed ISP (Internet Service Provider), at the rate required by that provider.

Also, the client doesn't need remote access servers. In order to connect two locations, a company will use a single dedicated line (see Figure 1), but as the number of work points will multiply so will the connection costs will grow. For example a company which will have 4 work point will need 6 dedicated lines to interconnect them; for 6 work points a company will use 15 dedicated lines for interconnections fact that will influence negatively the QoS of the video stream transmission.

2 Virtual Private Network Tunneling

VPN is a private and secure connection [1] between two or more networks or computers who share protected data, using a single secure channel between the endpoints, over a public data network (for example WAN) or through the Internet. Tunneling represents the ability to make circuit oriented connections in WAN topologies oriented on packets. This process is the main technical concept of VPN.

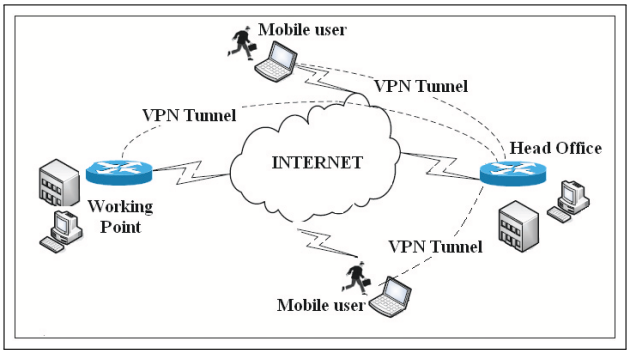


Figure 1: Virtual Private Network Tunneling concept

Unlike packet oriented protocols, like IP, which can send data packets on different routes to a common destination; a tunnel represents a dedicated virtual circuit between two endpoints of a communication network. Since this process takes place over a shared network and tunneling can be implemented on a medium technological level, VPN is economically efficient; with implementation costs between packets based communications and leased line communications.

VPN was created not to replace the other security mechanisms of the IEEE 802.11 standard, but to complete them.

The main modes of use supported by VPN are:

- LAN-to-LAN internetworking;
- Controlled access within an intranet;
- Internet remote access client connections.

Protocols based on the OSI model (for data link layer and network layer) have been implemented in VPN tunneling. In order to send data on layer 2 VPN uses frames and on layer 3 VPN uses packets for data sending.

In Figure 2 can be seen a representation of VPN protocols on OSI Model.

Point-to-Point Tunneling Protocol (PPTP) encapsulates PPP frames for transmission over IP internet works in IP datagrams. For tunnel maintenance a TCP connection is used in PPTP, in order to encapsulate PPP frames in tunnelled data is used a modified version of GRE (Generic Routing Encapsulation). The content encapsulated with PPP frames can be compressed or encrypted (view Figure 3).

$$H = H_{GRE} + H_{PPP} + H_{IP} \tag{1}$$

Layer Two Tunneling Protocol (L2TP) encapsulates PPP frames, encrypted and/or compressed, which can be sent over X.25, ATM, Frame Relay or IP networks [2]. For a secure enabled tunnel L2TP protocol can be combined with IPSec. L2TP tunneled data uses UDP to send L2TP encapsulated PPP frames (view Figure 4).

