Evaluation of Security Architecture for Wireless Local Area Networks by Indexed Based Policy Method: A Novel Approach

Debabrata Nayak[1], Deepak B. Phatak[1], and Ashutosh Saxena[2]

(Corresponding author: Debabrata Nayak)

IIT Mumbai, Kanwal Rekhi school of Information technology[1]
IIT Bombay, Powai 400076, India (Email: {Debu,dbp}@it.iitb.ac.in)
Institute for Development and Research in Banking Technology, Reserve Bank of India, Hyderabad[2]

(Received Jan. 30, 2006; revised and accepted May 7, 2006)

Abstract

In this paper, we have focus existing and proposed WLAN security technologies designed to improve 802.11 standard by applying security policies. We have extensively analyzed the effect of crypto parameters over WLAN based on packet level characteristics by applying security policy to individual packet. We have also analyzed the effect of TCP and UDP traffic over our proposed WLAN test bed architecture. We found that TCP and UDP traffic behaves erratically, when policy index changes causing drastically degradation of system performance. We present a detail study of performance overhead caused by the most widely used security protocols such as WEP, IPSEC VPN and 802.1X. Furthermore, we analyze the effectiveness of such solution, based on measurement of policy indexing model implementation. Performance measurement indicates that 802.1X and VPN policy based method can be used based on the service time in future wireless systems, while it can simultaneously provide both the necessary flexibility to network operators and a high level of confidence to end users. We have coined security policy factor (SPF), which is defined as the percentage overhead in terms of bit rate caused by security policy $P\varphi$ with respect to security policy P0. Based on SPF designer can decide there best optimized Secure WLAN infrastructure.

Keywords: 802.1X, EAP, security policy factor, security policy index, SQoS, WPA, WVPN, WVLAN

1 Introduction

A good security policy will give the network administrator a security model for managing the network. It will define limitations for acceptable network operation and performance. These limitations will vary from network to network and so will the resulting security policies. The security model provides a baseline for security policy and must be dynamic to change as technology and security needs change. The security policy will include policy for all aspects of managing a network including the site and infrastructure of the network, administrative issues and the user [37, 38].

The most secure network can become vulnerable if the users are not aware of security policies. It is important to have a method of communicating and enforcing security policies. Without enforcement, even the best-intentioned employee becomes lax in performing his daily tasks in a secure manner. For example, the worker that introduces an improperly secured wireless access point into the business network may not realize the security risk he has introduced to the network [12].

Firewall hardware and software can be configured to allow safe Internet traffic to enter a network and block unsafe Internet traffic. It uses a series of rules to intercept and analyze data to determine whether the traffic is safe to enter either wired or wireless networks. The purpose of a firewall in a notebook using a wireless network is to prevent unsafe traffic from entering not only the notebook but also the network through the notebook. If there is a small group of users, the network can be limited to assigning a certain number of DHCP addresses equal to the number of possible users. If everyone is on the network and someone cannot log on, then there is an unauthorized logon. RADIUS is a protocol for authentication, authorization and accounting of remote access connections. The user inputs his name and password and submits it to the RADIUS server. The RADIUS server determines if the user is authorized to use the network. It can be set up to provide different access levels to the network. Communication between the user and the RADIUS server is encrypted; however, the RADIUS protocol does not provide data encryption. RADIUS is often used with a VPN.

The VPN provides a virtual "tunnel" to allow the user to access the corporate network through a public network like the Internet. It does this by authenticating, encrypting and encapsulating data. There are many different ways to set up a VPN, some of which are very costly. To provide a secure environment, the administrator must know how to properly set up the VPN. When the VPN is set up properly, it is generally considered one of the most secure ways to transfer data across the wireless network or the Internet. The VPN usually causes a loss of performance in the network; however, it should improve as hardware acceleration engines for algorithm encryption is built into processors [31]. All unauthorized access points must be banned to secure a network. An unauthorized access point that is added to the network is not likely to be configured in such a manner to be secure.

This security policy must be communicated to users. The network administrator can scan for rogue access points by using free software such as Netstumbler to locate unauthorized access points [13].

2 802.1X Model

There were ten Security Policy Indexes selected to present a hierarchical order of the security mechanisms available from both 802.11 and 802.1X standards.

The ten Security Policy Indexes of this model are:

- Policy Index 1 No security: This is the default security setting provided by vendors. There is no security mechanism activated with default configuration.

- Policy Index 2 MAC address authentication: This Index provides MAC address authentication carried out at the AP.

- Policy Index 3 WEP authentication: The shared key authentication method specified in the 802.11 standard is used.

- Policy Index 4 WEP authentication with 40-bit WEP encryption: This Index combines the encryption algorithm to provide data privacy.

- Policy Index 5 WEP authentication with 128-bit WEP encryption: The 128-bit shared key used is proprietary-based.

- Policy Index 6 EAP-MD5 authentication: This is one of the 802.1X standard's authentication methods, using password or username.

- Policy Index 7 EAP-TLS authentication: This is the PKI-based authentication method supported by 802.1X.

- Policy Index 8 EAP-MD5 with 128-bit WEP encryption: The combined effect of these tools provides strong data protection.

- Policy Index 9 EAP-TLS with 128-bit WEP encryption: The combined effect of these tools provides the strongest Index of encryption and authentication using per-session keys.

- Policy Index 10 EAP-TTLS with 128-bit WEP encryption: The combined effect of these tools provides the strongest Index of encryption and authentication using dynamic per-session keys.

The Security Policy Indexes 2 to 5 of the 802.1X model are consistent with the 802.11 standard. Security Policy Indexes 6 to 10 are provided by the 802.1X standard.

3 VPN Model

There are two types of authentication methods deployed in our experiments: Device authentication method using PKI with X.509 certificates User authentication methods selected based on open-standards - CHAP and EAP-TLS. These two methods provide direct comparison with the authentication methods deployed in the 802.1X model. PPTP has been selected to provide a performance comparison with tunnelling techniques. Rinc?n [2002] observed in his research that L2TP/IPSec tunnelling produced greater performance overheads than PPTP. Ten Security Policy Indexes were specified:

- Policy Index 1 No security: This is the default security setting. Both the 802.lX and VPN models have this in common.

- Policy Index 2 PPTP tunnelling with CHAP: Authenticated tunnel provided using PPTP tunnelling and CHAP authentication.

- Policy Index 3 IPSec tunnelling with CHAP: Authenticated tunnel using IPSec tunnel and CHAP authentication.

- Policy Index 4 Firewall with PPTP and CHAP: Introducing a firewall into the architecture to filter the network traffic.

- Policy Index 5 Firewall with IPSec and CHAP: A firewall is introduced into an IPSec based network. From this index onward, all the security Indexes will be based on IPSec design.

- Policy Index 6 Firewall with IPSec and EAP-TLS: Applying user-based PKI with device based certificate authentication.

- Policy Index 7 IPSec with CHAP and DES: Provides DES encryption to IPSec with CHAP user authentication.

- Policy Index 8 IPSec with EAP-TLS and DES: Applies DES encryption to EAP-TLS user authentication.

