International Research Journal of Computer Science (IRJCS)
Issue 11, Volume 4 (November 2017)
ISSN: 2393-9842
www.irjcs.com

WLAN AND ITS SECURITY WITH DATA INTEGRATION AND PREVENTION OF LOSS OF DATA

S.MURUGAVALLI,
Associate Professor, Department of CSE
M.A.M School of Engineering, Tiruchirapalli, INDIA
Vallisangilimuthu2012@gmail.com;

E.PRIYANKA,
Assistant Professor, Department of CSE
M.A.M School of Engineering, Tiruchirapalli, INDIA
Splinecg11@gmail.com;

D.DEEPIKA
Assistant Professor, Department of CSE
M.A.M School of Engineering, Tiruchirapalli, INDIA
Deebi.b1992@gmail.com;

Manuscript History
Number: **IRJCS/RS/Vol.04/Issue11/NVCS10086**
DOI: 10.26562/IRJCS.2017.NVCS10086
Received: 08, October 2017
Final Correction: 27, October 2017
Final Accepted: 12, November 2017
Published: November 2017
Citation: MURUGAVALLI, PRIYANKA & DEEPIKA (2017). WLAN AND ITS SECURITY WITH DATA INTEGRATION AND PREVENTION OF LOSS OF DATA. International Research Journal of Computer Science (IRJCS), Volume IV, 23-30.
doi: 10.26562/IRJCS.2017.NVCS100086
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract- Wireless local area network (WLAN) has been widely used in many sectors. The popularity gained is due to many reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. However, regardless of the benefits mentioned above, WLAN have some security threats, in which anyone who use it or intend to use it should be aware. This paper begins by introducing the concept of WLAN. The introductory section gives brief information on the WLAN components and its architecture. In order to examine the WLAN security threats, this paper will look at Denial of Service, Spoofing, and Eavesdropping. This paper will also tell about the reasons of loss of data and the security measures that are involved to reduce the loss of data from hackers by using the data confidentiality and prevention and access control mechanism.

I. INTRODUCTION TO WLAN

In 1999, the Institute of Electrical and Electronics Engineers (IEEE) published standard 802.11, which Specified a group of technologies governing wireless Ethernet connectivity between client devices such as desktop computers, laptops, and personal digital assistants (PDAs)—and the wireless hubs connected to the physical network. Wireless LANs typically emulate the wired network's traditional hub-spoke configuration and comprise two primary components: a wireless network interface card (NIC) and an access point (AP). The 802.11 standard represents a significant step in electronic-data infrastructure evolution, which in the last ten years has proceeded from coax, token ring, and 10/100 Base T Ethernet cabling to wireless radio transmissions.

The best known and most widely used variation of the 802.11 wireless LAN standards is 802.11b. Products conforming to the 802.11b standard are called "Wi Fi" for "wireless fidelity," so named by the Wireless Ethernet Compatibility Alliance. This alliance is an independent organization that promotes interoperability between 802.11b-based devices. Under ideal conditions, Wi Fi products can receive and transmit data at speeds up to 11 Megabits per second (Mbps). However, in typical conditions, most Wi Fi devices operate at speeds between 1 and 5 Mbps.

II. WLAN COMPONENTS

One important advantage of WLAN is the simplicity of its installation. Installing a wireless LAN system is easy and can eliminate the needs to pull cable through walls and ceilings. The physical architecture of WLAN is quite simple. Basic components of a WLAN are access points (APs) and Network Interface Cards (NIC).

2. A) Access Points

Access Point (AP) is essentially the wireless equivalent of a LAN hub. It is typically connected with the wired backbone through a standard Ethernet Cable, and communicates with wireless devices by means of an antenna. An AP operates within a specific frequency spectrum and uses 802.11 standard specified modulation techniques. It also informs the wireless clients of its availability, and authenticates and associates wireless clients to the wireless network.

2.b)Network Interface Card:

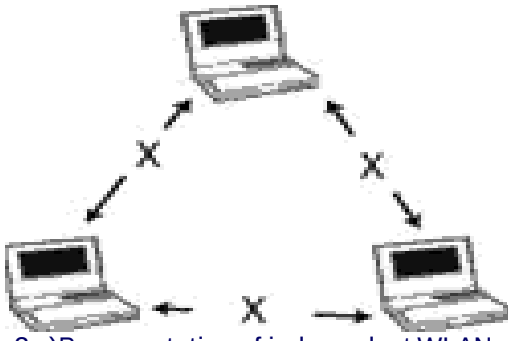
Wireless client adapters connect PC or workstation to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with APs Available in PCMCIA (Personal Computer Memory Card International Association) card and PCI (Peripheral Component Interconnect), it connects desktop and mobile computing devices wirelessly to all network resources. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client. It is coupled to the PC/workstation operating system using a software driver. The NIC enables new employees to be connected instantly to the network and enable Internet access in conference.

III.WLAN ARCHITECTURE

The WLAN components mentioned above are connected in certain configurations. There are three main types of WLAN architecture: Independent, Infrastructure, and Microcells and Roaming.

