An Experimental Study on Wireless Security Protocols over Mobile IP Networks

Avesh K. Agarwal
Department of Computer Science
North Carolina State University
Raleigh, NC 27695
Email: akagarwa@unity.ncsu.edu

Jorinjit S. Gill
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC 27695
Email: jsgill@unity.ncsu.edu

Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC 27695
Email: wwang@unity.ncsu.edu

***Abstract*— Security protocols have emerged as a vital issue to support secure and reliable communications over wireless networks. Many work have discussed security services from a functional perspective; however, there is a lack of quantitative results demonstrating the impact of security protocols on system performance that can be affected dramatically by applying security policies in combination with mobility. Therefore, we conduct an experimental study on a wireless IP testbed, and analyze the interaction of security protocols at different layers with respect to data streams, delay and throughput. In this paper, we present a comprehensive analysis of performance measurements and the overhead associated with several most widely used protocols such as WEP, IPSEC, 802.1x and SSL.**

I. Introduction

Wireless technologies provide ease of accessibility to the Internet virtually from anywhere and enable freedom of mobility for users by releasing the constraint of physical connections to networks. Besides these advantages, inherent broadcast nature of wireless networks has raised security concerns because when data is exchanged over air medium, interception and eavesdropping become easier to anyone with radio access equipment. Consequently it necessitates the need to deploy security services provided by security protocols.

Existing security protocols provide security features at different network layers. For example, Wired Equivalent Privacy (WEP) is the very first protocol to be considered for a wireless network, which works at Medium Access Control (MAC) layer but has been identified with major security drawbacks. To overcome WEP weaknesses, a new standard 802.1x is designed, which also works at MAC layer, and provides port-based access control for wireless nodes. Also, 802.1x exploits the use of Extensible Authentication Protocol (EAP), which is used as a transport mechanism. At network layer, we consider IP Security (IPsec) protocol suit, which is originally designed for wired network, but it is now being considered for wireless network due to its strong authentication and encryption methods. Secure Sockets Layer(SSL) is a transport layer protocol, and it is the most widely deployed security protocol on the Internet today. At application layer, Remote Authentication Dial-In User Service (RADIUS) protocol is considered, which is based on client-server architecture.

Although security protocols exist at every network layer; however each security protocol has its own weaknesses. Paper [2] shows serious weaknesses in WEP. Another Paper [6] explains different types of attacks on 802.1x. The main issue, we observe, is that research efforts have been focused on security aspects with little concern about performance overhead caused by security protocols in real systems. These protocols impact the performance of network entities in terms of delay and throughput. Therefore, we conduct an experimental study providing comprehensive quantitative measurements on actual systems to show the performance degradation caused by security policies in various mobility circumstances.

Further, we discuss a comparative study of different security policies over variety of mobile environments. Moreover, we also provide a deep insight into the impact of security protocols on the system performance regarding authentication delay and throughput, which will help in building a solid ground for network designers to develop new security services with respect to quality of service (QoS) satisfaction.

The remainder of the paper has been organized as follows. Section II discusses related work. Descriptions of testbed architecture to explain real environment used for our experiments, security policies, mobility circumstances and performance metrics are in Section III. Section IV presents experimental results for each mobility scenario in the context of different security policies. We conclude paper in Section V.

II. Related Work

Paper [3] shows performance of IPSEC mechanisms analyzing different security algorithms. Similarly, paper [8] analyzes IPSEC performance as virtual private networks (VPN). Furthermore, the study conducted in [2] discusses advantages and disadvantages of security protocols with respect to security aspects by showing serious weaknesses in WEP. Another Paper [6] explains different types of attacks implemented on 802.1x. Based on these studies, we notice that limited effort is focused on performance aspects of security protocols.

Our study is different from existing studies because our paper, besides considering different traffic types such as TCP and UDP, also focuses on the impact of security protocols in mobile environments. Moreover, our work has considered a

0-7803-8521-7/04/$20.00 © 2004 IEEE

wide rage of security protocols at different network layers, such as 802.1x, WEP, SSL other than just IPSEC. In addition, We also discuss the combined impact of security protocols when configured together in the network. Unlike existing studies, We mainly focus on the quality of service (QoS) aspects of the network. To our knowledge, this is the first study that analyzes security protocols in different mobility scenarios by considering traffic streams with different characteristics.

III. Infrastructure and Performance Evaluation

To achieve the aforementioned goals, we designed various experiments based on security policies, mobile scenarios and performance metrics, which are described in this section.