- Policy Index 9 IPSec with CHAP and 3DES: Provides strongest encryption (3DES) with CHAP.
- Policy Index 10 IPSec with EAP-TLS and 3DES: Encrypts data traffic with the strongest encryption and user authentication methods.

The VPN model can be grouped into two parts; Security Policy Indexes 2 to 4 require authentication and tunnelling using either PPTP or L2TP/IPSec before and after the firewall. Security Policy Indexes 5 to 10 requires the IPSec protocol suite with a firewall to carry out authentication and encryption.

4 Security Policy Configuration

4.1 Policy Definition

Policies are rules with possible actions that work on an if-then structure and can prohibit, permit, or require actions for both people and hardware and software on the network. A policy sets the threshold for an alarm, and another sets the policy for the resulting action by the network manager (GARTNER). But our definition of Security Policy is people can define high level of policy with security requirement, which can be further transformed to low level security parameters with improved performance.

4.1.1 Security Variables

- Strength of cryptographic algorithm RSA, DES, AES measured in terms of the work factor associated with a brute force attack.
- Length of cryptographic key.
- Characterize by bit-length. Percentage of packet authenticated.
- Characterize by percentage of data modification or less confidence of policy enforcement in remote login environment. Characterize by third party evaluation, robustness of authentication mechanism [43].
- Weak password, strong password, biometric, smart card.

4.1.2 Policy Configuration

Here we analyze through experimental analysis of security protocols at different network layers in real time environment. By configuring different security policies and finding their impact on different system parameters i.e. authentication delay & throughput has been considered [39].

Here we have considered specific security policies M_U:

- $\{M_{u1}, M_{u2}, \cdots, M_{un}\}$ are the users in the network;
- N_R-$\{N_{R1}, N_{R2}, \cdots, N_{Rn}\}$ Non-roaming scenario;
- S-$\{S_1, S_2, \cdots, S_n\}$ representing the subnet in the network;
- V-$\{V_1, V_2, \cdots, V_n\}$ representing various VLANs in the network;
- P-$\{P_0, P_1, \cdots, P_n\}$ Policy Index configured in the network;
- T_R : Response Time;
- SQoS: $\{T_{Auth}, Th_{time}, T_R, P_{index}\}$; SQoS: Secure quality of service associated with the network. For each security protocol, we have extensively found out enabling variances, authentication and encryption mechanisms and their impact on response time.
- $E_{k(1,2)} = \{E_{k1}, E_{k2}, E_{k3}, \cdots, E_{kn}\}$;
- $K_e = K_d = K - Scenario - 1$ or $K_e \neq K_d - Scenario - 2$;
- Set of encryption provided by various protocol: $Auth = \{A_1, A_2, \cdots, A_n\}$;
- Set of authentication algorithm provided by the protocols: $K = \{K_1, K_2, \cdots, K_n\}$;
- Set of key management schemes provided by the protocol: $P = \{P_0, P_1, \cdots, P_n\}$ are the set of policy index configured for various protocol in the network.
- E_n: Encryption algorithm configured in the network;
- A_n: Authentication algorithm configured in the network;
- K_n: Key management protocol configured in the network;
- P_n: Policy index configured in the network; $P_n = \{E_n, A_n, K_n\}$.

4.1.3 Associated Overhead with Security Policy

By statically configuring various security policies, we found that various security protocols offer various security parameters, which has considerable impact on system performance.

Therefore, we have configured different security policies for experiencing using different traffic types using different protocols:

- P_0 indicates the policy index with no security policy, i.e. the overhead caused due to this is negligible.
- P_n represents security policy when various encryption and authentication and key management protocols are in operation.
- $T_s(K, P_n)$ denotes the time required to process the K^{th} packet by a sender 'i' with security policy P_n.
- $T_r(K, P_n)$ denotes the time required to process K^{th} packet by a receiver 'j' with security policy P_n.

- $T_n(K, P_n)$ denotes the time involved in processing K^th packet traversing between various VLANs between the sender and receiver using security policy P_n.

So $T_t(K, P_n) = T_s(K, P_n) + T_r(K, P_n) + T_n(K, P_n)$, where T_t represents the total time i.e end to end time.

The above equation represents the time taken for processing K^{th} packet between the sender and receiver with security policy P_n. Assume that '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_n' is the sum of time involved in processing all 'N' packets. So the total time for 'N' packets:

- $\sum_{K=1}^{N} T_t(K, P_n) = \sum_{K=1}^{N} T_s(K, P_n) + T_r(K, P_n) + T_n(K, P_n)$;
- Assume that the size of K^{th} packet is l_k bits, and the total number of bits for N packets, denoted by B_n, is $B_n = \sum_{K=1}^{N} l_k$;
- Let BR (P_n) - bit rate (bits / sec.) that can be achieved during security policy P_n. So BR (P_n) = $\frac{B_n}{\sum_{K=1}^{N}(T_t(K,P_n))}$; BR ($P_n$) = $\frac{\sum_{K=1}^{N} l_k}{\sum_{K=1}^{N} T_s(K,P_n)+T_r(K,P_n)+T_n(K,P_n)}$;
- Let $B_r(P_0)$ denotes the bit rate (bits/sec.) achieved with security policy P_0. So BR(P_0) = $\frac{B_n}{\sum_{K=1}^{N}(T_t(K,P_0))} = \frac{B_n}{\sum_{K=1}^{N} T_s(K,P_n)+T_r(K,P_n)+T_n(K,P_n)}$. % of overhead associated with security Policy P_n is=$\frac{BR(P_n)-BR(P_0)}{BR(P_0)}$.

The percentage of overhead signified that the impact of optimized security policy over the network with respect to, the standard security policy configured in the network.

So policy overhead can be defined as the overhead associated with a security policy during data transfer between sender and receiver [41].

- Network Scenario-1. Non Roaming (N) 2. Roaming (R).
- M_U-$\{M_{u1}, M_{u2}, \cdots, M_{un}\}$ are the users in the network.
- N_R-$\{N_{R1}, N_{R2}, \cdots, N_{Rn}\}$ Non-roaming scenario;
- R=$\{R_1, R_2, \cdots, R_n\}$ set of roaming scenario in the network when at least one user is in the foreign domain.
- SQoS=$\{AT_u, Th_u, T_R, P_u\}$;
- User Mobility profile $\{M_u, C_u, Qu(t)\}$;
- $U_i \in U$=User is within network;
- $H_{ui} \in S$=Home domain far user 'i';
- $H_{uj} \in S$=Home domain far user 'j';
- $C_{ui(t)} \in S$=Current domain of user 'i' at time 't';
- $C_{uj(t)} \in S$=Current domain of user 'j' at time 't';
- $Q_{ui(t)}$=SQoS profile fore u_i at time 't';
- $Q_{uj(t)}$=SQoS profile for u_j at time 't';
- $M_{ui(t)}$=Mobility status of u_i at time 't';
- $M_{uj(t)}$=Mobility status of u_j at time 't'.

