IMPACT OF USING UPPER LAYERS SECURITY TECHNIQUES IN AD HOC WIRELESS NETWORKS

Jalal FRIHAT[1], Florica MOLDOVEANU[2], Alin MOLDOVEANU[3]

Rețelele ad hoc reprezintă o nouă tehnologie de rețele fără fir. Sunt folosite cu precădere în aplicațiile comerciale. O provocare frecventă în designul rețelelor ad hoc este vulnerabilitatea lor la atacurile variate ale securității.

În acest articol analizăm pericolele asupra unei rețele ad hoc şi scopurile de securitate care trebuie realizate. Apoi prezentăm rezultatele studiului nostru de utilizare a tehnologiei securității de nivel înalt precum: firewalls, sistemul de detectare a intruşilor (intrusion detection system) şi rețele private virtuale (virtual private networks (VPN)), pentru a îmbunătăți securitatea rețelelor ad hoc.

Ad hoc networks are a new wireless networking technology. They have tremendous usage in commercial applications. One main challenge in design of ad hoc networks is their vulnerability to various security attacks.

In this paper, we analyze the threats on ad hoc network faces and the security goals to be achieved. Then, we present the results of the conducted study of using upper layer security techniques such as firewalls, intrusion detection system and virtual private networks (VPN), to improve the security of ad hoc networks.

Keywords: Ad hoc, WEP, Firewall, VPN and IDS

1. Introduction

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network, there is no fixed infrastructure such as base stations or central access points. Mobile stations that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to forward messages to them. The mobile devices serve as routers for mobile hosts. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

The interest in ad hoc networks largely stems from the ability to rapidly deploy them under both normal and harsh conditions. These networks can be

[1] PhD student, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania, Email: Frihat_Jalal@yahoo.com
[2] Professor, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania
[3] Lecturer, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania

quickly deployed in situations where no infrastructure exists and it would be impractical or infeasible to deploy infrastructure. In such networks, nodes are expected to cooperate to perform essential networking tasks such as routing.
Wired Equivalent Protocol Privacy (WEP) is the basic security algorithm used in the ad hoc networks. A combination of simple security measures with the upper layer security techniques such as firewalls, Intrusion Detection System (IDS) and the Virtual Private Networks (VPN), will increase the security level of the ad hoc networks.
In this paper we analyze the effect of adding security techniques to the ad hoc wireless networks. The analysis is carried out over our experiments on IEEE 802.11g wireless test bed environment, by enabling WEP with different keys sizes and then analyzing the transfer time and the throughput variation of different file sizes. The work in this paper starts by setting a test bed based on no security and WEP encryption, and analyzing the initial results to create a baseline and compare the results obtained from the different experiments.

2. Architecture of the wireless networks

A network based on the IEEE 802.11 standard is composed of a number of nodes that form cells, which can overlap. The Basic Service Set (BSS) represents the coverage area of an individual cell, and outside the BSS, a wireless station cannot communicate with stations in this cell.

IEEE 802.11 standards define two modes of operation: infrastructure mode (also known as BSS), and ad-hoc mode known as Independent BSS (IBSS).

In the infrastructure mode, all wireless communications pass through a central station known as Access Point, which manages the network flow and access. The access point provides functionality similar to that provided by a base station in other cellular networks, because it acts as a bridge between the wireless segment and the wired segment. This architecture allows the interconnection of several basic service sets, which form an Extended Service Set (ESS).
The ad-hoc mode is composed solely of clients within a mutual communication range via the wireless medium; the Ad-Hoc mode is also called peer-to-peer or Independent Basic Service Set (IBSS). Ad hoc wireless networks are self-configuring networks, and consist of a set of wireless users that communicate over wireless links.

A wireless ad hoc network requires at least two mobile devices to be able to form a simple peer-to-peer network that will allow the wireless stations to share resources. Because the nodes are mobile, the topology of the network can be changed without any prediction. All the activities of the network, such as discovering the type of topology to be used, delivering and routing messages,

must be done by the nodes themselves. Ad-hoc is a decentralized network type where the functionality of the wireless local area network is based on the nodes.

