Measuring Performance Impact of Security Protocols in Wireless Local Area Networks

Avesh K. Agarwal Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC 27695

Abstract - In this paper, we study and quantify the impact of the most widely used security protocols, such as 802.1x, EAP, IPSEC, SSL and RADIUS, in wireless local area networks (WLANs). Based on the measurements in a wireless network testbed, we present quantitative, realistic findings with regards to both security functions as well as network performance. First, we describe experimental setup including system configuration and protocol stack. Then, we consider a variety of individual and hybrid security policies in order to capture the impact of security services at different network layers. Moreover, depending upon mobile nodes' current location, user mobility is categorized into non-roaming and roaming scenarios. In addition, we define several performance metrics such as authentication delay, authentication messages, response time, throughput to measure the overhead associated with security policies on system performance. Comprehensive experimental measurements and analysis are provided for TCP/UDP traffic streams and network variations to demonstrate the impact of security protocols in wireless local area networks.

Keywords- Wireless local area network, security protocols, security policies, performance metrics, network scenarios.

I. Introduction

Wireless local area networks (WLANs) have become increasingly popular for their deployment in organizations, campuses and public hotspot areas such as airports and hotels. This is due to freedom of mobility for users by releasing the constraint of physical connections as well as increase in usage of mobile devices such as laptop computers and handhelds. Besides these advantages, inherent broadcast nature of wireless networks has raised security concerns [1], [2]. Wireless networks are susceptible to many attacks since interception and eavesdropping of data in transit is possible for anyone with access to wireless network [3], [4], [5]. Such security issues necessitate the need to apply security mechanisms to protect the communications at the expense of system resource. Meanwhile, security services are not free as security protocols consume valuable system resources. Thus, providing high level of security becomes a concern in mobile environments in which system resources are very limited [6].

The system resources, which are of concern in mobile wireless environments, include such as bandwidth, memory, processing power and devices, such as computer Laptops and Handhelds, which operate on battery power. Devices can not implement system programs with high computational requirements, because system programs developed for mobile wireless networks must be resource efficient. Therefore, there is an acute need to quantify and analyze the performance overhead introduced by security protocols so that appropriate security services can be provided in mobile wireless environments.

Throughout our experimental study for mobile wireless LANs, we focus on addressing the following questions:

- Which security policy is appropriate in a particular mobility scenario so that bandwidth utilization and delay are degraded as little as possible?
- How much system overhead is caused by different security policies for various network scenario?
- What traffic stream is the most appropriate for each security policy in a particular mobility scenario?
- How much authentication delay is caused by each security policy in different mobility scenarios?
- What is the performance impact of hybrid security policies in the wireless local area networks?

In order to address the cross-layer questions, we present a thorough experimental analysis of security policies at different network layers. We conduct a comparative study of different security policies over variety of mobile environments. Moreover, we analyze traffic streams such as TCP and UDP in each network scenario for each security policy. Measurements provided in this study are explained to show how integration of quality of service (QoS) and security service affects system performance. In addition, our paper provides comprehensive quantitative analysis demonstrating the impact of security protocols on the system performance in term of authentication delay, throughput and response time. We believe that our paper provides a solid ground for network designers to develop new security services in combination with QoS satisfactions.

To conduct our research systematically, we have setup an experimental testbed. The testbed is a miniature of existing wireless networks, which ensures that our experimental results can be mapped to large scale wireless networks. Moreover, our experimental study aims to uncover performance issues for security protocols at different network layers, which will help network designers to optimize system programs to be used in the mobile wireless networks and to choose better security service while maintaining network QoS requirements.

The remainder of the paper has been organized as follows. Section II introduces background and related work. We describe implementation details in Section III. Network scenarios, security policies and performance metrics are illustrated in Sections IV, V, VI, respectively. Details about data acquisition are provided in Section VII. Experimental results and performance analysis are presented in Sections VIII and IX, respectively. In Section X, we conclude the paper.

II. Background

The motivation behind this study is mainly because of the following concerns in wireless local area networks:

- Performance issues in WLANs;
- Security in WLANs;
- Resource constraints in WLANs; and the most important
- Impact of security services on QoS in WLANs

Network performance is characterized by certain parameters such as end-to-end delay, total system throughput, bandwidth usage perception, packet loss, user level response and so on. These parameters enable both network administrator and mobile users to quantify QoS provided by the network. Moreover, wireless networks provide relatively low bandwidth and higher packet loss due to unreliable radio links [6]. In addition, wireless networks are highly susceptible to many kinds of attacks due to their inherent broadcast nature and shared air medium. In addition, devices used in wireless networks are equipped with less processing power, less memory space leading to stringent system requirements on the use of system resources. Therefore, it is vital to determine the performance impact caused by security services in mobile wireless networks.

To address security issues, many protocols are developed, which operate at different network layers. Wireless Equivalent Privacy (WEP), 802.1x with Extensible Authentication Protocol (EAP), Remote access dial in user service (RADIUS), IP security (IPSEC) and Secure Socket Layer (SSL) are some of the protocols used in wireless networks. We focus on studying these security protocols because they operate at different network layers, which will help us to analyze the overhead introduced by security services across network layers. Moreover, these protocols are widely adopted in the wireless networks providing a very close analysis which will be useful for the real time networks. Brief description of these protocols is as follows:

MAC Layer Protocols: WEP is the very first protocol to be considered for wireless networks. WEP has been identified to be susceptible to many type of attacks [3]. To overcome WEP weaknesses, IEEE 802.1x standard is designed to provide stronger security [7], [8]. 802.1x works at MAC layer and provides port-based access control for wireless nodes. In addition, 802.1x exploits the use of EAP(MD5,TLS), which is used as transport mechanism [9]. Besides considering MAC layer security protocols, we also evaluate network layer and transport layer security protocols such as IPSEC, SSL and RADIUS.

Higher Layer Protocols: IPsec is a network layer protocol, originally designed for wired network, which is now being considered for wireless networks due to its strong authentication and encryption methods. Further, SSL is a transport layer protocol, and it is the most widely deployed security protocol on the Internet today. At application layer, we consider RADIUS protocol, which is based on client-server architecture.