4.2 Algorithm for Mobility Tracing

```
$M_{ui(t)} = \{H_{ui}, C_{ui(t)}, Q_{ui(t)}\}$
$M_{uj(t)} = \{H_{uj}, C_{uj(t)}, Q_{uj(t)}\}$
If $H_{ui} = C_{ui(t)} \bigwedge H_{uj} = C_{uj(t)}$
        Then $\{M_{ui(t)}, M_{uj(t)}\} \in N$
Else if $H_{ui(t)}! = C_{ui(t)} \bigvee H_{uj(t)}! = C_{uj(t)}$
        Then $\{M_{ui(t)}, M_{uj(t)}\} \in R$
End if.
```

User in Transition – Individual security policies:

- P=$\{P_1, P_2, \cdots, P_n\}$ where P - defines set of security policies configured in the network for security protocol.
- I=$\{I_1, I_2, \cdots, I_n\}$ where I - defines set of Individual security policies configured in the network for security protocol.
- H=$\{H_1, H_2, \cdots, H_n\}$ H - defines set of Hybrid Security policies configured in the network. It defines security policies are distributed across various protocols.

4.3 Algorithm for Security Policy

- $E\beta\epsilon E := \beta_{th}$ - Encryption algorithm configured in the network;
- $A\alpha\varepsilon A := \alpha_{th}$ - Authentication algorithm configured in the network;
- $K\kappa\varepsilon K := \kappa_{th}$ - Key Management Protocol configured in the network;
- $P\varphi := \varphi_{th}$ - Security Policy Configured in the network, where $P\varphi\varepsilon\{E\beta, A\alpha, K\kappa\}$.

if $E\beta, A\alpha, K\kappa\varepsilon$ Single Security Protocol then $P\varphi\varepsilon I$
else if $E\beta, A\alpha, K\kappa/\varepsilon$ Single Security Protocol then $P\varphi\varepsilon H$
end if.
{User has not compiled to any security policy}.

4.4 Selection of Security Policy

1) 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:

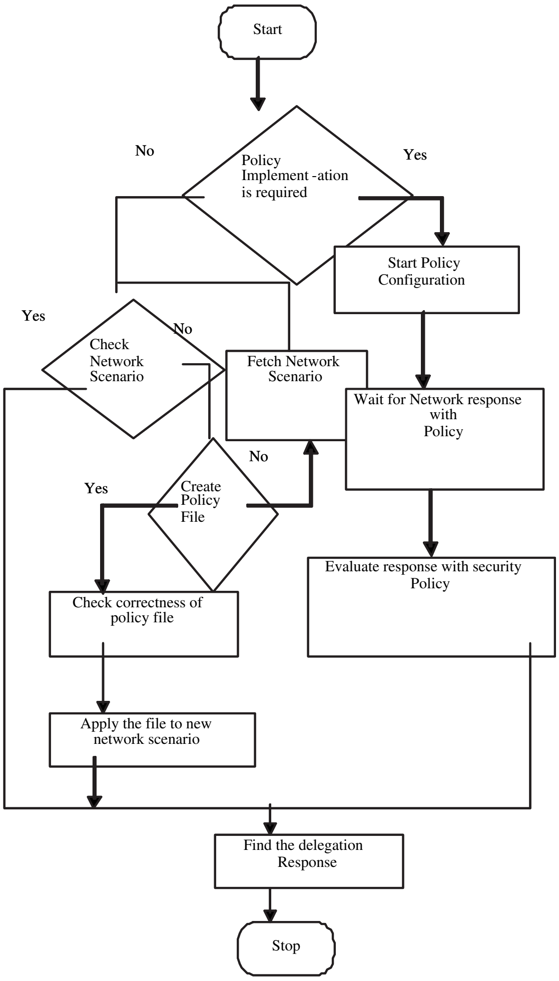
Start
Policy Implement -ation is required
No
Yes
Start Policy Configuration
Yes
Check Network Scenario
No
Fetch Network Scenario
Wait for Network response with Policy
No
Yes
Create Policy File
Evaluate response with security Policy
Check correctness of policy file
Apply the file to new network scenario
Find the delegation Response
Stop

Figure 1: Flow chart for policy selection in optimized manner

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

b. Assume N packets are exchanged during authentication phase. Let total time in processing N packets is represented by $TN(P_\varphi)$ which can be calculated as follows:$TN(P_\varphi) = \sum_{K=1}^{N}(t_k(P_\varphi))$.

c. Let AT denote authentication time. As it depends on mobility scenarios N, R and security policies P as defined in Sections 4.2 and 4.3, therefore AT can be represented as $AT(N, R, P)$ and can be calculated using as follows: $AT(N, R, P) = \sum_{K=1}^{N}(t_k(P_\varphi))$.

2) Number of Authentication Messages (AM) is concerned with the messages exchanged during an authentication phase.

3) Policy Overhead (Bit/Sec) $O(P_\varphi)$. Refers to the overhead associated with a security policy during data transfer between sender and receiver.

4) Response Time (End-to-End) (RS) is a measure of the delay in transmission of data between a sender and a receiver.

5) 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:

Step 1. Determine time $t_f(P_\varphi)$. When first data packet is sent from a sender i to a receiver j with security policy (P_φ).

Step 2. Determine time $t_l(P_\varphi)$. When last data packet is delivered to a receiver j from a sender i with security policy (P_φ).

Step 3. Calculate total time, denoted as tt, by subtracting $t_f(P_\varphi)$.from $t_l(P_\varphi)$.which can be given as follows: $tt = t_l(P_\varphi) - t_f(P_\varphi)$.

Step 4. 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 as follows: $dt = \frac{D}{t_1(P_\varphi) - t_f(P_\varphi)}$.

Step 5. Since throughput Th depends on factors such as N,R, P, Tr and D, where Tt represents traffic types such as TCP or UDP, D 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 follows: $Th(N, R, P, T_t, DS) = \frac{D}{t_1(P_\varphi) - t_f(P_\varphi)}$.

6) Centralized WEP Key Management and Policy Based Key Rotation: We have used centralized key management method, once mutual authentication has been successfully completed, the client and radius servers each derive the same session keys.

7) Wireless LAN Policy Checklist.

8) Usage Policies:

a. Applications Across the WLAN: Bandwidth-intensive applications and extremely confidential enterprise data may not be best suited to run on the wireless LAN.

b. Network Roaming: Define the access points and WLANs that each station is allowed to connect to roaming clients.

c. Uncontrolled Environments: Define where organization-owned, wireless-enabled laptops are allowed to connect to uncontrolled wireless LANs. Establish VPN capabilities for remotely connection to the enterprise network from home WLAN or hotspot.

9) Configuration Policies:

   a. Encryption & Authentication for All WLAN Traffic: At a minimum, enterprises should employ the built-in WEP encryption. However, 802.1x, WPA and proprietary technologies (LEAP) are highly recommended for enterprise WLANs. Traffic should be monitored to ensure that traffic is encrypted & authenticated.

   b. Authorization - MAC Filtering or RADIUS Server: MAC address filtering provides basic control over which stations can connect to an enterprise WLAN. Larger enterprises will require a RADIUS server to manage hundreds of stations and dozens of access points. Monitor the WLAN for unauthorized users.

   c. Naming the Network - Changing Default SSIDs: Service Set Identifiers should be changed from default settings and renamed as to not draw attention from outsiders. (e.g. Avoid SSIDs of *CEO Office* or *Cash Register*) Monitor the WLAN for access points with default or improper SSIDs [38].

   d. Reconfigure Default Windows XP Settings: Windows XP stations should be reconfigured from default settings that connect the station to the access point with the strongest signal - even if it's not an authorized access point. Monitor all stations for insecure stations and accidental associations.

