GATELINK PERFORMANCE EVALUATION WITH WPA-2 AND IPSEC SECURITY METHODS

Natalia Ezagui Garcia Rocha, nataliaerocha@gmail.com
EMBRAER – Empresa Brasileira de Aeronáutica – Av. Brigadeiro Faria Lima, 2170, Putim, São José dos Campos, Brasil.

Alessandro Anzaloni, anzaloni@ita.br
ITA – Instituto Tecnológico de Aeronáutica - Praça Marechal Eduardo Gomes, 50, São José dos Campos, Brasil.

Abstract. *This paper will analyze the impact of WPA-2 and IPsec security mechanisms for different values of MTU (Maximum Transfer Unit) on the time necessary to transmit a PHM (Prognostics and Health Monitoring) file from an aircraft to its airline maintenance center. The considered scenario is composed by an 802.11 wireless link and a wired link using Frame Relay.*

Keywords: *Gatelink, PHM, Ipsec, WPA-2*

1. INTRODUCTION

The PHM (Prognostic and Health Monitoring) concept states that raw data related to the health of the components of the aircraft may be sent to the maintenance and control position of an airline for analysis and investigation. This should be done either every flight or after a certain number of flights, in this way preventing components faults and systems failures.

The transmission of this raw data can be done by many ways. This paper considers a wireless technology for data transmission at airports, called Gatelink, which is based on the 802.11 protocol and WPA-2 for security. This study will analyze the impact of this security method on the final throughput of data transmitted. In addition, the airport must have an infrastructure of a wired network to support data transmission to the airline VPN (Virtual Private Network) and IPsec is the method adopted in this study to protect this part of the link. An investigation of the space overhead, which is the overhead associated to IPsec packet frames, will give an estimation of the time necessary to transmit the PHM file. This study will also analyze how the MTU (Maximum Transfer Unit) variation impacts on the time to transmit each data packet. This parameter is important to meet the requirements of maximum time and file size.

Considering that on the wireless link there is probability of frames retransmission due to factors such as SNR (Signal-Noise Ratio) and MTU size, the final throughput can be reduced. This paper presents a study of the time necessary to transmit a frame on Wi-fi format with WPA-2 security according to the MTU available on the data field. Similarly, an evaluation of the time required to transmit a frame on the wired link on Frame Relay format with IPsec security method according to the encapsulated MTU is performed. The time necessary to transmit a MTU of a certain size is defined as the sum of the two delays previously defined – the time on the wireless link and the time on the wired link.

In order to achieve the proposed objective it will be presented on Section 2 the importance of PHM, on Section 3 the considered scenario to develop this study and also the requirements which the communication system shall meet. Section 4 presents the delays to transmit a MTU of a certain size and the time required to transmit the entire PHM file from the aircraft (source) to the maintenance center (receiver) for a given MTU. Finally, on Section 5 are presented the conclusions related to the final results and future works are proposed.

2. PHM

In a further effort to improve aircraft safety rather than to wait for an accident to happen, the FAA (Federal Aviation Administration) has issued in September 20 of 1995 the FOQA (Flight Operational Quality Assurance Program) which recommends that the airlines look at the information provided by the digital flight data acquisition units at regular intervals (Wright and Ziarno, 2008).

The PHM (Prognostics and Health Monitoring) concept combines data acquisition, monitoring and aircraft analysis in order to determine the actual status of the systems and components optimizing maintenance processes. By monitoring data in regular and defined intervals of time, the PHM platform can bring economic benefits to the airline and also to the supplier of the systems and components. As a result of a systematic process, airlines can better respond to faults and failures in the monitored components, which mean less interruptions, delays and cancellations during regular operation. In addition, predictive maintenance tasks can be better scheduled according to the health of a specific component, reducing the risks of incidents and accidents and optimizing maintenance costs.

3. SCENARIO AND REQUIREMENTS

This paper will consider a wireless data transmission system called Gatelink, which has been specified by the aeronautical industry (AEEC 763) to provide high-speed wireless communications between an aircraft and a network on the ground at an airport terminal or at a maintenance position.