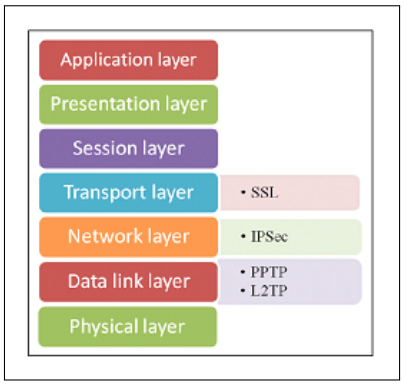


Figure 2: VPN protocols on OSI Model

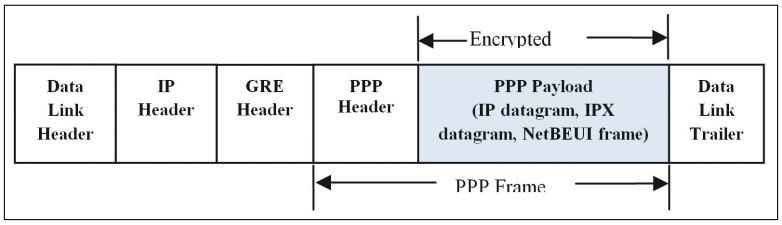


Figure 3: PPTP Tunnel Data Frame Format

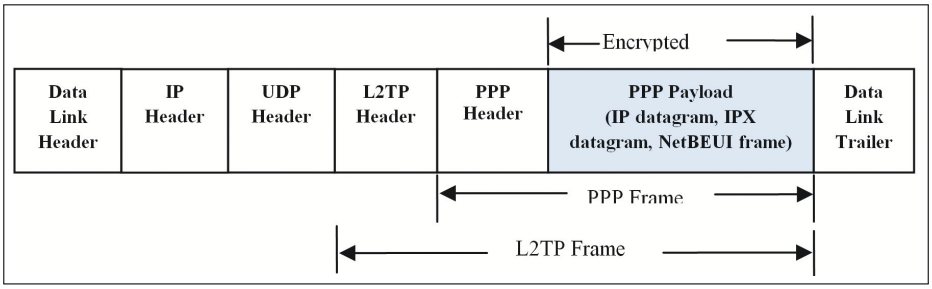


Figure 4: L2TP Tunnel Data Frame Format

$$H = H_{IP} + H_{UDP} + H_{L2TP} + H_{PPP} \tag{2}$$

Internet Protocol Security (IPSec) is a collection of multiple related protocols. It can be used as a complete VPN protocol solution or simply as the encryption scheme within L2TP or PPTP. IPSec ESP (Encapsulating Security Payload) encrypts the L2TP packet. Known to be the strongest authentication and encryption method IPSec works at layer 3 of the OSI network model.

An alternative to IPSec are SSL VPN's, they operate at a higher layer level than IPSec and it offers network administrators a greater control access to different network resources. SSL (Secure Socket Layer) enables secure transactions of data and relies on several security measures like private or public key and digital certificates [3]. Using SSL security encryption in a WLAN environment forces a mobile wireless equipment to authenticate itself before any data transactions.

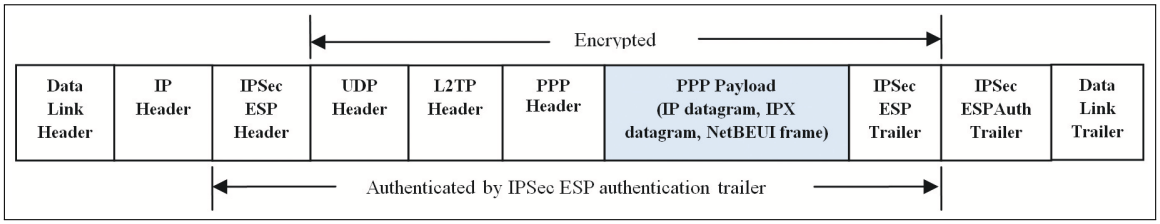


Figure 5: L2TP/IPSec Tunnel Data Frame Format

$$H = H_{IP} + H_{ESP} + H_{UDP} + H_{L2TP} + H_{PPP} \tag{3}$$

Due to the standardization of tunneling protocols they become vulnerable to any firewall stopping and blocking at any level. VPN uses encrypting routers to ensure unauthorized access to the data that is being sent in a communication transmission; also limiting third parties data access to the network connection.

There are lots of encryptions type's algorithms. In most algorithms, the original data is encrypted using a certain encryption key. Only the receiver computer or the recipient user can decrypt the message using a specific decryption key. SSL, DES and PGP are some encryption algorithms that create or change these keys. Authentication and encryption used in VPN depend on implementation. Implementations like PPTP use the RC4 algorithm on 40/56/128 bits, while L2TP and IPSec can use a wide range on encryption algorithms, like AES on 128/192/256 bits, DES on 56 bits and 3DES on 168 bits.