10) Security Policies:

   a. Prohibit Unauthorized "Rogue" Access Points: All access points should be securely deployed through the IT organization. Organizations should monitor all WLAN activity to detect rogue WLANs attached to the wired network.

   b. Prohibit Ad Hoc Networks: Stations should be configured to not allow peer-to-peer, ad hoc networks between stations. Monitor the WLAN to identify ad hoc networks and recognize stations that are configured to allow ad hoc networks even if no peer-to-peer network exists at that time [41].

   c. Limit Off-Hours Traffic: Turn off the access point during non-use hours and monitor the airwaves for off-hours traffic.

   d. Vendor-Specific Hardware: Limit WLAN hardware to select vendors which support the deployed security measures and monitor for unauthorized vendors [41].

11) Performance Policies:

   a. Maximum No. of Stations Connected to an Access Point: Network performance decreases dramatically when too many stations connect to the same access point. Network administrators should be alerted to when more than 15 or 20 stations are on the same access point [39].

   b. Maximum Bytes allowed between an Access Point and the Wired Network: Make sure your WLAN does not overly drain bandwidth from the wired network by establishing a maximum number of bytes for traffic between the access point and wired network [39].

   c. Maximum Bytes allowed between an Access Point and a Single Station: Establish a performance threshold for the maximum number of bytes allowed between an access point and individual stations to guard against one station utilizing excessive bandwidth degrading the performance of others connected to the access point [39].

5 Experimental Testbed

All systems use RHL 9.0 kernel 2.4.20. Routers, Hosts are IBM systems (Pentium IV 2.8 GHZ). Moreover, Sharp Zaurus (Intel XScale 400 MHz with Linux Embedix), iPAQ (Intel StrongARM 206 MHZ with Familiar Linux) and IBM Laptop (Celeron Processor 2.4GHZ with RHL 9) are used as Roaming host. Open source softwares such as FreeSwan for IPSEC Xsupplicant for 802.1x supplicant, Free Radius for Radius server, OpenSSL for SSL, Mobile IP from Dynamic, Ethereal (packet analyzer), Netperf and ttcp (network monitoring utilities) are used for different functionalities in the tested.

1) experimental environment consists of windows XP OS. (As XP has built in implementation of 802.1X).

2) Server ML-530, XEON, 1 GHz, 1 GB RAM, 128 GB HD.

3) Cisco Aironet 1100 - wireless access point RAM Installed (Max): 16MB, Flash Memory Installed (Max): 8 MB flash. Ethernet, Fast Ethernet, IEEE 802.11b. SNMP, Telnet, HTTP, DHCP support, BOOTP support, VLAN support, manageable.

4) Windows XP clients with 2.4 Ghz, 512 RAM, ORINICO USB client and OriNiCO gold card.

5) Mobile Pentium Centrino with 2.4 GHz, 512 MB RAM, 60 GB HDD, 8X CD/DVD writer, Wireless LAN with windows XP.

6) PIX 535 Processor: 1.0-GHz Intel Pentium III, Random Access Memory: 512 MB, or 1 GB of SDRAM, Flash Memory: 16 MB, Cache: 256 KB level 2 at 1 GHz, System BUS: Dual 64-bit, 66-MHz PCI; Single 32-bit, 33-MHz PCI.

7) Cisco secure access control server.

8) Windows 2000 server for certificates [27, 39].

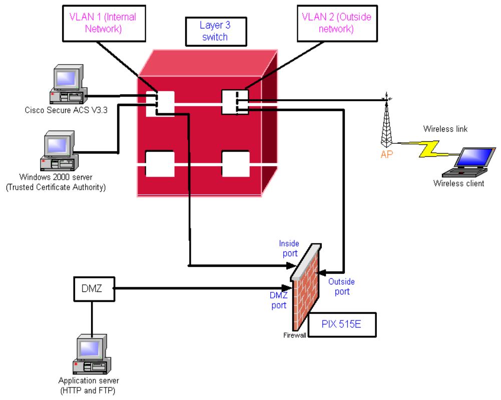

Figure 2: Test bed architecture for policy indexing model implementation

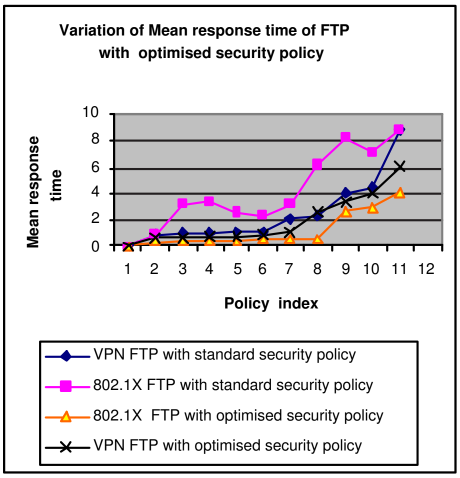

Figure 3: FTP mean response time for 802.1X and VPN

6 Performance Analysis

6.1 Measuring Performance

Some of the performance measurements are [40]: Response time, Throughput, Coverage area, Mobility, Bandwidth, Latency, Radio signal strength, etc.

6.1.1 Response Time

The total time required traffic to travel between two points. It includes the time of dial-up connection establishment, security negotiation time between the server and the clients and the actual data transfer

6.1.2 Throughput

The total number of bytes transmitted over the network in a given time (response time).

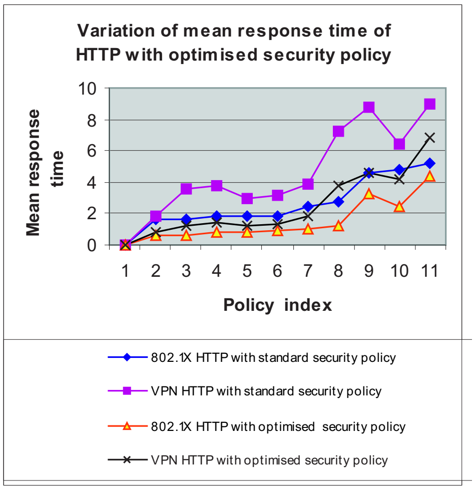

Figure 4: HTTP mean response time for 802.1X and VPN

6.1.3 Outgoing Bandwidth

The incoming bandwidth of an 802.11b Access Point is 11 Mbps (according to standards).Since we were interested in the behavior of networks under congestion, we decided to set the outgoing bandwidth of each client to be 12 Mbps [47].

6.1.4 Traffic Type

It was decided to experiment with TCP and UDP protocols, as these protocols form the basis of all the applications running on the IP protocol stack. Our studies have evaluated the performance of TCP and UDP protocols over wireless networks along with the impact of different security policy mechanism into account [39].