A. Testbed Architecture

Figure 1 shows the testbed architecture used for our experiments. There are two subnets in the testbed, each consisting of a router which acts as a home agent (HA) and a foreign agent (FA) connected to Cisco Access Points to provide wireless connectivity. Each router also has functions of an IPSEC gateway and a RADIUS server for authentication in IPSEC and 802.1x policies respectively. Different security protocols have been configured to provide security over wireless segments of the network. An IPSEC tunnel is setup between two home agents to provide security over wired segments of the network. So each segment in the network is secured. Here below we provide hardware and software details for each network entity. All systems use Redhat Linux 9.0 kernel 2.4.20. Hardware

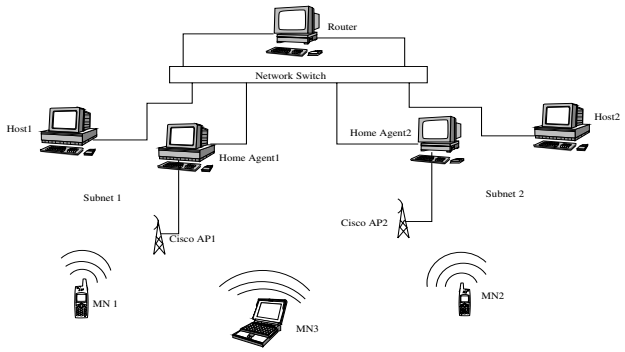

Fig. 1. Testbed Architecture.

specifications of components in the testbed are listed below:

- Router : Dell PC, Pentium IV 2.6 GHZ (Linux)
- Home Agents : Dell PC, Pentium IV 2.6 GHZ (Linux)
- Hosts : Dell PC, Pentium IV 2.6 GHZ (Linux)
- MN iPAQ : Intel StrongARM 206 MHZ (Familiar Linux)
- MN Sharp Zaurus : Intel XScale 400 MHz (Linux Embedix)
- MN Dell Laptop : Celeron Processor 2.4GHZ (Linux)
- Access Points : Cisco Aironet 1200 Series
- Network Switch : Cisco Catalyst 1900
- Wireless Cards : Netgear MA 311

Open-source software components used are as follows.

- FreeSwan [4] for IPSEC
- Xsupplicant [1] for 802.1x supplicant
- FreeRadius [9] for Radius server
- OpenSSL [7] for SSL
- Mobile IP from Dynamic [5]
- Ethereal packet analyzer
- Netperf and ttcp network monitoring utilities

B. Security Policies

Security policies are designed to demonstrate potential security services provided by each security protocol. Each protocol uses various authentication and encryption mechanisms to provide security. Therefore, by configuring different security mechanisms for each protocol, a variety of security policies are implemented in the testbed. Besides individual policies, hybrid security policies are also configured involving multiple security protocols at different network layers. All security policies demonstrated in the paper are shown in TABLE I.

TABLE I
Security Policies

Policy No.	Security Polices
PN-1	No Security
PN-2	WEP-128 bit key
PN-3	IPSEC-3DES-SHA
PN-4	IPSEC-3DES-SHA-WEP-128
PN-5	8021x-EAP-MD5
PN-6	8021x-EAP-TLS
PN-7	8021X-EAP-MD5-WEP-128
PN-8	8021X-EAP-TLS-WEP-128
PN-9	8021X-EAP-MD5-WEP-128-IPSEC-3DES-MD5
PN-10	8021X-EAP-TLS-WEP-128- IPSEC-3DES-MD5
PN-11	8021X-EAP-MD5-WEP-128-IPSEC-3DES-SHA
PN-12	8021X-EAP-TLS-WEP-128-IPSEC-3DES-SHA

C. Mobile Circumstances

We evaluate security policies in different mobile scenarios by considering current location of the mobile node (MN) in the network. Therefore, we investigate both ”no roaming” (NR) and ”with roaming” (WR) scenarios. ”With Roaming” (WR) scenario refers to the situation when one of the mobile nodes is visiting a foreign network, whereas ”no roaming” (NR) scenario means when all MNs stay in their home network. Moreover, those mobility scenarios take into account the presence of correspondent nodes (CN) also. In our testbed, we have considered correspondent nodes as both wireless and wired. TABLE II shows all the scenarios considered.

D. Performance Metrics

We measure the impact of policies on the system performance and QoS with regard to following metrics.