Examples of ad-hoc networks applications include rescue operations, conferences, and military operations. The coverage area is composed of the overlapping coverage area of each client.

Wireless ad hoc networks can be classified by their application:

- Mobile ad hoc networks (MANETs): self-configuring network of mobile hosts connected wirelessly. The mobile hosts are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may be used for conferencing and file sharing. Vehicular Ad-Hoc Networks (VANETs) are used for communication between vehicles and nearby fixed equipment. The main goal of VANET is providing safety and comfort for passengers. A special electronic device will be placed inside each vehicle which will provide ad hoc network connectivity for the passengers.
- Wireless mesh networks: communication networks made up of mobile nodes in which there are at least two pathways of communication to each node.
- Wireless Sensor Networks (WSN): wireless networks consisting of distributed devices using sensors to cooperatively monitor physical conditions, such as temperature and pressure, at different locations.

3. Security of Ad hoc wireless networks

Wireless networks do not have any physical connection They send data over the air using radio waves that travel between client devices, which mean that any wireless station within transmission area can receive data transmitted to or from other wireless stations. Thus, if not encrypted, the transmitted packets can be viewed by anyone within the radio frequency range. However, the traditional IEEE 802.11 WLAN provides some security means to protect the network. These security means include the use of open or shared-key authentication and static Wired Equivalent Privacy (WEP) keys. Their combination provides a level of access control and privacy but each one of them can be compromised.

Most of the vulnerabilities of MANETs come from their open architecture; the wireless medium is accessible to both legitimate and illegitimate network users. Attacks against ad hoc networks can be divided into two groups: passive attacks and active attacks [16]. Passive attacks involve only *eavesdropping* of data with no altering of the transmitted data. *Active attacks* involve actions performed by attackers to replicate, modify and delete the exchanged data. Since malicious insider nodes already belong to the network as an authorized party, they may use the standard security techniques to actually protect their attacks. These kind of

malicious parties are called c*ompromised nodes*, as their actions compromise the security of the whole ad hoc network.
Active attacks have several forms:

- External attacks that are targeted to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls and encryption.
- Denials of Service (DoS) attacks produced by malicious actions. The success of such attacks depends on the area of application of the ad hoc network. For example, in a conference room any of the nodes can be damaged without completely destroying the ad hoc network. On the other hand, in the military application, such as a battle field, the efficient operation of the ad hoc network depends on the operation of all the soldiers' mobile devices. If the network is shutdown, the soldiers cannot communicate with each other or to the headquarters. In the worst case, the attacker is able to change routing protocol to operate in the way the attacker wants.
- Impersonation attacks occur when a compromised node is able to join the network or send false routing information. Impersonation attacks concern all critical operations in ad hoc networks. In the conference room, the impersonation attack is not feasible, and has small effect. In the military example, the impersonation is much more severe. A malicious node controlled by the enemy may be able to join the ad hoc network undetectably and cause permanent damage to other nodes. Impersonation threats are mitigated by applying strong authentication mechanisms. In many cases, lighter solutions like the use of keyed hash functions or session keys are needed.
- There are ad hoc routing protocols attacks which are beyond the scope of this paper.

In this paper we will focus on the fundamental security techniques of protecting the MANET ad hoc networks connectivity between mobile nodes. The common concerns in ad hoc networks include the access control method for restricting the access of foreign nodes to the network, which requires the use of a proper authentication mechanism and securing end-to-end communication by using data encryption; this is especially important in military applications [17].

In ad hoc networks the possibility of Denial of Service (DoS) attacks must also be mitigated, to ensure full network availability, with the use of ad hoc node redundancies [17].

Antivirus solutions, firewalls and intrusion detection systems can be used to detect and mitigate against worms, viruses and malicious activities.