Existing security protocols have some drawbacks and are prone to several attacks. For example, according to previous studies, WEP and 802.1x are susceptible to many types of attacks [3], [4] and [5]. In addition, there are other studies which explain the security aspects of WLANs providing overview of various security protocols such as [2]. To overcome these problems, researchers have come up with many solutions to improve the security aspects of these protocols in recent years. For example, recently a new authentication protocol is proposed for wireless networks in [10]. In addition, other works have proposed solutions to improve security for mobile wireless networks [11], [12] and [13]. Moreover, there are other studies, which focus on performance aspects of security protocols. For example, a performance analysis of different protocols of IPSEC is provided in [14]. Similarly, IPSEC performance is also analyzed as virtual private networks (VPN) in [15]. In addition, a proposal is provided to implement wireless gateway for WLAN based on IPSEC protocol in [16]. But, we observe that most of the research is focused on security aspects with little thoughts given to performance impact of security protocols on system performance. Therefore, we conduct comprehensive experimental analysis to uncover performance issues associated with security protocols in mobile wireless LANs.

Research conducted in this paper is different from previous studies in many ways. Our study, besides considering different traffic types, focuses on the impact of security protocols on different user's mobility scenarios in combination with Mobile IP which introduces WLAN roaming. Moreover, our analysis has considered a wide range of security protocols at different layers such as 802.1x, WEP, SSL other than just IPSEC. Unlike previous studies, we focus on the quality of service (QoS) aspects of the network determining impact on QoS when security services are enabled in the wireless networks. To our knowledge, this is the first experimental study on this issue, which analyzes security protocols in various mobility scenarios.

III. Implementation Setup

Our platform is a miniature of WLANs, on which we carry out a variety of experiments, which are designed to address performance aspects of security protocols. In this section, we provide details of our testbed including hardware equipments and software configurations. Fig. 1 shows an example of testbed architecture in which two subnets are illustrated. Although, we show only two subnets; with different combinations in hardware and software, virtually we create a heterogeneous environment that captures mobile aspects of WLANs.

A. Hardware Configuration

Home agents (HA), B and C, act as gateways for Subnets I and II and are Dell PC with Pentium IV 2.6 GHZ. In addition, HAs also act as foreign agents (FA) and are connected to Cisco Access Points (Cisco Aironet 1200 series) to provide wireless connectivity. Moreover, B and C have functions of IPSEC gateways and RADIUS server for IPSEC and 802.1x, respectively. Further, security over wireless segment in the testbed is provided by configuring different security protocols. An IPSEC tunnel is setup between HAs to provide security over the wired segment in the network. Hosts A and D act as wired correspondent nodes in Subnets 1 and 2 and are Dell PC with Pentium IV 2.6 GHZ. Different mobile devices are iPAQ (Intel StrongARM 206 MHZ), Sharp Zaurus (Intel XScale 400 MHz) and Dell Laptop (Celeron Processor, 2.4GHZ). Cisco Catalyst 1900 series is used as a network switch to provides connectivity between two subnets via router, which acts as a gateway. In addition, we have used Netgear MA 311 wireless cards in our mobile devices.

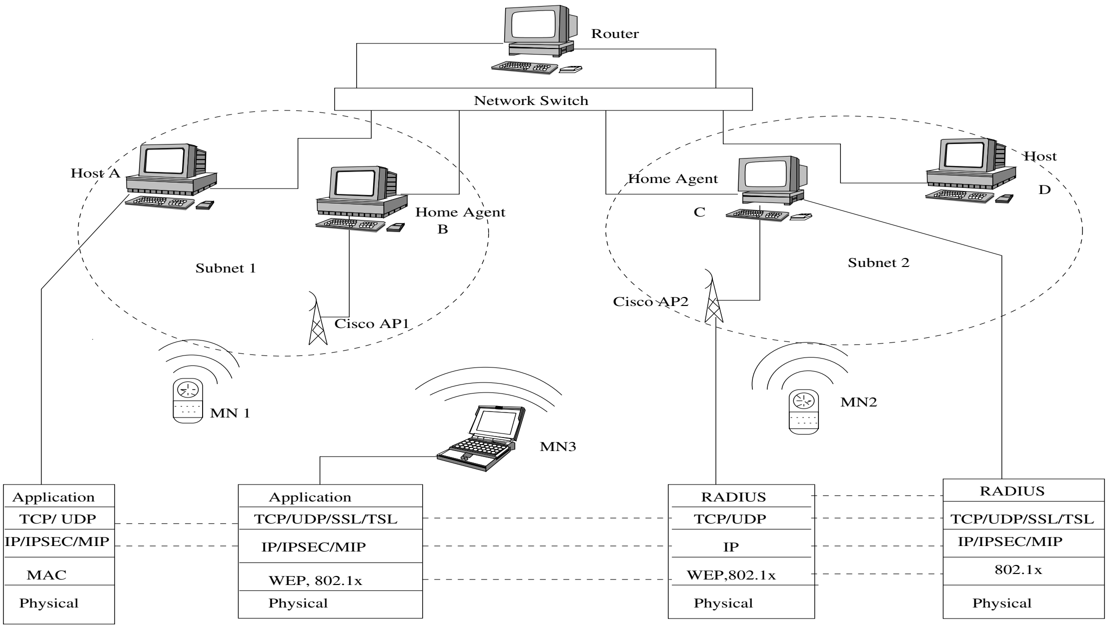


Fig. 1. Testbed Architecture.

B. Software Configuration

Fig. 1 shows protocol stacks installed for different network entities in the testbed. All systems use Redhat Linux 9.0 kernel 2.4.20. We have installed open-source software components for various protocols in the testbed as follows:

- FreeSwan open source is installed on home agents and mobile nodes for IPSEC functionality [17] .
- Xsupplicant, which provides 802.1x client functionality supplicant has been installed on MNs [18].
- RADIUS server functionality has been provided by FreeRadius and has been installed on HAs [19] .
- OpenSSL open source software is installed on HAs [20] .
- To introduce user mobility in our network, Mobile IP implementation from Dynamic is installed on mobile nodes and home agents [21].
- Ethereal packet analyzer is used for packet capturing.
- Iperf and ttcp are used for generating different traffics.

IV. Network Scenarios

Network scenarios are classified into non-roaming ($\mathcal{N}$) and roaming ($\mathcal{R}$) based on user's current location, whether a user is in its home domain or foreign domain respectively. By designing these scenarios, we can capture different mobility situations.

A. Network description

Network scenarios can be described by the following factors:

- User Set, $\mathcal{U} = \{u_1, u_2, \ldots, u_i, \ldots\}$, which represents mobile users in the network.
- Subnet Set, $\mathcal{S} = \{s_1, s_2, \ldots, s_t, \ldots\}$, which represents network domains in the whole network.
- Non-Roaming Scenarios, $\mathcal{N} = \{N_1, N_2, N_3, N_4, N_5\}$. This set defines non-roaming scenarios configured in the wireless network testbed when communicating mobile users are in their home domains.
- Roaming Scenarios, $\mathcal{R} = \{R_1, R_2, R_3, R_4\}$. This set defines roaming scenarios in the network when at least one of communicating mobile users is in a foreign domain.