This system is composed by an on-board architecture and an 802.11 WLAN infrastructure installed at the airports, which include Access Points and routing equipments. The Access Points are connected through a wired network to the airline Server. The wired part of the system utilizes Frame Relay for being a technology commonly used by Internet Service Providers.

Figure (1) shows the scenario, where an aircraft parked at the gate transmits the PHM information via an 802.11 link to the Access Point. Before that, the aircraft is authenticated in a RADIUS server. The Access Point routs the data through the airport LAN through a Frame Relay wired link. After going through the Internet, it is possible to access the VPN of each airline.

The communication system shall meet a requirement of a minimum throughput enough to send a file of 10Mbytes, which corresponds to a usual PHM file size, in 5 minutes. The value of 10Mbytes was defined from the quantity of parameters that are collected at specific sampling rates during a typical regional flight of 90 minutes. The parameters were defined according to the systems that are being monitored for a certain aircraft. The time of 5 minutes is based on the idea the maintenance center may have enough time to analyze and make decisions before the aircraft leaves the gate for a new flight, therefore data should be transmitted as soon as the aircraft parks at the gate.

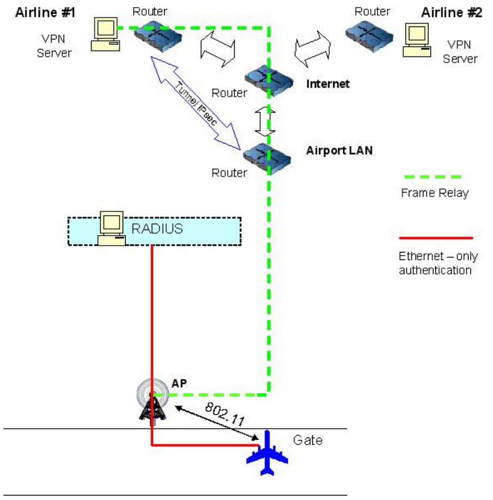

Figure 1– Scenario of data transmission at the airport

4. SECURITY

The wireless and wired link may be secure to guarantee the integrity and privacy of the data transmitted. The information belongs to a private company and is confidential as the data regarding the health of systems and components may be reliable, because based on them the maintenance team diagnoses and make decisions.

Therefore, security mechanisms are being adopted in this study to protect the transmission of the PHM file from the source to the airline server. In this way, it is being considered the last version of AEEC specification for Gatelink, the GATELINK822 based on WPA-2 for the wireless link and IPsec for the wired link.

All these security mechanisms implemented degrade the final throughput of the aircraft (source) and increases the time necessary to transmit all the data packets.

In this section, it will be defined the time necessary to transmit a packet in the wireless link according to the transported MTU. After that, the same is defined for the wired link. The section ends with the calculation of the time to transmit all the PHM file of 10Mbytes from the aircraft to the maintenance center, verifying in which conditions the requirement specified on section 3 is met.

4.1. 802.11 / WPA-2

The 802.11g standard utilizes the 2,4Ghz frequency band with OFDM modulation technique, with a data rate up to 54Mbps.

The IEEE 802.11 specification protects the data on data link layer during wireless transmission between clients and Access Points with a security protocol called Wi-fi Protected Access (WPA), which has the WPA-2 as its advanced version. The WPA-2 provides protection by securing that only authenticated users can have access to the WLAN. In addition, it utilizes the AES (Advanced Encryption Standard) for encryption. With AES, bits are encrypted in text blocks that are calculated independently, instead of one encryption key that encrypts all the data flow, as in TKIP (Temporal Key Integrity Protocol) used in the previous version of WPA. The AES utilizes the Counter Mode/CBC Mac Protocol, known as CCMP, which algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame.

The WPA-2 authentication occurs over the protocol 802.1x and the Extensible Authentication Protocol (EAP) is used as an authentication method. The IEEE 802.1x is a protocol based on port authentication, based on the concept of the uncontrolled and controlled data paths. The uncontrolled data path allows all 802.1X authentication traffic through to the network while the controlled data path blocks normal network traffic until successful client authentication occurs (Tanenbaum, 2003).