- *Authentication Time (AC)* is the time involved in an authentication phase of a security protocol.
- *Encryption Cost (Bytes/Second) (EC)* refers to the overhead associated in encrypting and decrypting the data.
- *Response Time (End-to-End) (EE)* is a measure of delay in transmission of data between end nodes.

TABLE II

MOBILITY CIRCUMSTANCES

No.	Scenario	Roaming
M1	Mobile To Mobile Node in Same Domain	No Roaming "NR"
M2	Mobile Node To Home Agent	
M3	Mobile Node to Corresponding (Fixed) Node in Same Domain (Register to HA)	
M4	Mobile Node To Mobile Node In Different Subnets	
M5	Mobile Node To Correspondent(Wired) node in same domain	
M6	Mobile Node To Mobile Node In Different Domains	With Roaming "WR"
M7	Mobile Node to Corresponding (Fixed) Node in Different Domain (Register to FA)	
M8	Mobile node and Correspondent(Wired) node in different domain	
M9	Mobile To Mobile Node in Same Domain	

- *Throughput (Bytes/Second) (TP)* is a measure of data transfer rate in unit time period between end nodes.

IV. EXPERIMENTAL RESULTS

In this section, we discuss performance impact of above-mentioned security policies in various mobility scenarios in terms of encryption cost, authentication delay and throughput.

A. Authentication Time

TABLE III shows authentication time (sec) for IPSEC and 802.1x security policies. Since WEP does not involve exchange of control messages, so there is no authentication time involved in it. Moreover, authentication time for IPSEC and 802.1x also involves Mobile IP authentication time. We observe that when an MN is not roaming, IPSEC authentication takes longer time than 802.1x. However, when an MN roams, the 802.1x authentication time is longer. This is due to the fact when a MN roams, MN reauthenticates with an FA using 802.1x mechanism, whereas this is not the case with IPSEC protocol, because the IPSEC tunnel is already established between the MN and the HA. It is also observed that 802.1x with IPSEC policies causes longer authentication delay than 802.1x without IPSEC policies. Furthermore, TABLE III shows that 802.1x-EAP-TLS authentication time is longer than 802.1x-EAP-MD5 because 802.1x-EAP-TLS uses digital certificates for mutual authentication, which involves exchange of several control packets.

B. Encryption Cost

Figures from 2 to 10 demonstrate encryption cost for TCP and UDP traffics in different mobility scenarios. It is observed that IPSEC causes more encryption overhead than WEP and 802.1x in most of the scenarios. We also notice that 802.1x and WEP encryption costs are almost the same because 802.1x uses WEP as its encryption mechanism. Now in next paragraphs, we discuss "NR" and "WR" scenarios in detail.

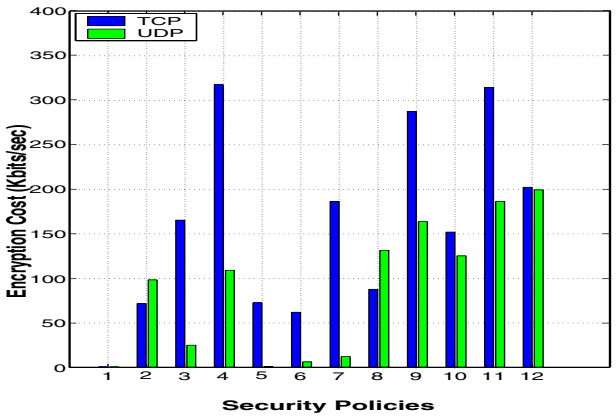

Fig. 2. Scenario M1 - TCP/UDP Encryption Cost.

1) Scenarios without Roaming: Encryption costs for TCP and UDP for M1, M2 and M3 are shown in Figures 2, 3 and 4 respectively. We observe that encryption overhead for TCP is higher than that of UDP for most of the policies in these scenarios. This is because TCP requires acknowledgments for each segment sent, whereas UDP being unreliable does not require such acknowledgments. We can infer that in these scenarios, applications running over TCP can suffer higher QoS degradation than applications running over UDP. If we compare M1 with M2, we observe that TCP encryption cost in M2 is more affected than in M1. But for UDP, encryption overhead for M2 is less affected than that of M1. In addition, scenario M3 behaves very similar to M1 because end points, as MN in M1 and CN in M3, are wireless nodes in the same domain leading to similar network structures.