Further, we provide definition of each network scenario.

B. Non-Roaming Scenarios

Here first we discuss Non-roaming scenario in which case mobile node stays in its home domain.

Scenario N_1**:** It deals with the situation when both mobile nodes are in same domain. In this case, both mobile nodes are in their home domain. This scenario aims to capture impact of security services in one domain only when nodes are communicating over a secure wireless network.

Scenario N_2**:** This specifies the scenario, when mobile node is communicating with home agent itself. It can happen if the home agent is functioning as an application server providing services to the clients in the network. Therefore, this scenario captures impact of the security service on the performance of an application server in the network. Here, the part of communication path is wired, which is not the case in the first scenario.

Scenario N_3**:** It occurs, when mobile node is communicating with correspondent node in the same domain. In this, correspondent node is wireless node without Mobile IP functionality. This scenarios is different from N1, because CN is not moving, which helps us in analyzing impact of security services when one end node is a non-MobileIP node, therefore segregating impact of security services from Mobile IP protocol. Here both end nodes are in their home domains.

Scenario N_4**:** It is to capture the impact of security services when participating end nodes are in different domains. Here, data stream from one node to another node traverses an entire network path which involves both wired and wireless segments. Wired segment can be compared with the Internet, where mobile nodes are communicating over Internet and the secure tunnel is setup between their home networks.

Scenario N_5: This is the case when an MN is communicating with the CN. This scenario is different from N_3 because correspondent node in N_3 is wireless node. Here again, both nodes are part of same domain. This scenario is different from previous scenario except N_2 in the sense one end is wired which helps us in analyzing impact of security services when communication path in mixed of wired and wireless networks. This scenario is different from N_2 in the functionality of one end since in N_2 one end node is home agent providing more functionality in the network which is not the case here.

C. Roaming Scenarios

Till now we have discussed network scenarios where mobile and other nodes are in their home domain. Now, we discuss scenarios where at least one end node is visiting a foreign network.

Scenario R_1: This scenario specifies when one end node, which is in a foreign domain, is communicating with the other node which is in home domain, but two nodes are in different domains. It aims to analyze the effect of security services on data streams when one node is roaming.

Scenario R_2: This network scenario is very similar to R_1 with the only difference that the other end node is wireless but not using Mobile IP protocol. This scenario helps us in understanding the impact of security services on applications when one communication node is normal internet node with no extra services such as Mobile IP. Here, CN can belong to any network except the one where mobile node is currently roaming.

Scenario R_3: This scenario is similar to R_2 but with a wireless correspondent node. Here we capture the scenario when both ends nodes are wireless devices, so source and destination networks are wireless networks, but network in transit can either be wired or wireless. In our case, it is wired segment.

Scenario R_4: The last scenario occurs when both nodes are in the same domain but one node is roaming and so current network is foreign domain for one network whereas home domain for other network. It helps us in analyzing performance impact on data streams when roaming node is communicating with a non-roaming node in the same domain.

In summary, our paper evaluates security policies in different mobile scenarios by considering current location of the mobile node (MN) in the network. We investigate both ”no roaming” ($\mathcal{N}$) and ”with roaming” ($\mathcal{R}$) scenarios. ”with roaming” ($\mathcal{R}$) scenario refers to when one of the mobile nodes is visiting a foreign network whereas ”no roaming” ($\mathcal{N}$) scenario refers to when all mobile nodes stay in home network. Mobility scenarios take into account the presence of correspondent nodes (CN), which can either be wireless or wired devices.

V. Security Services and Associated Overhead

Security policies are designed to demonstrate the potential security services provided by each security protocol. Each protocol uses key management protocols, various authentication and encryption mechanisms to provide security. Therefore, several security policies are configured for experiments using different security services provided by each security protocol.

A. Security Configuration

For each security protocol, we conduct experiments exhaustively, consisting of security functions in combination with various encryption, decryption and authentication algorithms. These variations are described as follows:

- Encryption Algorithms $\mathcal{E} = \{E_1, E_2, \ldots, E_\beta, \ldots\}$, which represents encryption algorithms provided by several security protocols in the network.
- Authentication Algorithms $\mathcal{A} = \{A_1, A_2, \ldots, A_\alpha, \ldots\}$, which defines a set of authentication algorithms provided by several security protocols in the network.
- Key Management Protocols $\mathcal{K} = \{K_1, K_2, \ldots, K_\kappa, \ldots\}$. It represents a set of key management protocols provided by several security protocols in the network.
- Individual Security Policies $\mathcal{I} = \{I_1, I_2, \ldots, I_6\}$. $\mathcal{I}$ defines a set of individual security policies configured in the network for security protocols.
- Hybrid Security Policies $\mathcal{H} = \{H_1, H_2, \ldots, H_6\}$. $\mathcal{H}$ defines a set of hybrid security policies configured in the network. It defines security policies which belong to multiple security protocols, which is described in Subsection C.
- Security Policies $\mathcal{P} = \{P_0, P_1, \ldots, P_{11}\}$. $\mathcal{P}$ defines set of security policies configured in the network.

In the following subsections, we explain these security policies and their significance in detail.

B. Individual Security policies

When security policies involve security mechanisms, which belong to single security protocol, then they are called *Individual security policies*. ”No security” means that there is no security services enabled in the network. ”No Security” policy helps us in comparing the overhead associated with other security services in terms of end-to-end response time, throughput and protocol overhead. In the following paragraphs we discuss security policies for each security protocol.

- **WEP Policies:** WEP supports two key sizes for encryption which are 128 bit and 40 bit keys. We analyze WEP for both of these key sizes but here we only present experimental results for 128 bit key sizes because from our analysis point of view, both modes of WEP behave similarly with little difference in measurements.
- **IPSEC Policies:** IPSEC standard supports a large set of encryption and authentication algorithms providing strong security. Since we use Freeswan [17] for IPSEC functionality, our analysis is restricted to the security services provided by Freeswan open source implementation. Freeswan includes 3DES as an encryption mechanism and, MD5 and SHA as authentication algorithms. Since IPSEC tunnel mode is considered better by providing stronger security services than IPSEC transport mode, we analyze only IPSEC tunnel mode in our setup. And again, we provide experimental results only for IPSEC with 3DES and SHA algorithms used in the tunnel mode.
- **802.1x Policies:** In case of 802.1x, we use RADIUS as backend server maintaining users’ secret credentials. 802.1x uses EAP as its transport mechanism which involves MD5 and TLS modes. In TLS mode, EAP uses SSL

as security mechanisms. Since FreeRadius open source also supports MD5 and TLS, we analyze 802.1x with EAP in both TLS and MD5 modes separately.