4.1.1. Wireless Link – Theoretical Analysis

802.11 WLANs use a mechanism known as carrier sense multiple access with collision avoidance (CSMA/CA). CSMA/CA is a listen before talk (LBT) mechanism. The transmitting station senses the medium for a carrier signal and waits until the carrier channel is available before transmitting.

The DCF is the basis of the standard CSMA/CA access mechanism. Like Ethernet, it first checks to see that the radio link is clear before transmitting. In DCF operation, a station that wants to transmit a frame must wait a specific amount of time after the medium becomes available. This time value is known as the DCF interframe space (DIFS). To avoid collisions, stations use a random backoff time after each frame, with the first transmitter seizing the channel (Roshan and Leary, 2003).

A station receiving a frame acknowledges error-free receipt of the frame by sending an acknowledgment frame back to the sending station. Before sending this frame, the receiving station waits for a short period of time known as SIFS (Short Interval Frame Space).

Figure (2) shows the transmission of the 802.11g packet with the time intervals mentioned above (Pellejero, 2005).

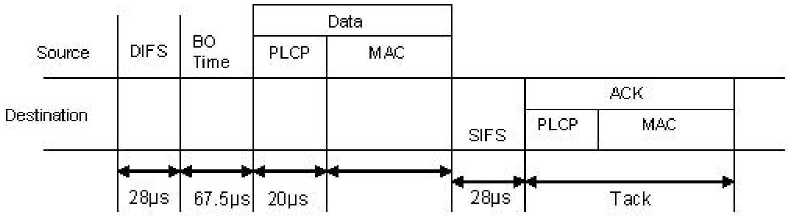

Figure 2– Time intervals for an 802.11g packet

The time required to send a packet depending on the MTU and without retransmissions can be written as:

$$Ttotal_{MTU(w/o\_retransmission)} = Tdifs + Tbo + Tsifs + Tack + Tdata_{MTU} \quad (1)$$

Where $Tdata_{MTU}$ is the time necessary to send the MTU. The 802.11g packet format gives the delay related to the PLCD overhead, according to Fig. (3):

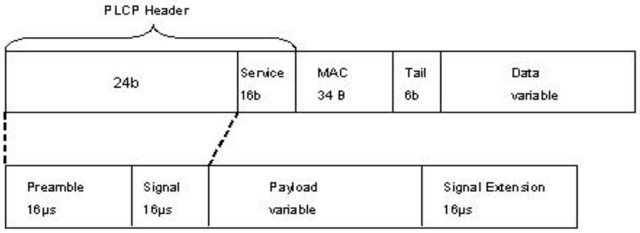

Figure 3 – 802.11g Frame format

PLCD header contains a preamble and a signal frame, which are defined as Tpreamble and Tsignal. Transmission time for a symbol is defined as Tsym. Delay values related to 802.11g standard are according Tab. (1) and defined in IEEE 802.11 Specification (Akhavan, 2006).

Table 1 – 802.11g Packet parameters

Parameters	**Time / Size**
Tslot	9 μs
Tsifs	10 μs
CW	15 ~ 1023
Tpreamble	16 μs
Tsym	4 μs
Tsignal	4 μs
Text	6 μs
Lservice	16 bits
Ltail	6 bits
Lack	14 bytes
Lmac	34 bytes
Lccmp	16 bytes

Some clarifications regarding the values of Tab. (1):

- For encryption and data transmission, 128 bits were added due to CCMP overhead.
- MAC header is 30 bytes, plus 4 bytes of Frame Check Sequency (FCS).
- Considering data rate of 54*Mbps*, the number of bits per symbol is 216 (Akhavan, 2006).