It is clear that the security threats of ad hoc networks form a very complex subject, because of the dynamic and unpredictable nature of most ad hoc networks. All security mechanisms applied in networking require the use of cryptography. On the other hand, ad hoc networks vary from each other greatly from the area of application. Some ad hoc networks may not need security solutions other than simple encryption and username-password authentication scheme, as in the conference room example, where speed of data transmission is very important, while networks operating in highly dynamic and hostile environments, such as in the military battlefield, demand efficient and strong confidentiality mechanisms, with the expense of lower data transfer rate that may result from applying extra security techniques.

The IEEE 802.11 standard provides two types of authentication: open system and shared key authentication. The open system authentication provides null security protection, while shared key authentication requires using the WEP algorithm to provide access control [1,6].

Ad hoc security can be improved by using other upper layer security techniques such as firewalls, intrusion detection and prevention system and the virtual private network. A firewall can be either a dedicated hardware or a special software running on computer, which inspects network traffic passing through it, and denies or permits message passing based on a set of rules [7].

In Virtual Private Networks (VPN), all the transmitted data is tunneled through another network, and dedicated for a specific network. When leveraging a VPN to encrypt IEEE 802.11 wireless data communications, each and every wireless node requires VPN client software in order to perform the necessary authentication and encryption. An Intrusion Detection System (IDS) generally detects unwanted attacks of any computer system, either through the Internet or inside the network. This includes network attacks and host based attacks such as privilege escalation, unauthorized logins, access to sensitive files and Malware (viruses, Trojan horses, and worms). One of the IDS types is the host-based intrusion detection system that consists of a software on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, access control list databases) and other host activities and states [8,13].

In [14] the authors studied the impact of WEP on Ad hoc networks. They have used two laptops with traffic generation software. They studied the case where one of the laptops was connected to the wired network and they measured the throughput of such a network. The authors of [15] presented an analysis of applying WEP on the traffic of ad hoc networks. They examined the effect of applying WEP to different packet sizes and using different distance between the communicating machines. The authors' results indicated that the throughput decreases with the presence of security.

In this paper we present the results of our study regarding the effect of applying upper layers security techniques (such as VPN, firewall and IDS) on the throughput of the ad hoc networks. Since the main usage of ad hoc networks is for file sharing**,** we measured the network throughput when transferring files between two laptops.

We studied the influence of these security techniques on the time required to transmit files of different sizes between mobile stations in ad hoc networks.

All measurements have been carried out in a non-interference environment: there are no other devices that use the frequency of the wireless devices (like microwave oven and personal digital assistants). The wireless devices used in the measurements brought closer to each other to eliminate any signal degradation. The data rate varies according to the distance between the wireless devices: data rate decreases as the distance increases. The maximum distance between the two laptops depends on the transmission power, i.e. 10 - 91 meters for IEEE 802.11g, while its 10-50 meters for IEEE802.11a [20]. Typically, the maximum distance, which gives the maximum data rate of 54 Mbps, between ad hoc devices is around 45 meters, throughput decreases as distance between the two computers increases

4. Study procedure

The measurements were carried out by using two laptops with the same characteristics and same operating system (Windows Vista home edition premium). The two laptops were connected to each other wirelessly to form an ad hoc network, then they were used to transfer files from one to another using different configurations of security.

We have used the following security combinations:

1. Only WEP: Wired Equivalent Privacy (WEP) with key length of 128 bit. WEP is a symmetric encryption algorithm where a shared secret key (40 or 128 bits) is used for encryption and decryption. WEP is the basic security algorithm used in wireless networks.

2. WEP and Firewall: the WEP encryption algorithm was used here and in addition a software firewall enabled on each wireless client. Examples of the personal firewalls are: ZoneAlarm for Windows Vista (http://blog. Washingt onpost .com /securityfix /2007 /06 / zonealarm_for_windows_vista_re.html) and Sunbelt Personal Firewall (http://www.sunbelt-software.com/Home-Home-Office/ Sunbelt-Personal-Firewall/). We used the firewall solution integrated in Windows Vista operating system.

3. WEP and VPN: a VPN tunnel was established between the two laptops. All the wireless transmission, which was encrypted with WEP, is now passed through this VPN tunnel. We can setup the VPN connection in Windows VISTA, using Control Panel/ Network and Internet connections.