6.1.5 Content of Packet

Content of each packet was decided to be random. This parameter was considered thoroughly in this research , It was decided to choose 40 and 2000 bytes as boundaries of IP packet sizes [37].

A. Mean Response Time Variation
We found in Figure 3 and Figure 4 that FTP performed better than HTTP because the later requires more interaction between the server and the client. Providing same data file sizes for both traffic types would represent a better measurement for HTTP.

B. Throughput Variation
An inverse relationship was found in both the 802.1X and VPN models between response time and throughput as response time increased throughput decreased as shown in Figures 5 and 6.

C. Impact of Packet Size on Mean Response Time
Varying the transmission packet size has a direct influ-

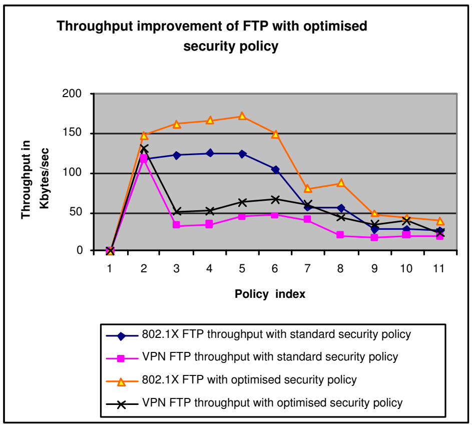

Figure 5: FTP throughput for 802.1X and VPN

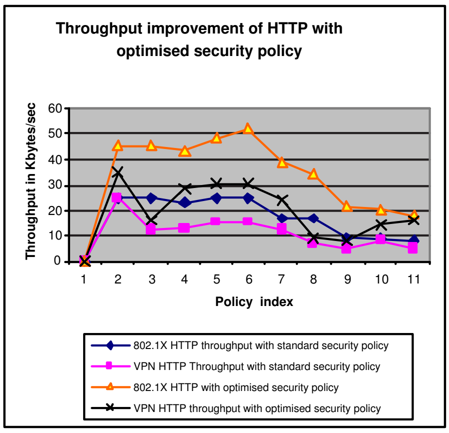

Figure 6: HTTP throughput for 802.1X and VPN

ence on mean response time in wireless network. This is because the larger the packet size, the longer is the packet transmission, propagation and processing times. The minimum and the maximum packet size consider in our experiment are from 100 byte to 2000 byte. The mean response time increases 4.25 ms per 100 bytes of packet length.

D. Impact of Packet Size on Throughput

Since wireless networking will be continuing to support HTTP and FTP based applications. We investigate the average throughput variation through the impact of packet size. Throughput increases from 27.5 to 155.4 kb/s when the packet size is increased from 100 to 1000 bytes. This corresponds to the increase of 392% in throughput. When the packet size increases to 1500 bytes the communication throughput reaches to 160 Kb/s. After reaching this packet size we found that by increasing the packet size then there will be no significance change in throughput as the throughput is maximum.

The use of large packet size can increase the performance of wireless networks in terms of throughput. However at for large packet size. We have increased the packet size to 2000 bytes and we found that the throughput gradually decreases. This is mainly happens due to the fragmentation of packets after 1500bytes.We observed that the throughput becomes 139.5 Kbytes/sec, which is 15.8% less in case of FTP traffic as shown in Figure 7 and Figure 8. This is happening due to there is the probability that the packet is get corrupted. This behavior is likely to occur in a wireless environment due to its high bit error rate, link loss probability contention from on going traffic and the number of neighboring nodes as compared with the wired medium.

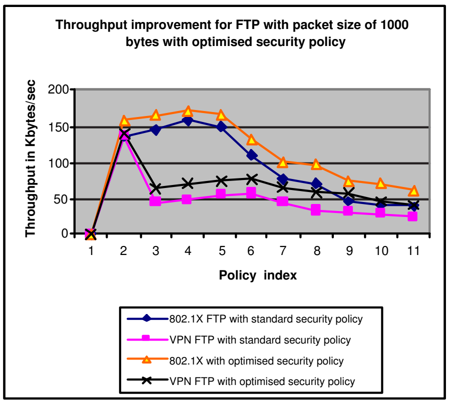

Figure 7: FTP throughput for 802.1X and VPN with packet size of 1000 byte

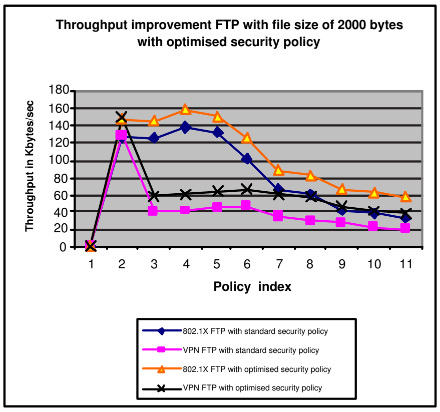

Figure 8: FTP throughput for 802.1X and VPN with packet size of 2000 byte

Throughput increases 5.14 Kbytes to 30 Kbytes for increase of packet size form 40 to 1000 bytes. When packet size increases to 2000 bytes then we observe that throughput decreases to 24.5 Kbytes for HTTP traffic. This is due to the defragmentation of packet and it reduces the throughput to 18.2% as shown in Figures 9 and 10 below.