C. Hybrid Security policies

When security policies involve security mechanisms, which belong to multiple security protocols at different network layers, then they are called *Hybrid security policies*. Such policies are required, if visiting clients have security support at more than one network layer. Therefore, the network can fulfill the needs of the large number of clients. Another reason may be that security functionalities required by the network can not be fulfilled by just one security protocol leading to the need for configuration of more than one security protocol in the network. Next, we describe details about hybrid security services.

Our study combines security services provided by WEP, IPSEC and 802.1x in different ways. Initially we focus on combination of IPSEC and WEP. We first analyze the overhead associated with IPSEC (3DES, MD5 and SHA) and WEP (40 or 128 bits), but here we present results for IPSEC (3DES, SHA) and WEP (128 bits). Then we perform experiments with 802.1x and WEP to capture combined effects of all security services at MAC layer and transport layer. Finally, we combine different security services of 802.1x, WEP and IPSEC together and analyze them. This combined study helps us in determining security services which contribute more towards overhead and whether it is useful to enable security services at different layer at the cost of adding more overhead. Table I provides a subset of security policies for each protocol alongwith security features associated with each security policy.

D. Overhead Associated with Security policies

Let P_0 denote the case that there is no security policy configured in the network and P_ϕ denote security policy when there is some security service configured in the network where $\phi = \{1, 2, \ldots, 11\}$. Let $T^s(k, P_\phi)$ denote the time required to process kth packet by a sender i with security policy P_ϕ. It may include adding extra header by security policy, encryption of packet and so on. Let $T^r(k, P_\phi)$ denote the time required to process kth packet by a receiver j with security policy P_ϕ. It can be the result of removing extra header of security policy, decryption of packet and so on. Let $T^t(k, P_\phi)$ denote the time taken by kth packet in traversing the network between the sender and the receiver using security policy P_ϕ.

Since total time involved in processing kth packet between the sender and the receiver during policy P_ϕ is the sum of three time periods defined above. Therefore total time of processing kth packet, which is denoted by $T(k, P_\phi)$, is given by

$$T(k, P_\phi) = T^s(k, P_\phi) + T^r(k, P_\phi) + T^t(k, P_\phi). \qquad (1)$$

Assume N packets are sent from the user i to user j, then the total time required for processing N packets between users during security policy P_ϕ is the sum of time involved in processing all N packets. Using (1), the total time for N packets can be obtained as follows:

$$\sum_{k=1}^{N}(T(k, P_\phi)) = \sum_{k=1}^{N}(T^s(k, P_\phi) + T^r(k, P_\phi) + T^t(k, P_\phi)). \qquad (2)$$

Assume that the size of kth packet is l_k bits, and then the total number of bits in N packets, denoted by B_n, is:

$$B_n = \sum_{k=1}^{N} l_k. \qquad (3)$$

Till now we have calculated total time required to process N packets and size of N packets. Let $BR(P_\phi)$ denote bit rate (bits/sec) that can be achieved during security policy P_ϕ. Using (2) and (3), bit rate for security policy P_ϕ can be obtained as:

$$BR(P_\phi) = \frac{B_n}{\sum_{k=1}^{N}(T^s(k, P_\phi) + T^r(k, P_\phi) + T^t(k, P_\phi)}. \qquad (4)$$

Let $BR(P_0)$ denotes the bit rate(bits/sec) achieved with security policy P_0. Therefore, using (4), we have bit rate for security policy P_0 as follows:

$$BR(P_0) = \frac{B_n}{\sum_{k=1}^{N}(T^s(k, P_0) + T^r(k, P_0) + T^t(k, P_0)}. \qquad (5)$$

Assume that $O(P_\phi)$ denotes the overhead associated with security policy P_ϕ, which is defined as the difference between bit rate for security policy (P_ϕ) and bit rate for (P_0). Therefore $O(P_\phi)$ can be calculated using (4) and (5) as follows:

$$\begin{aligned} O(P_\phi) = & \frac{B_n}{\sum_{k=1}^{N}(T^s(k, P_\phi) + T^r(k, P_\phi) + T^t(k, P_\phi))} \\ & - \frac{B_n}{\sum_{k=1}^{N}(T^s(k, P_0) + T^r(k, P_0) + T^t(k, P_0))}. \end{aligned} \qquad (6)$$

VI. Performance Metrics

We measure the performance impact of security policies on system's QoS with regard to the following metrics:

Authentication Time (AT**)** is defined as the time involved in an authentication phase of a security protocol. Here, we describe steps to calculate the authentication time (AT) as follows:

1) Assume that security policy P_ϕ is configured in the network. Now, through experiments we determine the time involved in processing k_{th} packet by P_ϕ during its authentication phase. Let, it be denoted as $t_k(P_\phi)$.

2) Assume N packets are exchanged during authentication phase. Let total time in processing N packets be represented by $TN(P_\phi$, which can be calculated as follows:

$$TN(P_\phi) = \sum_{k=1}^{N} t_k(P_\phi). \qquad (7)$$

3) Let AT denote authentication time. As it depends on mobility scenarios $\mathcal{N}$, $\mathcal{R}$ and security policies $\mathcal{P}$ as defined in sections IV

TABLE I

FEATURES OF SECURITY POLICIES.

Policy No.	Security Policies	Authen-tication	Confid-entiality	Data Integrity	Non Repudiation	Mutual Auth
P-0	No Security					
P-1	WEP-128 bit key	Y	Y			
P-2	IPSEC-3DES-SHA	Y	Y	Y	Y	Y
P-3	IPSEC-3DES-SHA-WEP-128	Y	Y	Y	Y	Y
P-4	8021x-EAP-MD5	Y		Y		
P-5	8021x-EAP-TLS	Y	Y		Y	Y
P-6	8021X-EAP-MD5-WEP-128	Y	Y	Y		
P-7	8021X-EAP-TLS-WEP-128	Y	Y		Y	Y
P-8	8021X-EAP-MD5-WEP-128-IPSEC-3DES-MD5	Y	Y	Y	Y	Y
P-9	8021X-EAP-TLS-WEP-128- IPSEC-3DES-MD5	Y	Y	Y	Y	Y
P-10	8021X-EAP-MD5-WEP-128-IPSEC-3DES-SHA	Y	Y	Y	Y	Y
P-11	8021X-EAP-TLS-WEP-128-IPSEC-3DES-SHA	Y	Y	Y	Y	Y

and V, therefore AT can be represented as $AT(\mathcal{N},\mathcal{R},\mathcal{P})$ and can be calculated using (7) as follows:

$$AT(\mathcal{N},\mathcal{R},\mathcal{P}) = \sum_{k=1}^{N} t_k(P_\phi). \tag{8}$$

Number of Authentication Messages (AM) is concerned about the messages exchanged during an authentication phase. Ethereal snapshots have been taken to obtain messages exchanged for different security protocols. This parameter is related to overhead signaling of authentication.