In VPN PPTP encryption is weak, sending distributed passwords in clear. Unlike PPTP, L2TP utilizes server-client digital certificates based ok PKI (Public Key Infrastructure). Some solutions of IPSec have the option of using pre-shared keys or PKI digital certificates [4].

When considering a secure wireless VPN connection:

$$H_{SEC} = H + H_{SOH} \tag{4}$$

where, H_{SOH} are security overheads; we have to take in account supplementary overheads (20 Bytes for WPA TKIP, 8 Bytes for WEP, 16 Bytes for WPA CCMP) [5, 6].

3 Practical Approach

This practical approach has tried to evaluate the theoretical approach presented before, in a stable environment (without electromagnetic pollution). Certain measurements were made using

different communication scenarios.

In the first scenario, we have sent a video stream with 1.164 GB of data through our private VPN, which uses PPTP encryption protocol, between two clients (n=*1*, where n is the number of clients); one has an Ethernet connection to the VPN server and the other has a wireless connection.

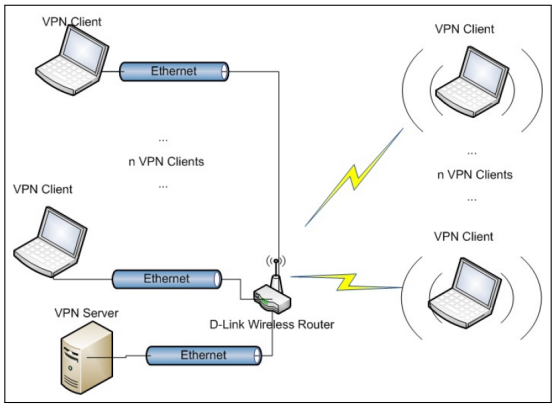


Figure 6: LAN-WLAN VPN Connections

For the first scenario the results have been achieved in interval 2.008 Mbps - 10.036 Mbps (see Figure 7).

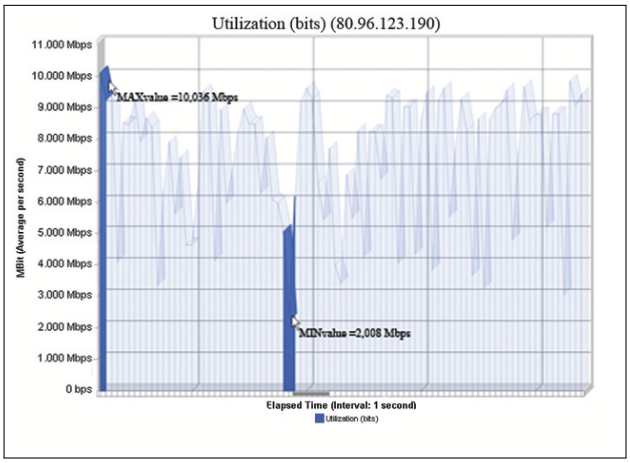


Figure 7: Minimum and Maximum values for LAN-WLAN VPN connection

In Figure 8 can be seen a network report for the first scenario, LAN-WLAN VPN connection.

Excluding IP overheads for PPTP, we have achieved an overhead length between 26 and 32 Bytes [7].