From the values of Tab. (1), time intervals for solving Eq. (1) can be determined according to previous work (Akhavan, 2006) and (Gast, 2003):

Table 2 – Delays for 802.11g

Parameter	**802.11g OFDM 54Mbps**
Tbo	(CWmin * Tslot)/2 = 67.5 μs
Tack	Tpreamble + Tsignal +Tsym * [(Lservice + Ltail + 8 * Lack) / 216] + Tex = 28.5 μs
Tdifs	2 * Tslot + Tsifs = 28 μs

$Tdata_{MTU}$ for 802.11g (considering OFDM and 54*Mbps* data rate) can be determined as the time of protocol overhead (including CCMP) and the time to transmit a given MTU:

$$Tdata_{MTU} = Tpreamble + Tsignal + Tsym \cdot \frac{(Lservice + Ltail + 8 \cdot (Lmac + Lmtu + Lccmp)}{216} + Tex \qquad (2)$$

Equation (2) shows that the time to transmit a packet is based on the 802.11g packet size as well as the MTU size, defined in the Eq. (2) as *Lmtu*. The MTU is a data field that in most cases is defined with 1500 bytes (including TCP and IP headers) for being the value used in Ethernet.

However, as the size of the data field increases, the probability of error during the packet transmission also increases. This characteristic is defined in (Shuwartz, 1987), and can be written as:

$$p = (l + l') * pb \qquad (3)$$

p = packet error probability
l = MTU size
l'= overhead related to 802.11/WPA-2

pb = bit error probability

Figure (4) shows the Packet Error probability for different values of MTU. The bit error probability is fixed in 10^{-5}.

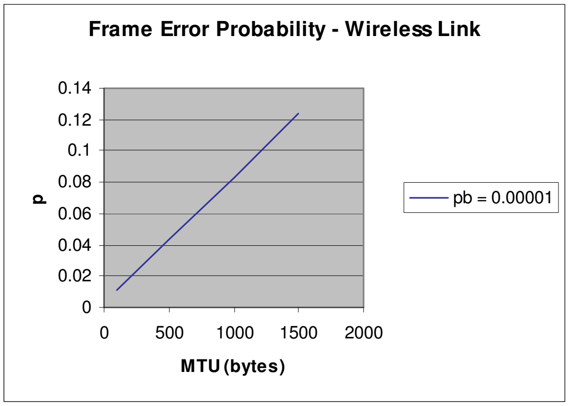

Figure 4 – Frame error probability for different values of MTU

Table (3) shows the values obtained from Eq. (2) for the total time to transmit a packet ($Tdata_{MTU}$) for different values of MTU:

Table 3 – 802.11g OFDM 54Mbps

MTU (bytes)	**100**	**500**	**1000**	**1500**
$Tdata_{MTU}$ (μs)	48.63	107.88	181.96	256.04
$Ttotal_{MTU(w/o\_retransmission)}$ (μs)	182.61	241.87	315.94	390.02

Considering that there is error in the transmission of a packet, it is possible to estimate the mean number of retransmissions E[n] as (Shuwartz, 1987):

$$E[n] = \frac{1}{(1-p)} \tag{4}$$

E[n] values are shown in Tab. (4):

Table 4 – E[n] per MTU

MTU (bytes)	**100**	**500**	**1000**	**1500**
E[n]	1.01	1.04	1.09	1.14

Thus, for a MTU packet of 1500 bytes to be transmitted with success, it has to be transmitted 1.14 times. In this way, it is possible to calculate the total time to transmit a given MTU considering retransmission:

$$Ttotal_{MTU(with\_retransmission)} = E[n] \cdot Ttotal_{MTU(w/o\_retransmission)} \tag{5}$$

Table 5 - Total time for each MTU considering retransmissions

MTU (bytes)	**100**	**500**	**1000**	**1500**
$Ttotal_{MTU(with\_retransmission)}$ (μs)	184.72	252.85	344.70	444.93

4.2 Wired Link - VPN / IPSEC

This study analyzes the use of a VPN to secure the wired link that starts on the Access Points (which can work as routing equipments) installed at the airport until the airline server. The study also considers the IPsec as security protocol used in VPNs.