Policy Overhead (Bytes/Second) $O(P_\phi)$ refers to the overhead associated in encrypting and decrypting data as shown in **??**. Once data transfer phase is initiated after initial protocol negotiation, encryption and decryption is the only operation on data. So their cost affects total overhead of security policies. We assume in our experiments that security policies do not renegotiate security parameters during a session, thus eliminating the overhead introduced by renegotiation of security policies.

Traffic Streams(Tr) is considered with regards to TCP and UDP traffic streams in our experiments. Since most of the applications run over TCP or UDP, our experimental data is applicable to many applications in wireless LANs.

Response Time (End-to-End) ($\mathcal{RS}$) is a measure of the delay in transmission of data between a sender and a receiver.

Throughput (Bytes/Second) (Th) is a measure of the data transfer during per unit time between participating nodes. The throughput is obtained according to following steps:

- Determine time $t_f(P_\phi)$ when first data packet is sent from a sender to a receiver with security policy P_ϕ.
- Determine time $t_l(P_\phi)$ when last data packet is delivered to a receiver j from a sender i with security policy P_ϕ.
- Calculate total time, denoted as tt, by subtracting $t_f(P_\phi)$ from $t_l(P_\phi)$ which can be given as follows:

$$tt = t_l(P_\phi) - t_f(P_\phi). \tag{9}$$

- Assume that total data exchanged between users i and j are denoted as D in bytes. Since data rate, denoted as dt, is defined as data sent per unit time, therefore dt can be represented using (9) as follows

$$dt = \frac{D}{t_l(P_\phi) - t_f(P_\phi)}. \tag{10}$$

- Since throughput Th depends on factors such as $\mathcal{N}$,$\mathcal{R}$, $\mathcal{P}$, Tr and DS, where Tr represents traffic types such as TCP or UDP, DS denotes total data sent between a sender i and receiver j and other denotations are the same as defined in Sections IV and V. Therefore, throughput can be represented as $Th(\mathcal{N},\mathcal{R},\mathcal{P},Tr,DS)$, which can be obtained by using (10) as follows:

$$Th(\mathcal{N},\mathcal{R},\mathcal{P},Tr,DS) = \frac{D}{t_l(P_\phi) - t_f(P_\phi)}. \tag{11}$$

VII. Data Acquisition

For each security service configured in the network, experimental data are collected in two phases. The first phase collects measurements from initial negotiation of protocols. The second phase focuses on generating different traffics and then collecting values for different parameters such as throughput, and response time for different security policies.

In the *First phase*, we concentrate on taking data that is related to initial negotiations, which take place during handshake stage of any protocol. We use Ethereal network packet analyzer to capture the packets exchanged during handshake. Using timestamp option provided in every packet's information, we record the time difference between the first and last packet of negotiation phase. Since in our analysis, we name initial negotiation phase as authentication phase, data obtained in this manner will be used to investigate and compare authentication time for different security services.

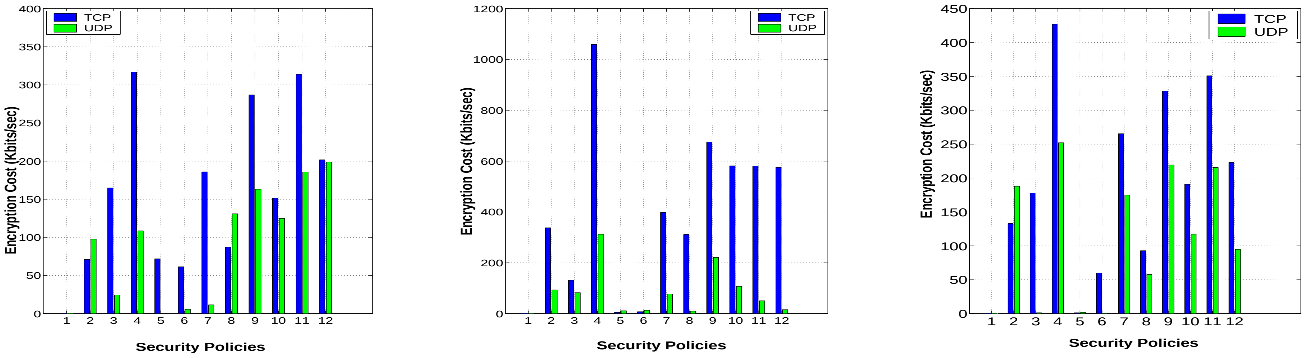
The *Second phase* in our study includes generating different traffic streams in the network between two participating nodes. We use ”ttcp” and ”Iperf” traffic generators, because they can generate TCP and UDP traffic. Moreover, these utilities provide different types of statistics such as end-to-end delay, throughput, packet loss and so on. Also, we can verify whether measurements provided by one tool are in consistent with experimental data provided by other tools.

Initially, we generate TCP and UDP streams with different data sizes. But after analyzing experimental data obtained, we

TABLE II

AUTHENTICATION DELAY

Policy	IPSEC(sec)	802.1x-EAP(MD5) without IPSEC(sec)	802.1x-EAP(MD5) with IPSEC(sec)	802.1x-EAP(TLS) without IPSEC(sec)	802.1x-EAP(TLS) with IPSEC(sec)
Non-Roaming	1.405	0.427	1.722	1.822	3.117
Roaming	1.432	1.749	1.749	3.144	3.144



(a) N1 - TCP/UDP Encryption Cost.

(b) N2 - TCP/UDP Encryption Cost.

(c) N3 - TCP/UDP Encryption Cost.

observed that, for smaller size data files, differences in measurements for different security services are not visible, so they are of no help in analysis. Then, we focus our measurement on larger data size such as 16MB from which we can observe significant difference in measurements for different security services. The data obtained in this manner, we use to investigate and compare network parameters such as end-to-end delay, network throughput, protocol overhead etc for different security services configured in the testbed. Moreover, we repeat experiments several times to obtain accurate measurements, and then, we calculate average value of these measurements.

VIII. Experimental Results

In this section, we discuss experimental results obtained for afore-mentioned security policies in various mobility scenarios. We provide experimental data for authentication delay, authentication messages, policy overhead and throughput.