3.a) Independent WLAN

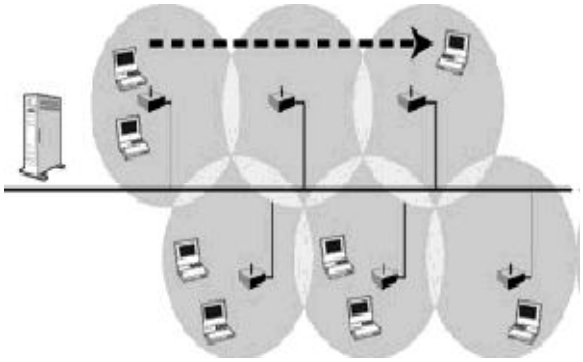
The simplest WLAN configuration is an independent (or peer-to-peer) WLAN. It is a group of computers, each equipped with one wireless LAN NIC/client adapter. In this type of configuration, no access point is necessary and each computer in the LAN is configured at the same radio channel to enable peer-to-peer networking. Independent networks can be set up whenever two or more wireless adapters are within range of each other.



3.a)Representation of independent WLAN

3.b) Infrastructure WLAN

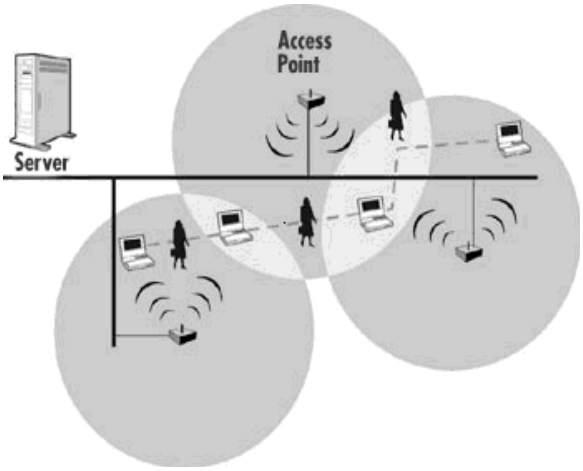
Infrastructure WLAN consists of wireless stations and access points. Access Points combined with a distribution system (such as Ethernet) support the creation of multiple radio cells that enable roaming throughout a facility. The access points not only provide communications with the wired network but also mediate wireless network traffic in the immediate neighborhood. This network configuration satisfies the need of large-scale Networks arbitrary coverage size and complexities



3. b) Representation of infrastructure WLAN

3.c) Microcells and Roaming

The area of coverage for an access point is called a "microcell'. The installation of multiple access points is required in order to extend the WLAN range beyond the coverage of a single access. One of the main benefits of WLAN is user mobility. Therefore, it is very important to ensure that users can move seamlessly between access points without having to log in again and restart their applications. Seamless roaming is only possible if the access points have a way of exchanging information as a user connection is handed off from one access point to another. In a setting with overlapping microcells, wireless nodes and access points frequently check the strength and quality of transmission. The WLAN system hands off roaming users to the access point with the strongest and highest quality signal, in accommodating roaming from one microcell to another.



3. c) Representation of microcells and roaming

IV. EXISTING MODEL:

Security in WLAN:

4.a) Denial of Service

In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission, the WLAN are very vulnerable against denial of service attacks. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to denial of service attacks. By using a powerful enough transceiver, radio interference can easily be generated that would enable WLAN to communicate using radio path.

4.b) Session Hijacking

This is where the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This happens because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. Attackers may therefore spoof MAC addresses and hijack sessions. Moreover, 802.11 do not require an Access Point to prove it is actually an AP. This facilitates attackers who may masquerade as AP's. In eliminating spoofing, proper authentication and access control mechanisms need to be placed in the WLAN.

4.c) Eavesdropping

This involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of the company.

V. WIRED EQUIVALENT PRIVACY

Wired Equivalent Privacy (WEP) is a standard encryption for wireless networking. It is a user authentication and data encryption system from IEEE 802.11 used to overcome the security threats. Basically, WEP provides security to WLAN by encrypting the information transmitted over the air, so that only the receivers who have the correct encryption key can decrypt the information. The following section explains the technical functionality of WEP as the main security protocol for WLAN.

WEP uses a pre-established shared secret key called the base key, the RC4 encryption algorithm and the CRC-32 (Cyclic Redundancy Code) checksum algorithm as its basic building blocks. WEP supports up to four different base keys, identified by Key IDs 0 thorough 3. Each of these base keys is a group key called a default key, meaning that the base keys are shared among all the members of a particular wireless network. Some implementations also support a set of nameless per-link keys called key-mapping keys.