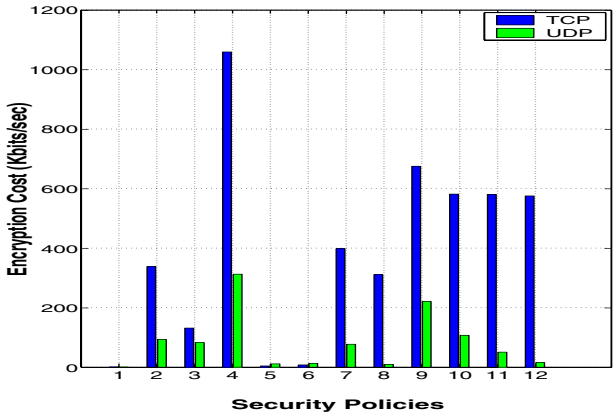

Fig. 3. Scenario M2 - TCP/UDP Encryption Cost.

Based on these observations, we can conclude that since a MN communicates with home agent only during initial setup so we suggest, for less authentication delay during initial setup, UDP data stream can be used by applications, and after that applications may switch to TCP for reliable communication at the cost of higher encryption overhead. Moreover, If a home agent is functioning as some application server, then applications running over UDP may suffer less performance

TABLE III

AUTHENTICATION TIME MEASUREMENTS FOR VARIOUS SECURITY POLICIES

Policy	M1	M2	M3	M4	M5	M6	M7	M8	M9
IPSEC(sec)	1.405	1.405	1.405	1.405	1.405	1.432	1.432	1.432	1.432
802.1x-EAP(MD5) without IPSEC(sec)	0.427	0.427	0.427	0.427	0.427	1.749	1.749	1.749	1.749
802.1x-EAP(MD5) with IPSEC(sec)	1.722	1.722	1.722	1.722	1.722	1.749	1.749	1.749	1.749
802.1x-EAP(TLS) without IPSEC(sec)	1.822	1.822	1.822	1.822	1.822	3.144	3.144	3.144	3.144
802.1x-EAP(TLS) with IPSEC(sec)	3.117	3.117	3.117	3.117	3.117	3.144	3.144	3.144	3.144

degradation whereas application running over TCP may suffer higher performance degradation. Also, if we compare PN3 security policy with the other policies, we observe that encryption cost in PN3 is the lowest compared with other policies except policies PN5 and PN6, but PN5 and PN6 do not use any encryption mechanisms. Therefore, we conclude PN3 may be a better choice for application running over TCP for providing security services over wireless networks.

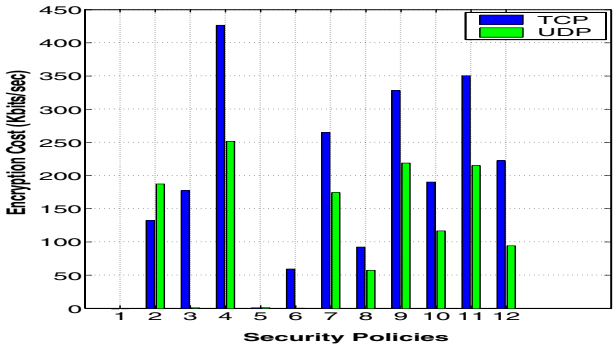

Fig. 4. Scenario M3 - TCP/UDP Encryption Cost.

Figures 5 and 6 show encryption costs for M4 and M5 respectively. We observe that in M4 and M5, UDP encryption cost is higher than TCP encryption cost. We infer that applications running over UDP in M4 and M5 may suffer more QoS degradation than application running over TCP. Further, we notice that encryption cost for UDP in PN12 is the minimum as compared to other policies. Since PN12 provides stronger security than other policies, it may be a better choice for UDP applications. In addition, PN12 may be a suggested choice for TCP applications also because it provides a better tradeoff between security and encryption overhead.

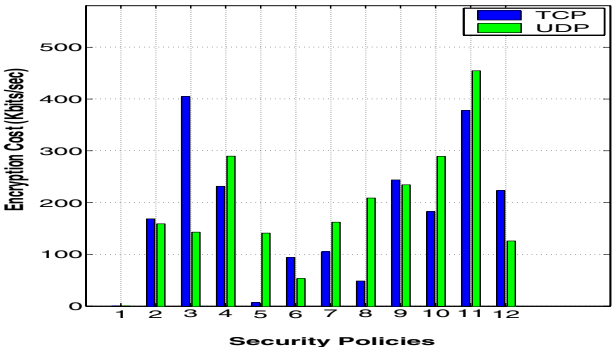

Fig. 5. Scenario M4 - TCP/UDP Encryption Cost.