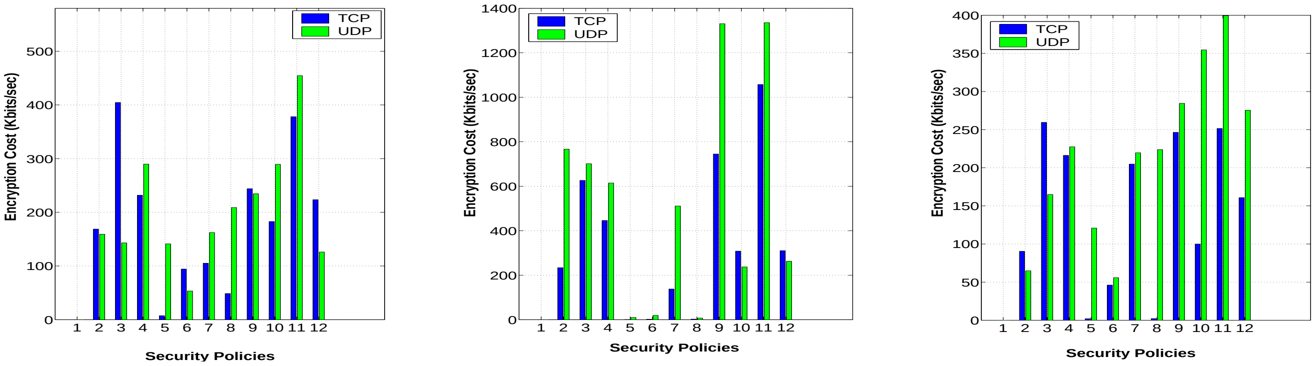
A. Authentication Time (AT)

TABLE II shows authentication time (AT in sec) for IPSEC and 802.1x policies. Since WEP does not involve exchange of control messages, there is no authentication time involved. Authentication time AT for IPSEC and 802.1x involves Mobile IP authentication time also. We observe that when an MN is not roaming, IPSEC authentication takes longer time than 802.1x with EAP-MD5. However, when an MN roams, the 802.1x authentication time is longer. This is because when an MN roams, the MN reauthenticates with an FA using 802.1x. This is not the case with IPSEC, because the IPSEC tunnel has already been established between the MN and the HA. We also observe that 802.1x with IPSEC policies causes longer authentication delay than 802.1x without IPSEC policies. TABLE II also shows that 802.1x-EAP-TLS authentication time is longer than 802.1x-EAP-MD5 which is due to the fact that 802.1x-EAP-TLS uses digital certificate for mutual authentication which involves exchange of several control packets.

B. Authentication Messages (AM)

The number of authentication messages (AM) has been measured because it helps us in determining why authentication time for a particular security policy is higher than others. Since, according to our definition, authentication time for various security protocols includes Mobile IP authentication phase too, the total number of authentication messages for a particular security protocol is the sum of authentication messages for both protocols, i.e. security protocol and Mobile IP.

We notice that Mobile IP involves 4 messages when an MN registers with an HA, and the same number of messages are exchanged when an MN roams to foreign network and registers with an FA. For IPSEC alone, we observe that 9 control messages are exchanged during authentication phase. Therefore, IPSEC involves 13 control messages in non-roaming scenarios ($\mathcal{N}$) and 17 in roaming scenarios ($\mathcal{R}$). Further, 802.1x-EAP (MD5) involves 8 control messages during authentication, therefore 802.1x-EAP (MD5) involves 12 control messages in non-roaming scenarios ($\mathcal{N}$). But in roaming scenarios ($\mathcal{R}$) , 802.1x-EAP (MD5) involves 24 control messages because when an MN roams to another network, it reauthenticates with the FA using 802.1x. In addition, we observe that 802.1x-EAP (TLS) involves 21 control messages. With the similar explanation as for 802.1x-EAP (MD5), we observe that 802.1x-EAP (TLS) exchanges 25 messages during non-roaming scenarios ($\mathcal{N}$) and 42 messages during roaming scenarios ($\mathcal{R}$). TABLE III shows number of authentication messages for different security protocols in non-roaming and roaming scenarios.



(d) N4 - TCP/UDP Encryption Cost.

(e) N5 - TCP/UDP Encryption Cost.

(f) R1 - TCP/UDP Encryption Cost.

TABLE III
AUTHENTICATION MESSAGES

Security Policies (Ratio)	$(\mathcal{N})$	$(\mathcal{R})$
IPSEC	13	17
802.1x-EAP(MD5)	12	24
802.1x-EAP(TLS)	21	42

C. Policy Overhead ($O(P_\phi)$)

Here we use policy overhead and encryption overhead terms interchangeably. Figs. from 2(a) to 2(i) demonstrate encryption cost for TCP and UDP in different mobility scenarios. We observe that IPSEC causes more encryption overhead than WEP and 802.1x in most of the scenarios, because IPSEC uses 3DES encryption mechanism, which is computationally slow. We also observe that 802.1x and WEP encryption costs are almost the same; this is because 802.1x uses WEP as its encryption mechanism leading to the same overhead. Further, we discuss encryption overhead for each scenario separately. First, we discuss non-roaming scenarios (N) and then, roaming scenarios (R).

C.1 Scenarios without Roaming

Encryption costs for TCP and UDP streams in N1, N2 and N3 are shown in Figs. 2(a), 2(b) and 2(c) respectively. We observe that encryption overhead for TCP is higher than that of UDP for most of the policies in these scenarios. This can be attributed to the fact that 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 scenarios N1 and N2, we observe that TCP encryption cost for N2 is more affected than TCP encryption cost for N1. But for UDP, encryption overhead for N2 is less affected than that of N1. In addition, Scenario N3 behaves very similar to N1, because other end points, as mobile node in N1 and correspondent node in N3, are wireless nodes and the end points are in the same domain.

Figs. 2(d) and 2(e) show encryption costs in N4 and N5 respectively. We observe that in both scenarios, UDP encryption cost is higher than TCP encryption cost. This can be attributed to the fact that some part of the network between two ends points is wired segment in N4 and N5 unlike in N1, N2 and N3, leading to network of different nature causing higher data loss for UDP and thereby increasing overhead.

C.2 Scenarios with Roaming

Figs. 2(f), 2(g), 2(h) and 2(i) show encryption costs in scenarios with roaming. We observe that UDP encryption cost in R1, R2 and R3 is higher than TCP encryption cost. But in R4, TCP encryption cost is higher which explains that not only mobility($\mathcal{M}$) but location of end points also effects encryption overhead. Difference in behavior in R4 can be attributed to the fact that, in R4, both end points are in same domain whereas in other mobility scenarios, end points are in different domains.