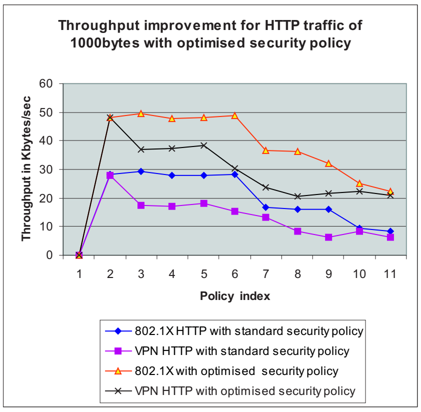

Figure 9: HTTP throughput for 802.1X and VPN with packet size of 1000 byte

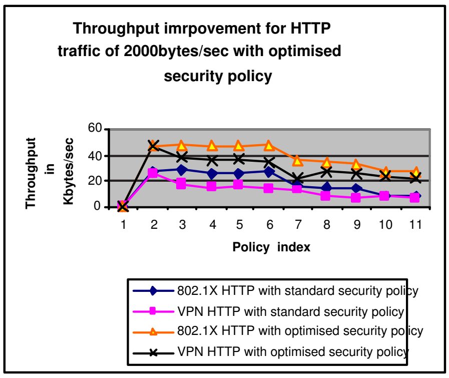

Figure 10: HTTP throughput for 802.1X and VPN with packet size of 2000 byte

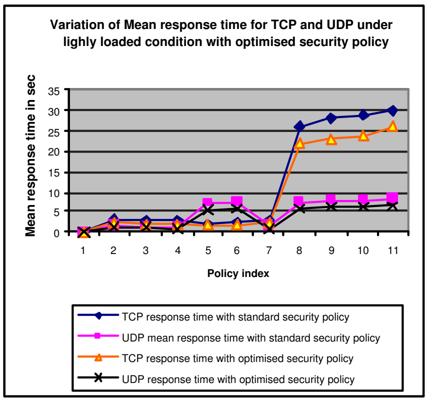

Figure 11: Variation of mean response time in heavily loaded condition

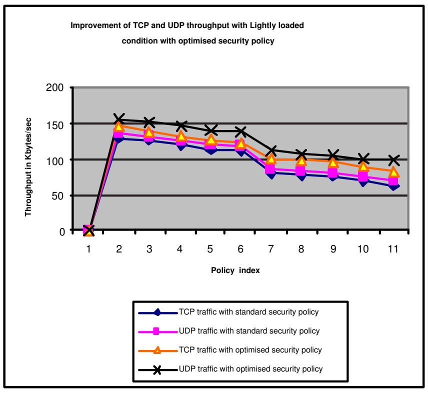

Figure 12: Throughput variation in lightly loaded condition

E. 802.1X Model Simulation Result

From result we found that MAC address authentication produces no performance overheads compared to default settings. WEP has minor impact on FTP throughput but decreases HTTP by 7.5% [4, 6]. Since the effect is small, WEP authentication should be deployed. Using 802.1X authentication methods degraded network performance significantly compared to WEP authentication. Further EAP-TLS produced greater performance impact than EAP-MD5, as it provides mutual authentication and key management. By using encryption of WEP with 128 bits will reduce FTP performance by less than 20% [13, 35, 49]. But the use of EAP-MD5 and EAP-TLS increases the response time by 100%; there will be performance degradation of 47.8%. When we analyses the combined effect of the encryption and authentication FTP response time increases by 268% and throughput decreases by 73% [5, 26].

F. VPN Model Simulation Result

In VPN model simulation authentication tunnel creates delay of response time of FTP by 245% and 113% for HTTP. So the throughput is reduced by 50%. But when employ EAP-TLS it takes delay time of 20%, which in turn decreases the throughput by 17%. By enabling DES and 3DES encryption for VPN model we found that there will be increase of response time by 130%, so the throughput decreases by 50% [6, 46, 48].

7 Simulation of WLAN with TCP and UDP Traffic

1) Mean Response Time Variation:
   Mean response time of UDP rises to 201%, where as in case of TCP it increases to 512% as shown in Figure 11.

2) Throughput Variation:
   Under lightly loaded condition i.e. the bandwidth of 1Mbps,TCP throughput is 13.8% more than UDP throughput as shown in Figure 12. But in case of heavily loaded condition i.e. in Figure 13, UDP throughput is 22.3% more at bandwidth of 12

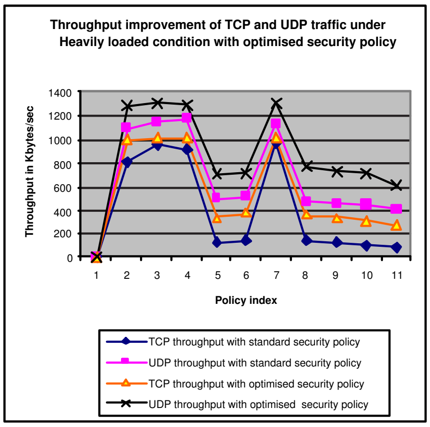

Figure 13: Throughput variation in heavily loaded condition

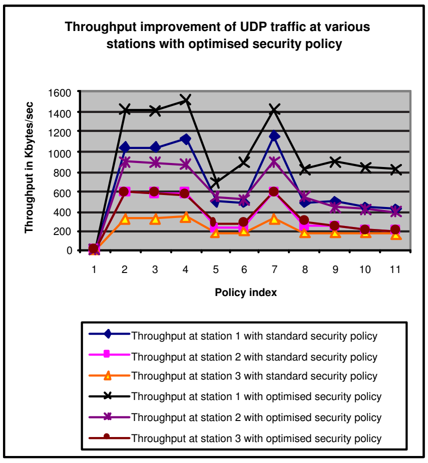

Figure 14: Throughput variation for multi AP scenario for UDP traffic

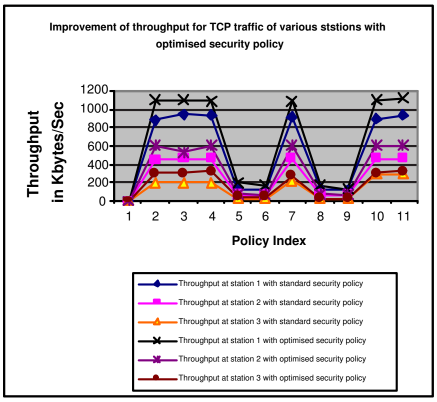

Figure 15: Throughput variation for multi AP scenario for TCP traffic

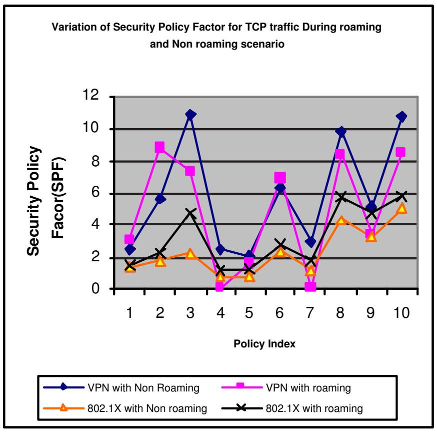

Figure 16: Variation of SPF for TCP traffic during roaming and non-roaming scenario

Mbps.In congested network, the overhead produced encrypting in each individual packets are significantly higher than that of EAP-TLS.Throughput drastically decreases when number of station are increasing as shown in Figure 14.

8 Conclusion

In this paper, we implemented the performance impact incurred with various security Policy mechanisms considering different security Policy indexes, and found that the more secured a network became, the higher the performance impact. This research was successful in investigating the performance and security issues of IEEE 802.11 wireless LANs with the layered security policy model, using multiple APs. It studied the interaction between different security policy layers and their effects on performance (response time and throughput) of congested and un-congested networks. The analysis confirmed that the security policy layers significantly differ from each other in their effects on the throughput of the network. When the network was not saturated (uncongested), the performance degraded as the quality of the security protection increased. The research also evaluated the effect of different TCP and UDP packet sizes on network performance with security policies, when utilizing different security mechanisms. We observe that the hybrid policies obtain higher SPF values than that of individual policies involve in multiple protocols. In addition it is noticed that security policies involving IPSEC leads to higher SPF values than those without IPSEC. Moreover in general security policies introduce higher overheads in roaming scenarios. Further if we compare SPF values for both TCP and UDP traffic we noticed that SPF values are higher for TCP than UDP.This is due the fact that TCP provides reliable communication involving extra overload. Therefore we may conclude that an effective wireless security policy is based on many factors. User needs, laptop control, importance

Table 1: Hybrid security policy configurations

Policy Index	**Policies configured**	**Authentication delay in sec in Non roaming scenario**	**Authentication delay in sec in roaming scenario**
P-1	IPSEC	1.405	1.432
P-2	802.1X-EAP(MD5) without IPSEC	0.427	1.749
P-3	802.1X-EAP(MD5)	1.722	1.949
P-4	802.1X-EAP(TLS) without IPSEC	1.822	3.144
P-5	802.1X-EAP(TLS) with IPSEC	3.117	3.817