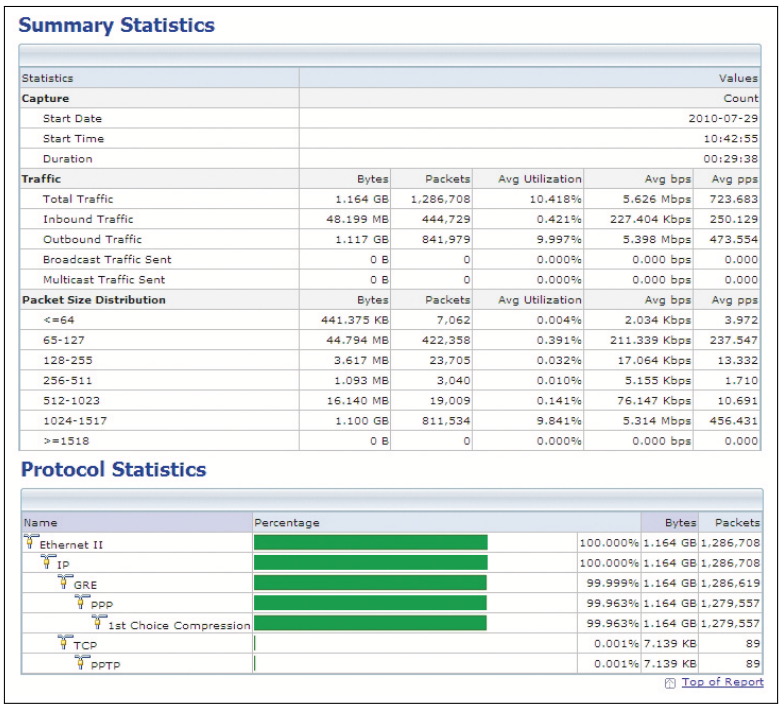
For an average upload speed of 5,398 Mbps we have 674,75 KB/s (Up_s = *674.75KB/s*).

We have an upload rate (Up_r) of:

$$Up_r = \frac{Up_s}{MTU} \tag{5}$$

where, MTU is Maximum Transmission Unit or maximum efficiency for the IP packet.

Normally, without PPTP VPN tunneling protocol, according to equation (5), we have an upload rate of 449.83 packets/s:



Summary Statistics

Statistics					Values
Capture					Count
Start Date					2010-07-29
Start Time					10:42:55
Duration					00:29:38
Traffic	Bytes	Packets	Avg Utilization	Avg bps	Avg pps
Total Traffic	1.164 GB	1,286,708	10.418%	5.626 Mbps	723.683
Inbound Traffic	48.199 MB	444,729	0.421%	227.404 Kbps	250.129
Outbound Traffic	1.117 GB	841,979	9.997%	5.398 Mbps	473.554
Broadcast Traffic Sent	0 B	0	0.000%	0.000 bps	0.000
Multicast Traffic Sent	0 B	0	0.000%	0.000 bps	0.000
Packet Size Distribution	Bytes	Packets	Avg Utilization	Avg bps	Avg pps
<=64	441.375 KB	7,062	0.004%	2.034 Kbps	3.972
65-127	44.794 MB	422,358	0.391%	211.339 Kbps	237.547
128-255	3.617 MB	23,705	0.032%	17.064 Kbps	13.332
256-511	1.093 MB	3,040	0.010%	5.155 Kbps	1.710
512-1023	16.140 MB	19,009	0.141%	76.147 Kbps	10.691
1024-1517	1.100 GB	811,534	9.841%	5.314 Mbps	456.431
>=1518	0 B	0	0.000%	0.000 bps	0.000

Protocol Statistics

Name	Percentage		Bytes	Packets
Ethernet II		100.000%	1.164 GB	1,286,708
IP		100.000%	1.164 GB	1,286,708
GRE		99.999%	1.164 GB	1,286,619
PPP		99.963%	1.164 GB	1,279,557
1st Choice Compression		99.963%	1.164 GB	1,279,557
TCP		0.001%	7.139 KB	89
PPTP		0.001%	7.139 KB	89

Top of Report

Figure 8: Network report for LAN-WLAN VPN connection

$$Up_r = \frac{Up_s}{MTU + PPTP_{overheads}} \tag{6}$$

Using equation (6), for a maximum PPTP overheads length (32Bytes) used for VPN tunneling, the packet rate will decrease at 440.43 packets/s.

At a maximum IP packet size (1.5KB) we have a loss of 32 bytes equaling 2.09% of bandwidth lost.

For encapsulating 1.5KB IP packet into L2TP, the packet becomes 1.54KB (1.5KB +0.04KB of UDP, IP and L2TP headers). Sending packets of data over Ethernet is a job that's requires fragmentation of the initial data into 1.5KB of data. So, the packet will be fragmented.

The first fragment has 1.5KB of data (1.46KB from the original IP packet and 0.04KB from L2TP encapsulation).