4. WEP and Intrusion Detection and Prevention system: WEP and IDS software were used together. The IDS software can detect any malicious traffic at the application level. An example of IDS software is the Securepoint Intrusion Detection System 1.0 (http://www.softpedia.com/progDownload/Securepoint-Intrusion-Detection-System-Download-1100.html). We used the IDS from Norton security suite software.

5. WEP, firewall and VPN: WEP combined with a firewall and VPN.
6. WEP, Firewall, VPN and IDS: a combination of WEP, Firewall, VPN and IDS.

For each combination of the security techniques listed above (from 1 to 6), the measurements were made at one laptop using capture software (Ehetreal). That software is used to capture all the traffic coming to that laptop, and measure the time required for transmitting different file sizes. In addition, the average number of bytes transmitted over that period is being calculated from the captured data. Each measurement was carried out six times and the average value of these trails was calculated.

5. The obtained results

The first stage was to set a baseline to our experiments. The time required to transfer a file of size 63.7 MB when using WEP 128-bit and 64-bit was measured and compared with the time when no security is applied. Table 1 illustrates the obtained results.

Table 1

Time and average Mega bytes per second for a 63.7 MB file in case of WEP encryption.

	No Sec	WEP64	WEP128
Time (Sec)	55.2167	56.3140	57.1590
MB/Sec	11.5376	11.3114	11.1443

The same results are illustrated in Fig. 1.

From table 1 it is clear that applying WEP with 128 bit key can decrease the throughput of the ad hoc network by 3.8% with respect to the no security case, while WEP-64 bit decreases it by 1.9%. To achieve maximum security, we choose a WEP-128 bit as our baseline.

The next stage was to use WEP-128 bit as our baseline, and then apply upper layer security techniques (the combinations 1-6 described previously). The time required and the average number of bytes transmitted over that time for a file of size 63.7 MB are shown in table 2.

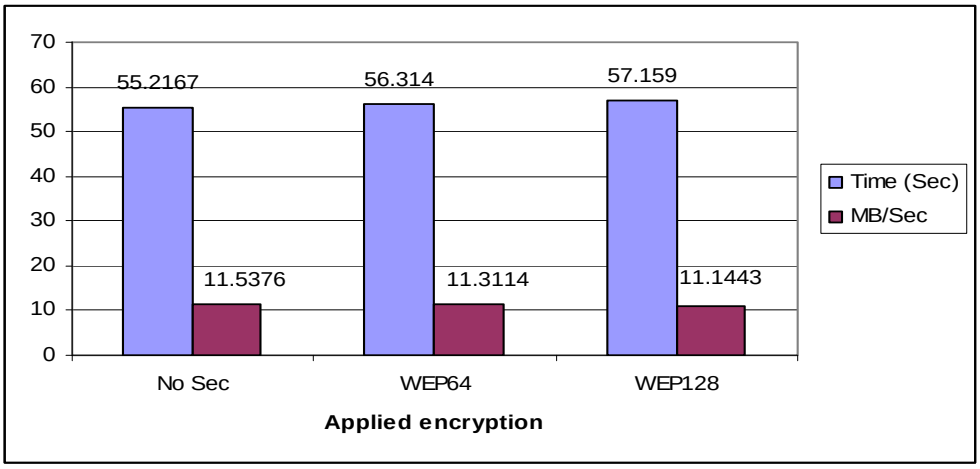

Fig.1 Transfer time and network throughput for 63.7 MB file

Table 2

Time and speed (average Mega Bytes per second)in case of transferring 63.7 MB file

Security technique	1	2	3	4	5	6
Time interval to transfer 63,7MB	57.475	57.369	79.27467	57.517	81.2325	81.4235
Speed: MB/Sec	11.1443	11.14367	8.0351	11.02	7.8412	7.8234

The same results are illustrated in Figs. 2 and 3 respectively.