D. Throughput (Th) and Response Time (RS)

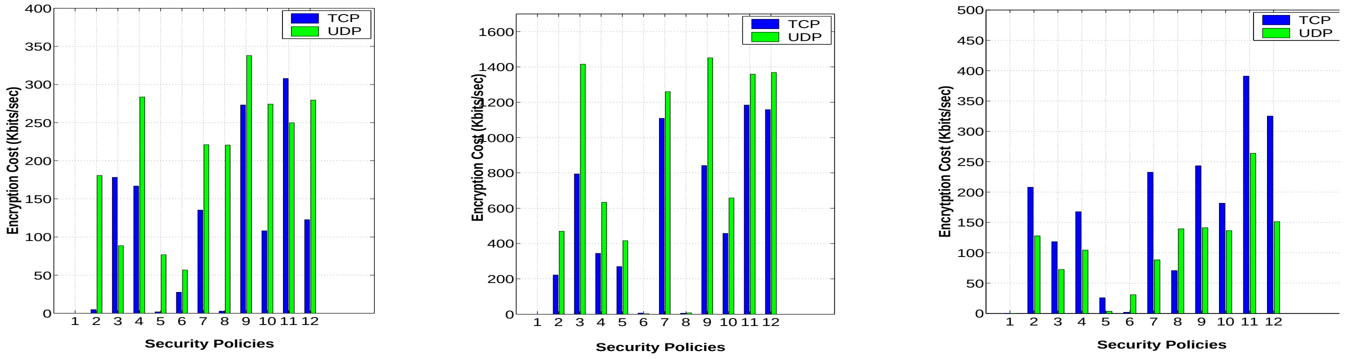
Figs. 2 and 3 show throughput variations (Th,(RS)) for TCP and UDP traffics for a subset of security policies in all network scenarios. Because of space limitation, we present only one security policy for each security protocol. We observe that IPSEC security policies cause greater decrease in throughput than WEP and 802.1x security policies. This is because IPSEC uses 3DES encryption algorithm, which is computationally slower than the encryption algorithm in WEP and 802.1x policies considered. But IPSEC provides stronger security services which compensates for the higher encryption overhead.

IX. Performance Analysis

We analyze different aspects of experimental results obtained in this section. In particular, the section focuses on finding out best security policy for a particular mobility scenario. We also discuss comparative studies for authentication delay, security service ratio and policy overhead. Moreover, we provide reasonings to explain the cause of difference in measurements.

A. Comparative study of Authentication Delay

TABLE IV demonstrates comparative study for IPSEC and 802.1x policies. We observe that IPSEC authentication takes approximately 3.29 times longer than 802.1x-EAP-MD5 in non-roaming ($\mathcal{N}$) scenarios; however it is about 82% less time than 802.1x-EAP-MD5 in roaming scenarios ($\mathcal{R}$). This is because



(g) R2 - TCP/UDP Encryption Cost.

(h) R3 - TCP/UDP Encryption Cost.

(i) R4 - TCP/UDP Encryption Cost.

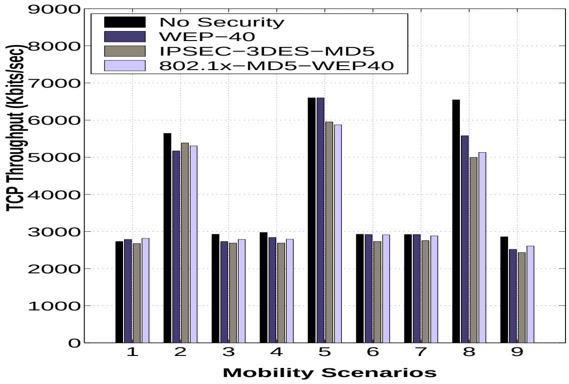


Fig. 2. TCP Throughput.

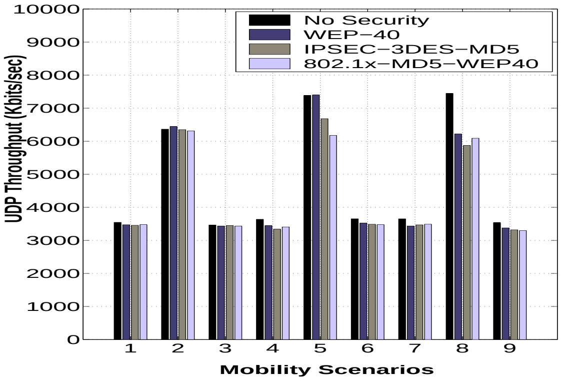


Fig. 3. UDP Throughput.

802.1x involves reauthentication during roaming scenarios ($\mathcal{R}$) leading to more authentication overhead. But IPSEC introduces less overhead when compared with 802.1x with EAP-TLS as shown in TABLE IV. Also, 802.1x (EAP-TLS w/o IPSEC) is 4.27 times expensive than 802.1x (EAP-MD5 w/o IPSEC) during non-roaming scenarios ($\mathcal{N}$). Overall, we observe that 802.1x with EAP-TLS causes longest authentication delay, and authentication delay of 802.1X with EAP-MD5 is the smallest.

Based on these observations, we can suggest that while transferring small size, non-critical data, 802.1x with EAP-MD5 authentication provides a better service. Since 802.1x-EAP-TLS causes longest authentication delay, it might lead to higher loss of data packets during handoff. For applications, which require stringent QoS requirements, it may not be a better choice. But applications which can tolerate some degradation in QoS requirements can use it for authentication.

TABLE IV
COMPARATIVE STUDY - AUTHENTICATION DELAY.

Security Policies (Ratio)	($\mathcal{N}$)	($\mathcal{R}$)
IPSEC(sec) / 802.1x-EAP(MD5)	3.29	0.82
IPSEC(sec) / 802.1x-EAP(TLS)	0.77	0.46
802.1x-EAP(TLS / MD5) w/o IPSEC	4.27	1.80
802.1x-EAP(TLS / MD5) with IPSEC	1.81	1.80

B. Security Policy vs. Mobility

We can infer from Figs. 2(a), 2(b) and 2(c) the following facts about scenarios N1, N2 and N3. Since a MN will communicate with a HA only during initial setup, we suggest, for less authentication delay during initial handshake, UDP data stream can be used by applications, and after that applications can switch to TCP for reliable communications with the cost of higher encryption overhead. Moreover, If HA is functioning as an application server, then applications running over UDP will suffer less performance degradation whereas application running over TCP will suffer higher performance degradation. In addition, if we compare P-2 security policy with other policies for both TCP and UDP, we observe that its encryption cost is the lowest from other policies except policies P-4 and P-5; but P-4 and P-5 do not use any encryption mechanisms leading to less secure environment. Therefore, for application running over TCP or UDP, policy P-2 may be a better choice for providing security services over the mobile wireless networks.