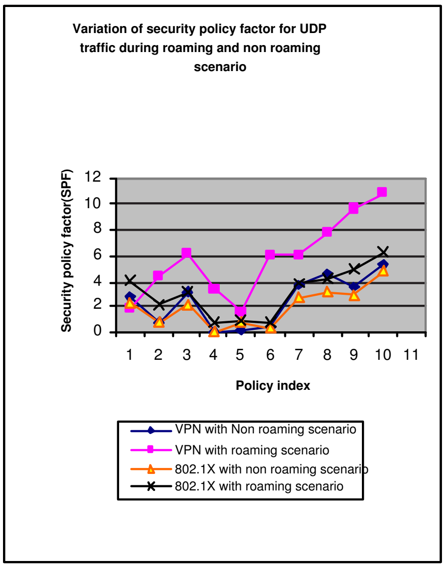

Figure 17: Variation of SPF for UDP traffic during roaming and non-roaming scenario

of data, existing infrastructure, and rogue APs all are factors to consider. As shown by our case studies, different types of organizations have vastly different needs. Understanding the authentication and encryption technologies is vital to creating an effective and manageable security policy.

9 Future Future Directions

A variety of techniques and some of the new Developments in Wireless Security environment are generally coming in near future like, IEEE802.11 (802.11i) working on extensions: WEP2/TKIP (Temporal Key Integrity Protocol), RrK (Rapid reKeying), ESN (Enhanced Security Network), AES (Advanced Encryption Standard), combination of these. Integration of WLANs (802.11) and WWANs (3G). E.g. handoff between 802.11b and CDMA networks secure handoff with existing security architectures. Furthermore, the research focused on 802.11b (Wi-Fi) protocol, as it is the most popular standard for wireless LAN networking. Evaluating the security performance of other 802.11 standards such as upcoming 802.11g, would be a foreseeable extension to this work.

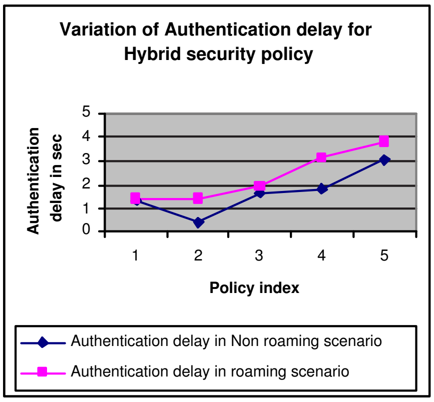

Figure 18: Variation of SPF for UDP traffic during roaming and non-roaming scenario

References

[1] *An Initial Security Analysis of the IEEE 802.1X Standard*, Mishra and Ar-baugh, University of Maryland, 2007. (http://www.cs.umd.edu/ waa/1x.pdf)

[2] W. A. Arbaugh, N. Shankar, and Y. C. J. Wan, *Your 802.11 Wireless Network has No Clothes*, Department of Computer Science, University of Maryland, Mar. 2001. (http://downloads.securityfocus.com/library/ wireless.pdf)

[3] P. Ashley, H. Hilton, and M. Vandenwauver, *Wired Versus Wireless Security*, Internet: white paper /2002.

[4] B. Askwith, M. Merabti, Q. Shi, and K. Whiteley, "Achieving User privacy in Mobile Networks," in *proceedings of the 13th Annual computer security Applications Conference*, pp. 108-116, IEEE, 1997.

[5] R. H. Baker, *Network Security*, Tate Mc-Graw Hill, 2nd Edition, 1995.

[6] V. Bharghavan, "Security issues in mobile communication," in *Proceedings of the Second International Symposium on Autonomous Decentralized Systems*, pp. 19-24, IEEE, 1995.

[7] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking*, pp. 56-67, July 2001.

[8] P. Brenner, *A Technical Tutorial on the IEEE 802.11 Protocol*, BreezeCOM Wireless Communications, 1997. (http://www.sss-mag.com/pdf/802_11tut.pdf)

[9] A. Chickinsky, *Wireless LAN Security Threats*, Litton/TASC, IEEE 802.11-01/258, May 2001.

[10] Cisco Systems white paper, *Wireless LAN Security*, 2007. (http://www.cisco.com/warp/public/cc/pd/witc/
ao350ap/prodlit/a350w_ov.pdf)

[11] J. Clift, *The GNU/Linux CryptoAPI site*, 12th May 2003, Retrieved 14 Sep. 2003. (http://www.kerneli.org/index.phtml)

[12] S. Convery, and D. Miller, *SAFE: Wireless LAN Security in Depth*, version 2, White paper, Cisco Systems, Inc., 2003. (http://www.cisco.com/warp/ public/cc/so/cuso/epso
/sqfr/safwl_wp.pdf)

[13] D. A. Cooper, and K. P. Birman, "Preserving privacy in a network of mobile computers," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 26-38, IEEE 1995.

[14] J. Edney, and W. A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Addison Wesley, 2003.

[15] D. B. Faria, and D. R. Cheriton, "DoS and authentication in wireless public access networks," in *Proceedings of the First ACM Workshop on Wireless Security (WiSe 02)*, pp. 47-56, Sep. 2002.

[16] S. Fluhrer, , I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," *Selected Areas in Cryptography 2001*, pp. 1V24, 2001.

[17] B. Harris and R. Hunt, "TCP/IP security threats and attack Methods," *Computer Communications*, vol. 22, pp. 885, 1999.

[18] R. Hunt, "Internet/Intranet firewall security-policy, architecture and transaction services," *Computer Communications*, vol. 21, pp. 1107-1123, Aug. 1998.

[19] IEEE, *IEEE Standard 802.11i / Draft 3.0. Draft Supplement to ISO/IEC 8802-11/1999(I) ANSI/IEEE Std802.11*, 1999 edition: Specification for Enhanced Security, pp.5-6, Nov. 2002.

[20] IEEE P802.11i/D9.0, Amendment to ANSI/IEEE Std 802.11-1999 Edition as amended by IEEE Std 802.11g-2003 and IEEE Std 802.11h-2003, Mar. 2004.

[21] IETF, *PPP EAP TLS Authentication Protocol*, RFC 2716, Oct. 1999.

[22] IPSEC. (http://www.freeswan.org)

[23] B. Jesiek, *InternetSecurity-Firewalls.* (http://www.ee.mtu.edu/course/ee465/groupb/fwll.html)

[24] T. Karygiannis, and L. Owens, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, National Institute of Technology, Special Publication, pp. 800-848, Nov. 2002.

[25] M. Komu, and T. Nordstrom, *Known Vulnerabilties in Wireless LAN Security*, Helsinki University of Technology, Oct. 1999. (http://www.niksula.cs.hut.fi/∼mkomu/docs/
wirelesslansec.html)

[26] M. j. Mayer, "A survey of security Issues in Multicast Communication," *IEEE transactions on Computer Networking*, vol. 4, no. 2, pp 12-23, Nov./Dec. 1999.