The second will have 0.06KB (0.02KB from IP overhead and last 0.04KB from the original IP packet). From the whole packet, only the first fragment of the packet will contains the L2TP header. The second fragment of the data packet has only IP header. Careless of the L2TP client type (LNS or LAC), the peer will assemble the two packet fragments back into original 1.54KB size.

$$Up_r = \frac{Up_s}{MTU + L2TP_{overheads}} \tag{7}$$

When we used L2TP VPN protocol the packet rate has decreased at 438.15 packets/s, in comparison with the case when we used PPTP VPN protocol, as concluded from (7).

At a maximum IP packet size (1,5KB) we have a loss of 60Bytes equalling 3.89% of bandwidth lost. When we used IPSec VPN protocol encapsulation the packet rate has decreased at 433.64 packet/s.

$$Up_r = \frac{Up_s}{MTU + IPSec_{overheads}} \tag{8}$$

In this case we have a 76Bytes loss (about 4.88% of all bandwidth), at a maximum IP packet size (1.5KB) (see Figure 9).

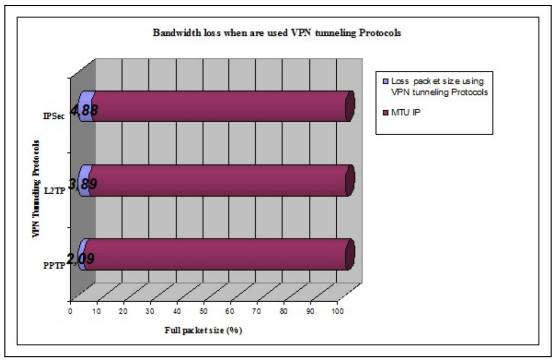


Figure 9: Bandwidth loss when using VPN Tunneling Protocols

In infrastructure wireless LANs with one access point (AP), the data frames do not travel directly among clients. Wireless clients send the data frame to the AP and then the AP resend the payload content of the original data frame, packed in a new data frame, to the receiving client. The AP bandwidth, and the radio space, is shared between the AP radio clients and the user available bandwidth is thus split among those clients [8].

In the second scenario, we have sent a video stream through our private VPN, which uses PPTP encryption protocol, between two wireless clients (n=*2*, where n is the number of wireless clients) (see Figure 10).

The link utilization factor is reflected in the efficiency of the communication channel. This can be viewed as the ratio between the total times that the channel is busy and the time for sending the data payload. The channel efficiency is the rapport between payloads (the useful bits of information) and the all the bits sent. For the ideal channel, the efficiency is:

$$E_f = \frac{L}{(L+H)} \tag{9}$$

where, E_f is channel efficiency, L is the number of useful data bits and H is the overheads bits.

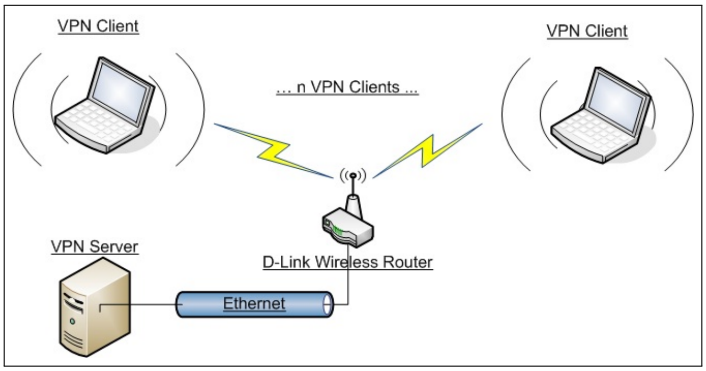


Figure 10: WLAN-WLAN VPN Connections

For the second scenario the results have been achieved in interval 1.857 Mbps - 14.326 Mbps (see Figure 11).

Each packet has *8L* useful bits. The determination of the total number of successful sent payload bits is made using the formula *S * N * 8L*, and the number of total transmitted bits can be calculated using the relation *N * 8 * (L + H)*.