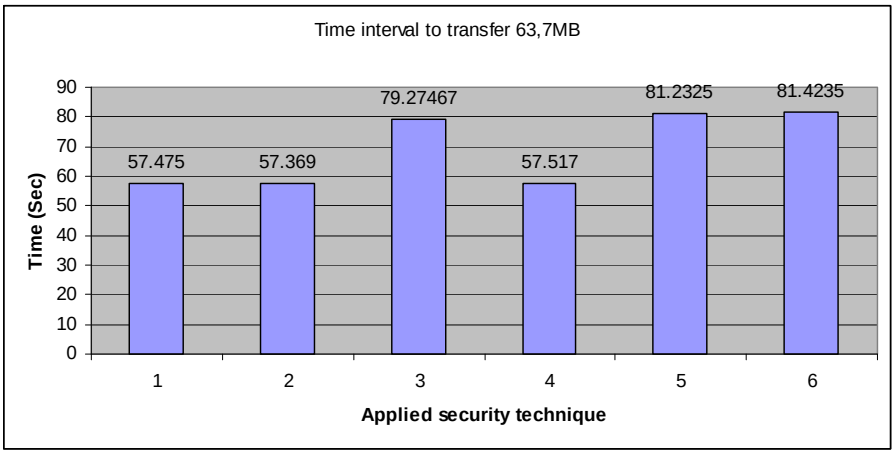

Fig.2 Transfer time for 63.7 MB file in case of different security techniques

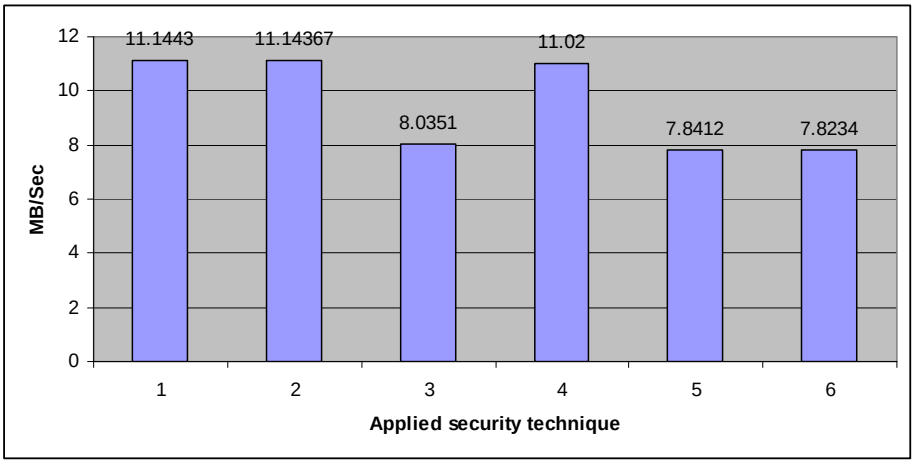

Fig.3 Transmission speed (average MB/Sec) for a 63.7 MB file

We repeated the experiments using a file of 12 MB. The results are shown in table 3, and figs. 4 and 5.

Table 3

Time and average Mega Bytes per second for a 12 MB file

Security technique	1	2	3	4	5	6
Time	13.09783	13.1876	34.66617	13.2346	34.6683	37.65933
MB/Sec	9.410667	9.0992	3.462034465	9.067142	3.461375	3.0727

From figs. 2 and 4 we can conclude that the time required to transfer files when using WEP, firewall and IDS (cases 1,2,4) is almost the same and less than the time required in case of using VPN in any combination (3, 5 and 6). This is because VPN requires an extra time to establish the VPN tunnel and to perform encryption. As a consequence, the number of MB/Sec transmitted when using

VPN (figs. 3 and 5), combinations 3, 5 and 6 are less than the number of MB/Sec transmitted without VPN (combinations 1, 2 and 4).