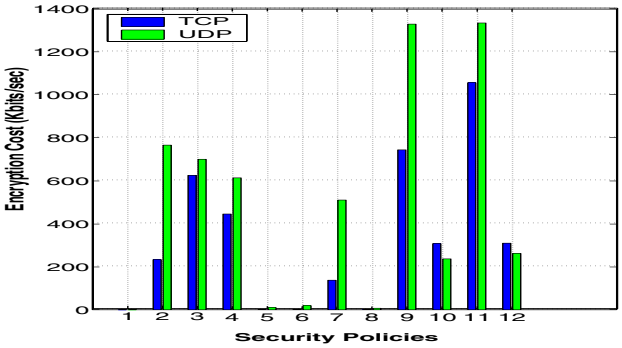

Fig. 6. Scenario M5 - TCP/UDP Encryption Cost.

2) Scenarios with Roaming: Figures 7, 8, 9 and 10 show encryption costs for scenarios with roaming. We observe that UDP encryption cost in M6, M7 and M8 is higher than TCP encryption cost. But in M9, TCP encryption cost is higher which explains that not only mobility but location of end points also effects encryption overhead. Difference in behavior in M9 can be attributed to the fact that, in M9, both end points are in the same domain, whereas, in other mobility scenarios, end points are in different domains.

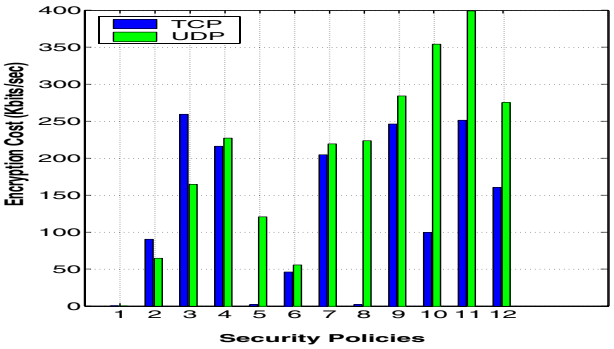

Fig. 7. Scenario M6 - TCP/UDP Encryption Cost.

We observe from Figure 7 that PN3 for UDP traffic provides less encryption overhead than other policies except PN2, PN5 and PN6, but PN2, PN5 and PN6 do not provide strong security so PN3 may be a recommended choice for applications running over UDP in M6. But for TCP, PN10 provides better tradeoff between security services and encryption overhead. Furthermore for scenario M7, we notice the same behavior as for M6. In addition, Figure 9 demonstrates that PN10 provides less encryption overhead than most of the other policies for both UDP and TCP streams in scenario M8, whereas we find that PN3 may be a better choice in M9 for providing security.

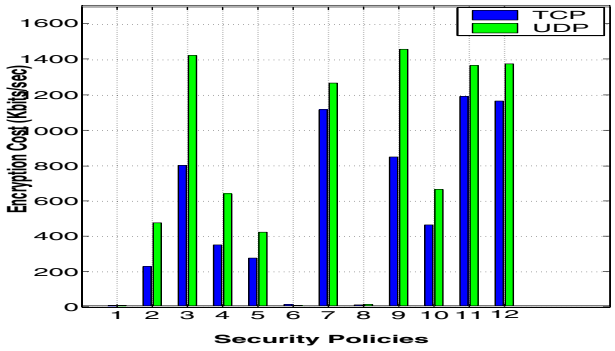

Fig. 8. Scenario M7 - TCP/UDP Encryption Cost.

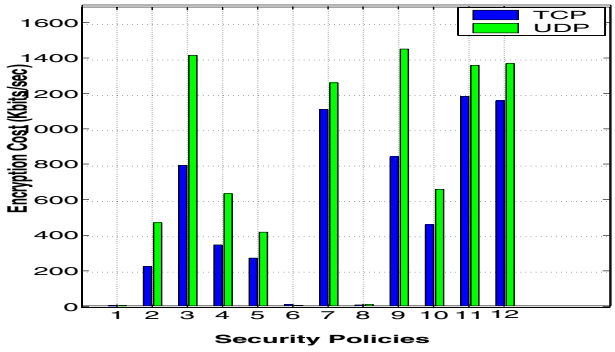

Fig. 9. Scenario M8 - TCP/UDP Encryption Cost.