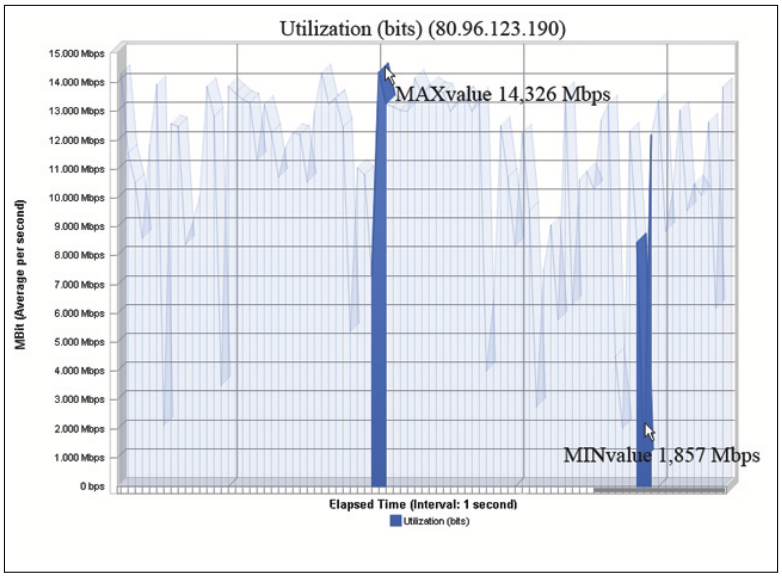


Figure 11: Min and Max values for WLAN-WLAN VPN connection

Supposing that in a unit of time are passed though the VPN channel N packets of data, and a part of them are successfully received by the another VPN client, the channel efficiency (E_{f0}), is (10):

$$E_{f0} = \frac{N * 8L * (1-p)^{8*(L-H)}}{N * 8 * (L+H)} = \frac{L}{L+H} * (1-p)^{8*(L+H)} \tag{10}$$

where, p is bit error probability.

The maximum size of one data packet sent on wireless environment is over 50% larger than the maximum packet size sent on the Ethernet networks. The maximum size of one data packet, in ideal condition, sent unencrypted on wireless environment is 2.304KB.

For the ideal VPN wireless channel, with one wireless VPN client, the efficiency is (11):

$$E_f = \frac{N_w}{L_w + H_{VPN}} \tag{11}$$

where, N_w is the number of frames in a unit of time, L_w is the number of useful data bits in wireless medium and H_{VPN} is the VPN overheads.

In a simple wireless video streaming, if no error occurs, the efficiency is (12):

$$E_f = \frac{N_w}{L_w} \tag{12}$$

From our scenarios we have found that the 7.54% from the maximum data packet unit is responsible for wireless VPN data packaging and 4.64% from the maximum data packet unit is responsible for wireless data packaging (see Figure 12).

In VPN the bandwidth reservation can be a challenge because of the unknown load distribution in a point-to-point connection [9].

As argued in [10], IPSec security encapsulation in VPN shows the performance in terms of average added overhead.

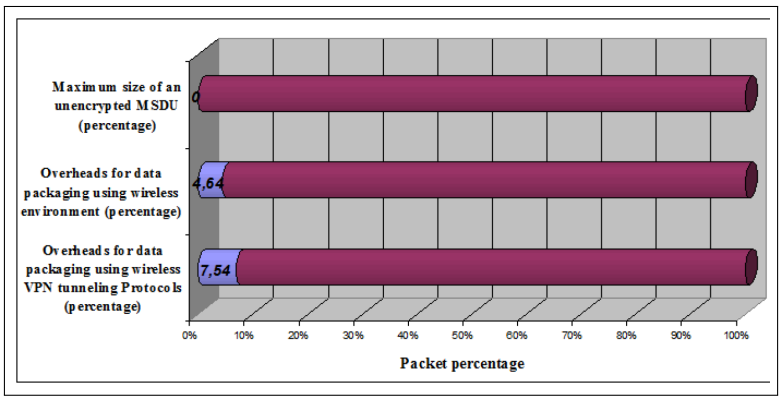


Figure 12: Overheads contribution in Wireless and Wireless VPN environment

4 Conclusions and Future Works

This paper evaluates the data communication efficiency for continuous data streaming and different scenarios in a wireless environment using a VPN solution. The results of the research would be considered as a base for the implementation of new solutions in the field of data streaming using heterogeneous communications medium and technologies.