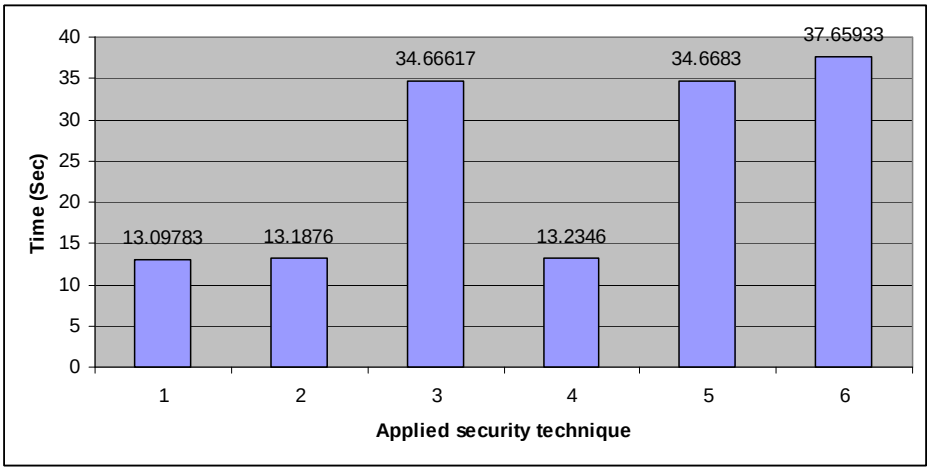

Fig.4 Transfer time for a 12 MB file

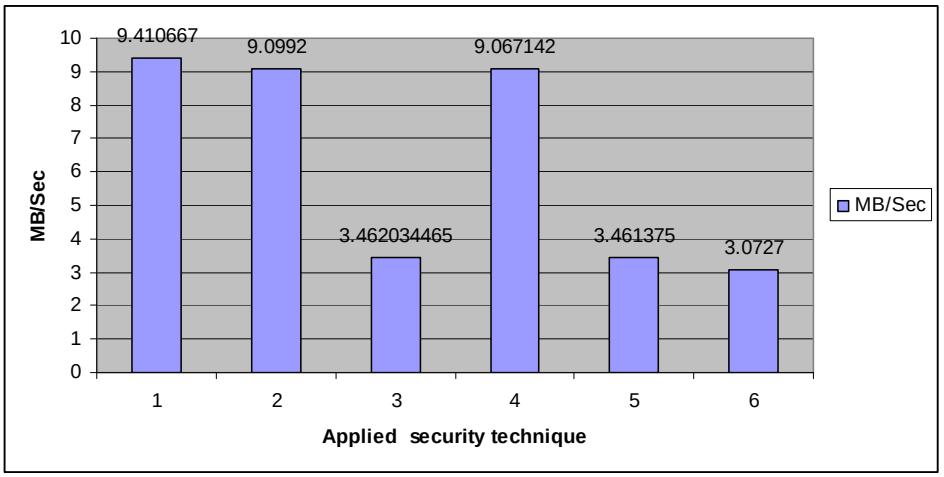

Fig.5 Average MB/Sec for a 12 MB file

From figures 3 and 5 we can see also that the average MB/sec for WEP, firewall and IDS is almost the same (cases 1, 2, 4). We can conclude that the effect of adding firewalls and IDS is negligible for any file size, while VPN adds extra overhead on each file.

6. Conclusions

Ad hoc wireless networks represent an important category of wireless local area networks. Their importance comes from the easy deployment and configuration in unusual conditions like places where there is an earthquake, and

where it is impossible to have a network infrastructure. Security is an important issue of ad hoc wireless networks, because they have weak built-in security mechanisms. The available security is the (WEP) mechanism, which is based on a shared secret key and can be cracked easily.

Since the main usage of the ad hoc networks is to transmit files between two wireless devices, we studied the effect of adding higher security techniques like firewall, VPN and Intrusion Detection Systems to add more security to the transmitted data. It should be noted that, these security techniques are not dedicated to wireless networks; they are used also for wired networks. We studied the impact of these additional security techniques on the time required to transfer files of different sizes. In addition, we studied the average bit rate when transmitting these files. The obtained results show that firewalls and IDS have a very little effect on the required time to transfer files of different sizes.