IPsec integrates security at the IP layer. In order to provide higher layer services such as the VPN, it defines the ESP (Encapsulation Security Payload) protocol. IPsec offers data privacy, data integrity, anti-replay protection and data source authentication. It can be used either in tunnel or transport mode. The transport mode leaves the IP header untouched and it is used to protect only the upper-layer protocols. The tunnel mode protects the entire IP datagram by use of encapsulation and therefore protecting traffic between two end-hosts or two gateways (e.g. routers, firewalls) or between an end-host and a gateway (Resende and Rapoport, 2003). Since this is more properly the case of this study, the focus will be on tunnel mode.

The data link to be used will be Frame Relay, a robust technology which does not discard packets in upper layers (application) due to physical failures. Despite it occurs in low layers and throughput be influenced by the number of users sharing the link, the maximum theoretical performance for a MTU of 1500 bytes up to 99.66% (Rattmann et al, 2006). The MTU must be configured with the same size on both ends of the tunnel.

4.2.1. Wired Link – Theoretical Analysis

The use of IPsec in tunnel mode increases the size of the packet and the processes of encapsulation, transmission over the tunnel and desencapsulation. As a result, performance of data traffic is degraded. The increase of packets transmitted is known as space overhead (Xenakis et al, 2006).

The ESP header contains from 2 to 3 words of 32 bits. There is a field Security Parameters Index (SPI) and sequence number. The third word of 32 bits is used to encrypt the data. The ESP uses encryption mechanisms such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard). The AES is an evolution of DES, presenting less processing time and greater security, by using different sizes of encryption keys and processing functions (Xenakis et al, 2006). The data integrity is achieved through the HMAC, a field of authentication of variable length and it is inserted after the payload and used for the digital signature with shared key (Tanenbaum, 2003). Figure (5) shows the headers added considering the ESP method (Xenakis et al, 2006).

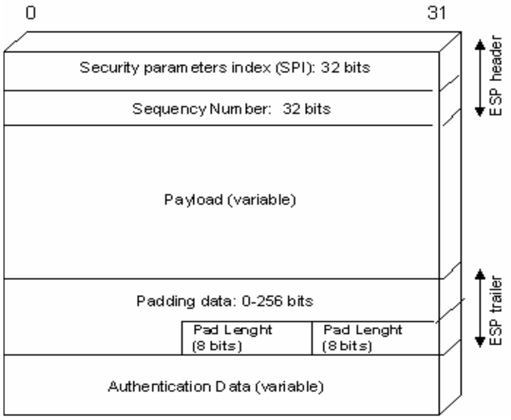

Figure 5 – ESP protocol overhead

In tunnel mode, the ESP header is inserted after the IP header encrypted, and then the new header created is inserted containing the routing information for the packet to traffic within the route of the tunnel. Thus, the total space overhead is the sum of the overheads of Fig. (5) with the new IP header. Figure (6) shows the IPsec frame format.

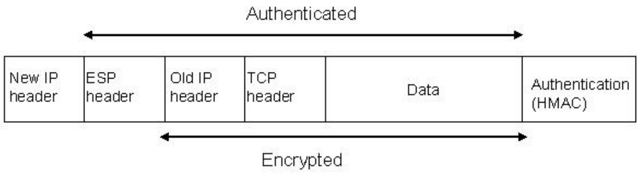

Figure 6 - IPsec frame with ESP protocol

The size of the protected package is given by Eq. (7), where (Xenakis et al, 2006):

Table 6 – Definitions and Equations for IPsec packet calculation

Parameter	Description	Size
$SL_{ESP-CNF-ATH}$	Protected packet size considering the IPSec ESP protocol with mechanisms for confidentiality and authentication	variable
Bl	Size of the field of encryption algorithms	8 bytes for DES, 16 bytes for AES
AuT_{ESP}	Size of the field of authentication of data of ESP protocol	12 bytes
H_{ESP}	ESP overhead size	8 bytes
H_{IP}	IP overhead size	20 bytes
H_{TCP}	TCP overhead size	20 bytes
S_d	User data packet size	MTU
T_{rESP}	ESP trailer size	2 bytes

$$SL_{ESP-CNF-ATH} = \left\lceil \frac{S_d + H_{TCP} + H_{IP} + T_{rESP}}{Bl} \right\rceil \cdot \left(Bl + H_{ESP} + H_{IP} + AuT_{ESP} \right) \tag{6}$$