Using wireless environment instead of Ethernet solution for sending video streaming data packets we lose approximately 34.89% from whole packet sent. When we used VPN for video streaming we also lose 2.9% from the packet sent. The biggest WLANs have about 100 nodes. A way in which we can extend them is by using VPN Tunneling.

With WiMAX and LTE technologies VPN video data transmission speeds will increase, both including "best-effort" and priority based QoS scalable solutions. Considering that only 2.09 % of the packet size is lost through VPN encapsulation is a price worth paying for a secure connection between two work points.

We conclude that we have achieved better speeds in a WLAN-WLAN video streaming scenario when we used PPTP tunneling protocol in given conditions compared to L2TP and IPSec VPN tunneling protocols.

In our next papers we will present a study on WiMax and LTE on video packet frames structure for downlink and uplink with a specific simulating software. We will simulate wireless VPN communication network with the two technologies, WiMax and LTE, on high performance hardware to obtain maximum speeds for data transfer. Future papers will analyze the effects of WiMax and/or LTE on live video streams, IPTV streams and multimedia.

Acknowledgements

This paper was supported by the project "Knowledge provocation and development through doctoral research PRO-DOCT - Contract no. POSDRU/88/1.5/S/52946", project co-funded from European Social Fund through Sectoral Operational Program Human Resources 2007-2013 and by the project "Improvement of the doctoral studies quality in engineering science for development of the knowledge based society - QDOC" contract no. POSDRU/107/1.5/S/78534, project co-funded by the European Social Fund through the Sectorial Operational Program Human Resources 2007-2013.

Bibliography

[1] Shihyon P., Bradley M., D'Amours D., William J. McIver Jr., *Characterizing the Impacts of VPN Security Models on Streaming Video*, Communication Networks and Services Research Conference (CNSR), Montreal, QC, Canada, ISBN:978-1-4244-6248-3, pp. 152 - 159, 2010.

[2] Townsley W., Valencia A., Rubens A., Pall G., Zom G., Palter B., *Layer two tunneling protocol (L2TP)*, RFC 2661, 1999.

[3] Hamzel K., Pall G., Verthein W., Taarud J., Little W, Zom G., *Point-to-point tunneling protocol (PPTP)*, RFC 2637, 1999.

[4] Prasad A.R., Prasad N.R., *802.11 WLANs and IP networking: Security, QoS and mobility*, Boston: Artech House, ISBN 1-58053-789-8, 2005.

[5] Potorac A.D., *Considerations on VoIP Throughput in 802.11 Networks*, Advances in Electrical and Computer Engineering - AECE, ISSN: 1582-7445 e-ISSN: 1844-7600, 9(3):45-50, 2009.

[6] Khan M.A.U., Khan T.M., Khan R.B., Kiyani A., Khan M.A. *Noise Characterization in Web Cameras using Independent Component Analysis*, INT J COMPUT COMMUN, ISSN 1841-9836, 7(2):302-311, 2012.

[7] Hossein B., *The Internet encyclopedia*, ISBN 0-417-22201-1, vol.3:425-428, 2004.

[8] Potorac A.D., Coca E. *QoS Consideration for 802.11 Networks*, European Conference on the Use of Modern Information and Communication Technologies - ECUMICT 2006, Ghent, Belgium, 30-31 March 2006, ISBN 9-08082-552-2, pp. 45-50, 2006.

[9] Volner R., Smrz V., *Virtual Private Networks - Based Home System*, Electronics and Electrical Engineering - Kaunas: Technologija, ISSN 1392-1215, 8(96):62-64, 2009.

[10] Berioli M., Trtta F. *IP mobility support for IPsec-based virtual private networks: An architectural solution*, 3rd IEEEGlobal Telecommunications Conference - GLOBECOM '03, Conference Publications, ISBN: 0-7803-7974-8, 3:1532 - 1536, 2003.