We recommend using WEP, firewalls and IDS in all ad hoc applications where the speed of data transmission is most important, such as conference rooms or VANET. Additionally, we recommend to use the VPN technology where the transmitted data requires a high security (like in case of military applications), because VPN tunnel encrypts the transmitted data in addition to the WEP encryption.

Table of abbreviations

BSS	Basic Service Set
ESS	Extended Service Set
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
MANET	Mobile Ad Hoc Network
VANET	Vehicle Ad Hoc Network
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WSN	Wireless Sensor Network

REFERENCES

[1] *Janice Reynolds "*Going WLAN: A practical guide to planning and building an 802.11 network", CMP Books 2003. ISBN-10: 1578203015

[2] Certified Wireless Network Associate Official Study guide, McGrew-Hill, 2nd edition, 2003

[3] IEEE 802.11, URL:http:// standards.ieee.org/getieee802/download/802.11.pdf

[4] *Kevin Tyrrell,* An over view of Wireless security issues, GSEC V1.4b SANS Institute, 2003

[5] *Jesse R. Walker*, IEEE 802.11 Wireless LAN Unsafe at any key size; an analysis of the WEP encapsulation, Oct. 27, 2000, URL:http://citeseer.ist.psu.edu/558358.html
[6] *C. Siva, B.S. Manoj* Ad Hoc networks, architecture and protocols, Prentice Hall book, 2005, ISBN-10: 1578203015.
[7] *Manu Arian*, Firewall Basics, July 2004, URL: http://www.securitydocs.com/library/2413
[8] *Mitchell Rowton*, Introduction to Network Security - Intrusion Detection, February 2005, URL: http://www.securitydocs.com/library/3009
[9] The Information Workers' Security Handbook, January 2005, URL: http:// www.secinf.net/ Network_Security/Information-Workers-Security-Handbook.html
[10] *Dan Simon, Bernard Aboba, Tim Moore*, IEEE 802.11 Security and 802.1X http://www. ieee802.org/1/files/public/docs2000/8021xSecurity.PDF
[11] *Jim Burns*, Best Practices Wireless LAN Security' URL: http:// www.mtghouse.com/ best_practices.pdf
[12] *Vijay Chandramouli*, A detailed study of wireless LAN technologies, URL: http:// crystal.uta.edu/~kumar/cse6392/termpapers/Vijay_paper.pdf#search='A%20Detailed%20Study%20on%20Wireless%20LAN%20Technologies'
[13] *Rolf Oppliger*, Internet and Intranet Security, Second edition, 2002, Artech House, ISBN: 1580531660
[14] *Ezedin Barka, Mohammed Boulmalf*, Impact of Security on the Performance of Wireless-Local Area Networks, the Proceedings of the IEEE International Conference on Innovations in IT, 2006, Dubai, UAE, November 2006
[15] *K. Agarwal, W. Wang*, Measuring Performance Impact of Security Protocols in Wireless Local Area Networks, The Second International Conference on Broadband Networks. October, 2005. Boston, Massachusetts, USA.
[16] *Vesa Kärpijoki*, Security in Ad Hoc Networks, URL: http://users.tkk.fi/~ vkarpijo/ netsec00/ netsec00_manet_sec.pdf.
[17] *H. Yang, H. Y. Luo,* Security in mobile ad hoc networks: Challenges and solutions, URL: http://www.cs.ucla.edu/~hyang/paper/WC04.pdf
[18] *Arun Kumar Bayya, Siddhartha Gupte. Yogesh Kumar Shukla, Anil Garikapati*, Security in Ad-hoc Networks, URL: http://www.geocities.com/prashthy/secure_routing_ad_hoc.html
[19] *Anil Garikapati,* IEEE 802_11tutorial, URL:http://www.ngia.rootforge.org/content/ Downloads /WiFi/HTML Pages.
[20] Connectivity _ An Overview of Connectivity Technologies, URL, http://www.idspackaging.com/ Common/Paper/Paper_357/connectiviy_whitepaper_5_21_041.pdf.