With values from Tab. (6), the simplified equation is:

$$SL_{ESP-CNF-ATH} = \left\lceil \frac{MTU + 42}{Bl} \right\rceil \cdot (Bl + 40) \tag{7}$$

The size of IPsec packet is shown in Tab. (7) for AES and DES algorithms:

Table 7 - IPsec packet for different encryption algorithms

MTU (bytes)	**100**	**500**	**1000**	**1500**
SL_{AES}(bytes)	497	1897	3647	5397
SL_{DES}(bytes)	852	3252	6252	9252

According to Tab. (7), it is possible to conclude that IPsec in tunnel mode significantly increases the size of the packet to be sent due to space overhead. These results are used to determine the time required to transmit a frame containing a particular Frame Relay MTU considering the usage of AES or DES encryption methods.

Whereas the overhead of a Frame Relay has 9 bytes (Tanenbaum, 2003), the Eq. (8) gives the time necessary to transmit the Frame Relay packet for each MTU. Results are shown in Tab. (8).

$$T_{IP\sec/FR_{MTU}} = \frac{9 + SL_{ESP-CNF-ATH}(MTU)}{2Mbps} \tag{8}$$

Table 8 - Time to transmit a packet on FR link

MTU (bytes)	**100**	**500**	**1000**	**1500**
Tipsec/FR(sec) - AES	0.0020	0.0076	0.0146	0.0216
Tipsec/FR(sec) - DES	0.0034	0.0130	0.0250	0.0370

Figure (7) shows the time to transmit a packet for the wireless and wired links considering AES and DES algorithms. Note that in the wireless link the time is very short if compared to the wired path even for the both algorithms, and therefore it has less impact in the degradation of the requirement. This is because the overhead in protocol WPA-2 is much smaller than that introduced by IPsec. It is important to note that the AES algorithm showed better results than the DES algorithm, due to the results obtained from Eq. (7) for the final size of the IPsec packet.

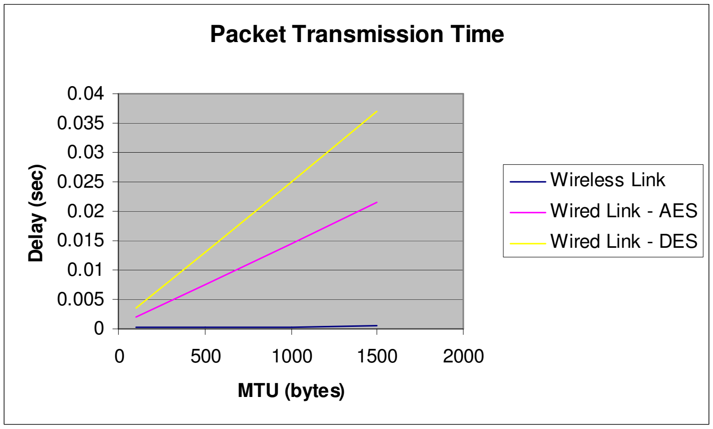

Figure 7 – Packet Transmission Time for wireless and wired paths

The time required to transmit a packet from the aircraft to the maintenance center for a certain MTU is given by Eq. (9):

$$T_{end\text{-}to\text{-}end} = Ttotal_{MTU(with\_retransmission)} + T_{IPsec/\,FR} \quad (9)$$

Finally, considering the 10Mbytes to be sent, the total time to transmit a file from the aircraft to the server (802.11 link + Frame Relay link) is given by Eq. (10) for various values of MTU, where $n(MTU)$ expresses the number of frames needed to transmit the 10Mbytes for each MTU, considering 40 bytes related to TCP and IP frames.

$$Tfinal = n(MTU)\cdot T_{end-to-end} \quad (10)$$

Figure (8) shows that, using the AES encryption and a MTU of 1500 bytes, the data transmission is performed in approximately 2.5 minutes.