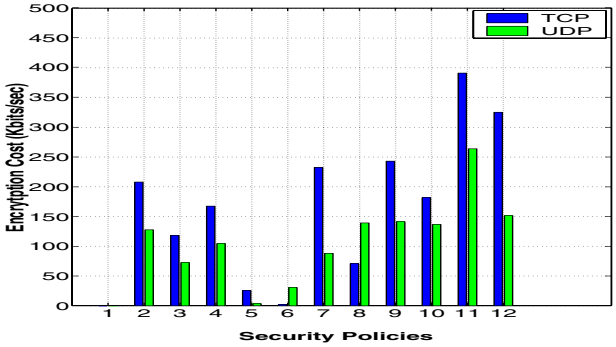

Fig. 10. Scenario M9 - TCP/UDP Encryption Cost.

C. Throughput

Figures 11 and 12 demonstrate throughput variations for TCP and UDP data streams for some security policies in all mobility scenarios. Here we have presented only one security policy for each security protocol. We observe that overall IPSEC security policies cause greater decrease in throughput than WEP and 802.1x security policies. This is because IPSEC uses 3DES encryption algorithm which is computationally slower than the encryption algorithm used in WEP and 802.1x. But IPSEC provides stronger security services which compensates for the higher encryption overhead.

V. Conclusion

Results presented in the paper demonstrate that WEP causes little overhead because WEP is implemented in hardware in

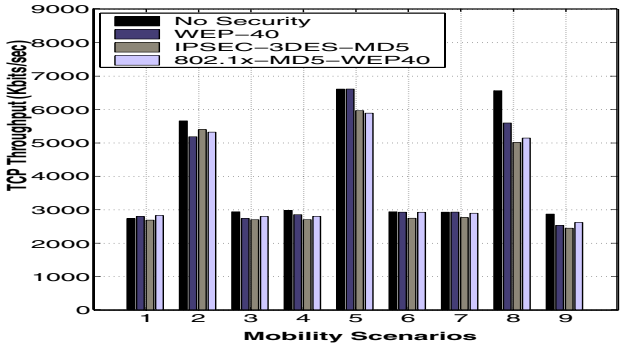

Fig. 11. TCP Throughput.

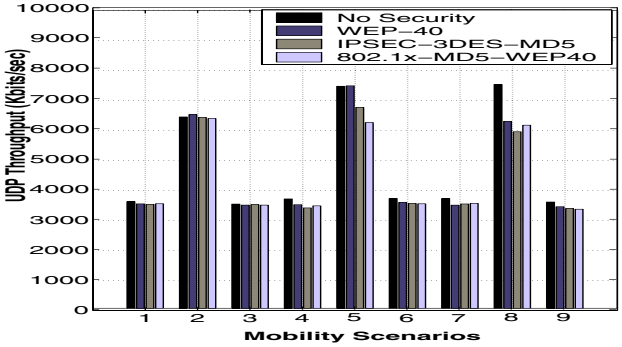

Fig. 12. UDP Throughput.

Cisco access points, whereas IPSEC policies cause significant overhead but provide strong security services. Moreover, 802.1x with EAP-MD5 introduces less overhead than 802.1x with EAP-TLS during authentication; but EAP-TLS provides stronger authentication than EAP-MD5, therefore 802.1x(EAP-TLS) offers better alternative for MAC layer authentication. Further, node mobility also effects overhead based on the location of end points and traffic stream(TCP or UDP) chosen. Also, we observe that throughput variations due to mobility are higher in UDP than in TCP.

References

[1] 802.1x Supplicant. *http://www.open1x.org*.
[2] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications:the insecurity of 802.11. *Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking*, July 2001.
[3] O. Elkeelany, M. M. Matalgah, K.P. Sheikh, M. Thaker, G. Chaudhary, D. Medhi, and J. Qaddour. Perfomance analysis of ipsec protocol: Encryption and authentication. *IEEE Communication Conference(ICC)*, pages 1164–1168, May 2002.
[4] IPsec. *http://www.freeswan.org*.
[5] Mobile IPv4. *http://dynamics.sourceforge.net*.
[6] Arunesh Mishra and William A. Arbaugh. An Initial Security Analysis of the IEEE 802.1X Standard. *http://www.cs.umd.edu/ waa/wireless.html*, Feburary 2002.
[7] OpesnSSL. *http://www.openssl.org*.
[8] Wei Qu and Sampalli Srinivas. Ipsec-based secure wireless virtual private networks. *MILCOM*, pages 1107–1112, OCT 2002.
[9] Radius. *http://www.freeradius.org*.