[27] Microsoft, *Wireless 802.11 Security with Windows XP*, 2002. (http://www.microsoft.com/windowsxp/pro/techinfo/administration/wirelesssecurity/XP
80211Security.doc)

[28] S. K. Miller, "Facing challenge of the wireless security," *IEEE Transactions on Computer*, vol. 3, no. 4, pp 16-18, July 2001.

[29] A. Mishra, N. L. Petroni, and B. D. Payne, *Open1x – Open Source Implementation of IEEE 802.1x*, Jun. 2003. (http://www.open1x.org/)

[30] F. Moioli, *Security in Public Access Wireless LAN Networks*, M.Sc. Thesis, Royal Institute of Technology, Stockholm, Jun. 2000. (http://downloads.securityfocus.com/library/fabio-thesis.pdf)

[31] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Wireless data networks lack inherent security," in *National Workshop on Cryptology*, pp. 67-75, Chennai, Oct. 2003.

[32] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Advantage of Elliptic curve cryptography for wireless networks," in *International Conference on Emerging Technology*, pp. 122-129, Bhubaneswar, Dec. 2003.

[33] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Mobile data Networks security issues and challenges," in *International Conference on Emerging Technology*, pp. 137-148, Bhubaneswar, Dec. 2003.

[34] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Various types of attacks in wireless Local area networks," in *National Conference on HSeCNET*, Hyderabad organized by CSI and IDRBT (Reserve bank of India), Jan. 2004.

[35] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Security issues in wireless local area network," in *Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering*, pp. 108-111, May 2004.

[36] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Security issues in mobile data network," in *IEEE Vehicular Technology International Conference 2004 - Fall, Wireless Technologies for Global Security*, pp. 45-49, Los Angeles, CA, Sep. 2004.

[37] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Modeling and evaluation of security architecture for wireless local area networks," in *Proceedings of Advanced computing and communication*, pp. 281-285, Ahmedabad, Dec. 2004.

[38] D. Nayak, D. B. Phatak, and V. P. Gulati, "Modeling and evaluation of security architecture for wireless local area networks by indexing methods: A novel approach," in *The First Information Security and Practice and Experience Conference (ISPEC - 2005)*, LNCS, no. 3439, pp. 25-35, Apr. 2005.

[39] D. Nayak, D. B. Phatak, and V. P. Gulati, "Performance evaluation of security architecture for wireless local area networks by security policy method," in *2005 IEEE Sarnoff Symposium*, pp. 37-40, Nassau Inn in Princeton NJ, USA, Apr. 2005.

[40] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Modeling and performance evaluation of security architecture for wireless local area networks," *International Journal of Computational Intelligence*, vol. 3, pp. 13-16, 2004.

[41] D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Policy based performance evaluation of security architecture for wireless local area networks," in *6th World Wireless Congress*, pp. 51-57, San Francisco, USA, May 2005.

[42] R. K. Nichols, *Wireless Security*, McGraw-Hill Telecom International Edition, 2002.

[43] D. Patiyoot and S. j. Shepherd, "Cryptographic security Techniques for wireless Networks," *IEEE Networks*, pp. 36-50, 2002.

[44] B. Potter and B. Fleck, *Chapter 1: A Wireless World, 802.11 Security*, O'Reilly & Associates, ISBN 0-596-00290-4, Dec. 2002.

[45] A. T. Rager, *WEPCrack Project Webpage*, Retrieved May 2003. (http://sourceforge.net/projects/wepcrack/)

[46] S. Ravi, A. Raghunathan, and N. Potlapally, "Securing wireless data: system architecture Challenges," *ACM Journal of Networks*, pp. 195-200, Oct. 2002.

[47] E. Sanchez and R. Edwards, "Optimization of the establishment of secure communication channel in wireless mobile networks," in *Proceedings of the International Parallel and Distributed Processing Symposium*, pp. 127-138, IEEE, 2002.

[48] R. E. Smith, *Internet Cryptography*, Addison-Wesley Publishing Company, 1999.

[49] W. Stalling, *Cryptography and network Security*, Prentice Hall, Second Edition, 2000.

[50] D. V. Thanh, "Security issues in mobile ecommerce," in *Proceedings of the 11th International Workshop on Database and Expert System Applications*, pp.1-14, IEEE, 2000.

[51] P. Trudeau, *Building Secure Wireless Local Area Networks*, Colubris Networks Inc., 2001. (http://www.wlana.com/pdf/security_colubris.pdf)

[52] J. R. Walker, *Unsafe at any Key size; An analysis of the WEP Encapsulation*, IEEE802.11-00/362, Oct. 2000. (http://grouper.ieee.org/groups/ 802/11/Documents/ DocumentHolder/0-362.zip)

[53] *WildPackets' Guide to Wireless LAN Analysis*, WildPackets Inc., 2001. (http://www.wildpackets.com/elements/Wireless_LAN_Analysis.pdf)

[54] *Wireless LAN Security: 802.11b and Corporate Networks*, Internet Security Systems, 2001. (http://documents.iss.net/whitepapers/wireless_LAN _security.pdf)

[55] Y. Zahur, and T. A. Yang, "Wireless lan security and laboratory designs," *Journal of Computing Sciences in Colleges*, vol. 19, no. 3, pp. 44- 60, Jan. 2004.

Debabrata Nayakreceived his Master degree from NIT Rourkela and currently he is persuing his PhD at K. R. School of Information Technology, Indian Institute of Technology-Bombay, India. His Research interest includes Security system Performance evaluation, Design of secure cryptographic system, Wireless Security and security policy design and implementation. He has reviewed various International Journals and Conferences papers, and is a Life Member of Cryptology Research Society of India and Computer Society of India and Student Member of IEEE Society and member of ISTE. He has to his credit more than 20 research papers published in National/ International Journals and Conferences.

Deepak B. Phatak received his Ph.D. degree from Indian Institute of Technology-Bombay, India. He is Subrao M. Nilekani Chair Professor with K. R. School of Information Technology, Indian Institute of Technology-Bombay, India. His research interests are in the areas of Data Bases and Information Systems, Software Engineering, System Performance Evaluation, IT enabled Education and IT strategy planning. His primary research inclinations are in Technology application and deployment areas.He is a Life Member of Computer Society of India and Member of IEEE Society. Dr. Phatak has a long association with Computer Society of India (CSI) spanning over two decades. He was awarded the CSI Fellowship in December 1999. He has also been elected fellow of IETE in March 2000. He is currently the chairman of the Academic committee for CSI. He works closely with NASSCOM on many of their initiatives related to innovation and education. He is a member of the NASSCOM committee for domestic markets and chairs the education subcommittee.

Ashutosh Saxena received his M.Sc. (1990), M. Tech. (1992) and Ph.D. in Computer Science (1999). Presently, he is working as Associate Professor in Institute for Development and Research in Banking Technology, Hyderabad.

He is on the Editorial Committees of various International Journals and Conferences, and is a Life Member of Cryptology Research Society of India and Computer Society of India and Member of IEEE Computer Society. He has to his credit more than 50 research papers published in National/ International Journals and Conferences. His main research interest is in the areas of Authentication Technologies, Smart Card, Key Management and Security Issues and Payment Systems in Banking.