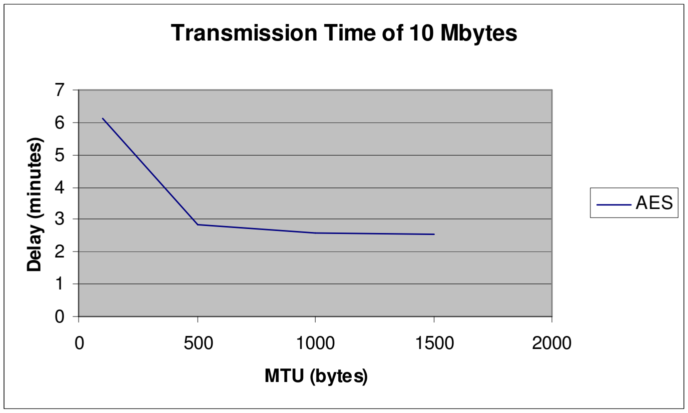

Figure 8 – Time to transmit 10Mbytes in all the link aircraft - server

5. CONCLUSIONS

The technologies addressed in this study - Gatelink associated with a network infrastructure at the airport - are capable to provide advanced security mechanisms to ensure that the raw data for PHM processing is delivered to the maintenance center of the airline for analysis and diagnosis. The WPA-2 ensures confidentiality and integrity with a high-throughput data, which allows data to be transmitted in a short time interval, for all sizes of MTU analyzed. IPsec generates a significant increase in space overhead, impacting directly on the time to transmit a packet. It is noticed that the use of AES encryption algorithm has minor damage on the packet transmission time. In addition, it is more secure than the DES. It is possible to conclude that the MTU is almost constant from 500 bytes to 1500 bytes. Thus, throughput can be estimated as reasonable to meet the requirements considering a probability of bit error of 10-5 for a MTU of 1500 bytes. Since this study was based on theoretical analysis, simulations on testbeds are essential to prove the results obtained herein, in a future work. In addition, future work should include evaluation of other parameters such as authentication time and SNR (Signal-to-noise) variation.

6. REFERENCES

Akhavan, M.R. “Study of the performance limits of IEEE 802.11 WLANs”, Master Thesis, Computer Science and Engineering, Lulea University of Technology, 2006, 49p.

Gast, M. “When Is 54 Not Equal to 54? A Look at 802.11a, b, and g Throughput” O’REILLY, 2003.

Gun, A., Hunt, R., “The Performance of the IEEE 802.11i Security Specifications on Wireless LANs”, Private Communication, University of Cantenbury, 2005.

Pellejero, I, “Compatibility between IEEE 802.11b and IEEE 802.11g networks: Impact on throughput”. Proceedings of THIRD INTERNATIONAL WORKING CONFERENCE. West Yorkshire, 2005.

Rattmann, A.C, Buscatto, A.C, Muncinelli, G. “Desempenho de redes WAN não é apenas throughput” RTI nº 74 Magazine, 2006 .

Rezende, J., Rapoport, E., “IPSEC – Protocolo de Segurança IP”, Private Communication, Universidade Federal do Rio de Janeiro, 2003.

Roshan, P., Leary, J., 2003, “802.11 Wireless LAN Fundamentals” Cisco Press, 312 p.

Shuwarrtz, M. “Telecommunication Networks: Protocols, Networking and Analysis” Prentice Hall, 1987, 724p.

Tanenbaum, A.S. “Computer Networks”. 4th ed, Prentice Hall, 2003, 384 p.

Wright, T.H., Ziarno, J.J., “Wireless, Ground Link-Based Aircraft Data Communication System with roaming feature”, United States Patent Application Publication, United States, US 7,426,388 B1, September 2008.

Xenakis, C. Laoutaris, N. Merakos, L. Stavrakakis, I. “A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms”, Computer Networks, vol 50, pp3226-3240, 2006.

7. RESPONSIBILITY NOTICE

The authors are the only responsible for the material included in this paper.