From Figs. 2(d) and 2(e), it can be suggested for N4 and N5, that applications running over UDP in these scenarios may suffer higher quality of service (QoS) degradation than application running over TCP. Moreover, Figs. 2(d) and 2(e) demonstrate that encryption cost for UDP during P-11 is the minimum as compared to other policies. Since P-11 provides stronger security services than other policies, it may be better choice for UDP applications. In addition, P-11 may be suggested choice for TCP applications too, because it provides a better balance between security services and encryption overhead.

We observe from Fig. 2(f) that P-2 for UDP traffic provides less encryption overhead than other policies except P-1, P-4 and P-5. But policies P-1, P-4 and P-5 do not provide strong security services, therefore P-2 may be recommended choice for applications running over UDP in scenario R1. But P-9 provides better tradeoff between security services and encryption overhead for TCP. We observe the same behavior for scenario R2 as for R1. Further, Fig. 2(h) demonstrates that P-9 provides less encryption overhead than most of the other policies for both UDP and TCP streams during R3. But we find that P-2 is better choice for providing security services during R4.

C. Throughput and Response Time

Figs. 2 and 3 depict that variations in throughput for most security policies is higher in case when mobile node is roaming than when mobile node is not roaming. It explains that node mobility causes higher variations in throughput. Figures also depict that variations in TCP and UDP throughputs are higher for mobility scenarios N5 and R3. It is due to the fact that one end point in N5 and R3 scenarios is wired, which is different in characteristics than the other end point which is wireless, leading to higher variations in these cases.

Further, we can also deduce that network with IPSEC policies will exhibit higher QoS degradation for applications. Devices with restricted system resources such as battery power, memory may suffer higher impact on system performance with IPSEC. It may be recommended that if data is not very critical than other security policies can be implemented in the network but for data, which require high security level, should be used with IPSEC security policies at the cost of some extra overhead.

D. Comparison

Here, we compare security services for non-roaming and roaming scenarios. We observe that, in general, encryption cost for TCP is affected more than that of UDP in ($\mathcal{N}$) scenarios. Whereas, in ($\mathcal{R}$) scenario, UDP encryption cost is impacted more than TCP encryption cost. It demonstrates that UDP stream is affected more due to mobility than TCP stream. This can be attributed to the fact that UDP being unreliable leads to more packet loss when an MN is roaming, thereby reducing system throughput and increasing overall overhead. Experimental results also show that most TCP and UDP encryption overhead is affected more in ($\mathcal{N}$) scenarios than that of ($\mathcal{R}$) scenarios. We also observe that P-2 and P-11 are recommended choices for ($\mathcal{N}$) scenarios, whereas P-2 and P-9 are recommended choices for ($\mathcal{R}$) scenarios. Almost in all scenarios, we observe that P-4 and P-5 policies cause least overhead, but these policies do not provide confidentiality so are not very valuable. But if some situation requires only strong authentication, P-5 policy is recommended choice since it provides strong authentication.

X. Conclusions

In this paper, we presented comprehensive experimental results and analysis, investigating the impact of security policies on system performance in various mobility scenarios. We provided quantitative measurements to demonstrate how bandwidth utilization and delay are affected by individual and hybrid policies and which policies may be recommended in a particular scenario.

Results demonstrated that WEP policies cause least overhead, and IPSEC policies cause significant overhead but provide stronger security. 802.1x-EAP-MD5 causes lesser overhead than 802.1x-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. Node mobility also affects overhead based on the location of end points and traffic streams being transmitted. We observe that variations in UDP throughput due to mobility are higher than TCP throughput. To our knowledge, there is no published literature with such a comprehensive experimental analysis. Therefore, our experimental measurements provide first-hand valuable results, which would be very useful to the design of network protocols for secure and flexible quality of service in future mobile networks.

References

[1] T. Karygiannis and L. Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices," *National Institute of Technology, Special Publication*, pp. 800–848, November 2002.

[2] Y. Zahur and T. A. Yang, "Wireless LAN Security and Laboratory Designs," *Journal of Computing Sciences in Colleges*, vol. 19, pp. 44–60, January 2004.

[3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications:The Insecurity of 802.11," *Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking*, July 2001.

[4] D. B. Faria and D. R. Cheriton, "DoS and Authentication in Wireless Public Access Networks," pp. 47–56, September 2002.

[5] W. A. Arbaugh, N. Shankar, J. Wang, and K. Zhang, "Your 802.11 network has no clothes," *IEEE Wireless Communications Magazine*, December 2002.

[6] K. Wang and S. Tripathi, "Mobile-End Transport Protocol: An Alternative to TCP/IP Over Wireless Links," in *IEEE INFOCOM*, pp. 1046–1053, April 1998.

[7] "IEEE Std 802.1x-2001x: Port-Based Network Access Control," *http://www.ieee802.org/1/pages/802.1x.html*, June 2001.

[8] "IEEE 802 Standards," *http://standards.ieee.org/getieee802*.

[9] IETF, "PPP EAP TLS Authentication Protocol," *RFC 2716*, October 1999.

[10] M. D. Corner and B. D. Noble, "Zero-Interaction Authentication," in *IEEE/ACM MOBICOM*, pp. 1–11, September 2002.

[11] S. Kasera, S. Mizikovsky, G. S. Sundaram, and T. Y. Woo, "On Securely Enabling Intermediary-Based Services and Performance Enhancements for Wireless Mobile Users," pp. 61–68, September 2003.

[12] J. Kong, S. Das, E. Tsai, and M. Gerla, "ESCORT: A Decentralized and Localized Access Control System for Mobile Wireless Access to Secured Domains," pp. 61–68, September 2003.

[13] Y. Matsunaga, A. Merino, T. Suzuki, and R. H. Katz, "Secure Authentication System for Public WLAN Roaming," pp. 113–121, 2003.

[14] O. Elkeelany, M. M. Matalgah, K. Sheikh, M. Thaker, G. Chaudhary, D. Medhi, and J. Qaddour, "Perfomance Analysis Of IPSEC Protocol: Encryption and Authentication," in *IEEE Communication Conference (ICC)*, pp. 1164–1168, May 2002.

[15] W. Qu and S. Srinivas, "IPSEC-Based Secure Wireless Virtual Private Networks," in *IEEE MILCOM*, pp. 1107–1112, OCT 2002.

[16] A. Godber and P. Dasgupta, "Secure Wireless Gateway," pp. 41–46, September 2002.

[17] "IPSEC," *http://www.freeswan.org*.

[18] "802.1x Supplicant," *http://www.open1x.org*.

[19] "RADIUS," *http://www.freeradius.org*.

[20] "*OpenSSL*," *http://www.openssl.org*.

[21] "Mobile IPv4," *http://dynamics.sourceforge.net*.