WEP tries to achieve its security goal in a very simple way. It operates on MAC Protocol Data Units (MPDUs), the 802.11 packet fragments. To protect the data in an MPDU, WEP first computes an integrity check value (ICV) over to the MPDU data. This is the CRC-32 of the data. WEP appends the ICV to the end of the data, growing this field by four bytes. The ICV allows the receiver to detect if data has been corrupted in flight or the packet is an outright forgery. Next, WEP selects a base key and an initialization vector (IV), which is a 24-bit value. WEP constructs a per-packet RC4 key by concatenating the IV value and the selected shared base key. WEP then uses the per-packet key to RC4, and encrypt both the data and the ICV. The IV and Key ID identifying the selected key are encoded as a four-byte string and pre-pended to the encrypted data. The IEEE 802.11 standard defines the WEP base key size as consisting of 40 bits, so the per-packet key consists of 64 bits once it is combined with the IV. Many in the 802.11 community once believed that small key size was a security problem, so some vendors modified their products to support a 104-bit base key as well. This difference in key length does not make any different in the overall security. An attacker can compromise its privacy goals with comparable effort regardless of the key size used.

VI. DRAWBACKS OF WEP

(i) No forgery protection

There is no forgery protection provided by WEP. Even without knowing the encryption key, an adversary can change 802.11 packets in arbitrary, undetectable ways, deliver data to unauthorized parties, and masquerade as an authorized user. Even worse, an adversary can also learn more about the encryption key with forgery attacks than with strictly passive attacks.

(ii) No protection against replays

WEP does not offer any protection again replays. An adversary can create forgeries without changing any data in an existing packet, simply by recording WEP packets and then retransmitting later. Replay, a special type of forgery attack, can be used to derive information about the encryption key and the data it protects.

(iii) Reusing initialization vectors

By reusing initialization vectors, WEP enables an attacker to decrypt the encrypted data without the need to learn the encryption key or even resorting to high-tech techniques. While often dismissed as too slow, a patient attacker can compromise the encryption of an entire network after only a few hours of data collection.

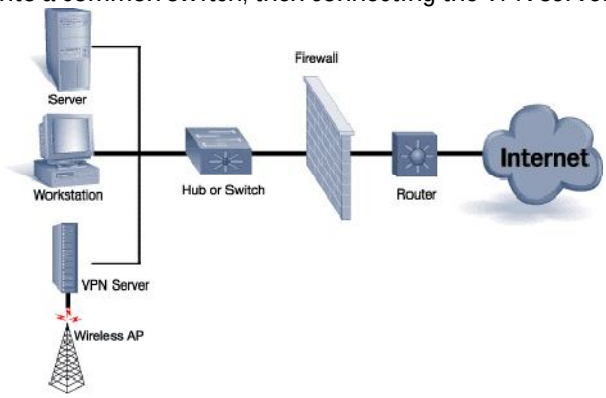
VII. PROPOSED METHODOLOGY

(i) Changing Default SSID:

Service Set Identifier (SSID) is a unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to a particular WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. In fact, it is the only security mechanism that the access point requires to enable association in the absence of activating optional security features. Not changing the default SSID is one of the most common security mistakes made by WLAN administrators. This is equivalent to leaving a default password in place.

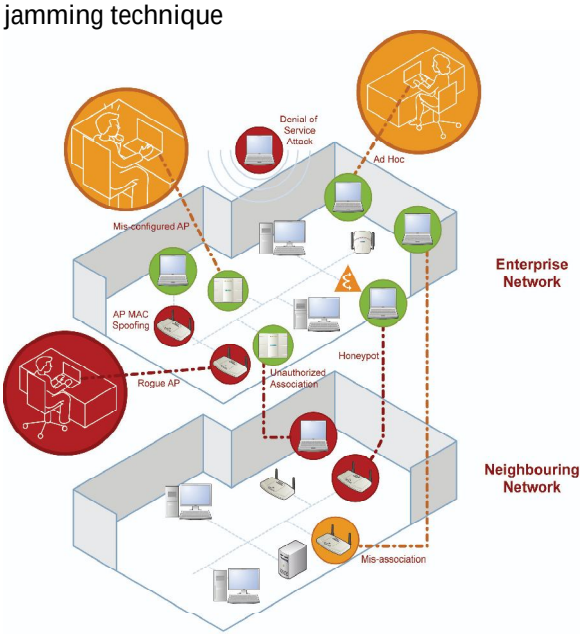
(ii) Utilize VPN

A VPN is a much more comprehensive solution in a way that it authenticates users coming from an untrusted space and encrypts their communication so that someone listening cannot intercept it. Wireless AP is placed behind the corporate firewall within a typical wireless implementation. This type of implementation opens up a big hole within the trusted network space. A secure method of implementing a wireless AP is to place it behind a VPN server. This type of implementation provides high security for the wireless network implementation without adding significant overhead to the users. If there is more than one wireless AP in the organization, it is recommended to run them all into a common switch, then connecting the VPN server to the same switch.



Minimize radio wave propagation in non-user areas

Try orienting antennas to avoid covering areas outside the physically controlled boundaries of the facility. By steering clear of public areas, such as parking lots, lobbies, and adjacent offices, the ability for an intruder to participate on the wireless LAN can be significantly reduced. This will also minimize the impact of someone disabling the wireless LAN with jamming technique



To be effective, WLAN security must address three critical areas;

- Data Confidentiality and Integrity
- Authentication and Access Control, and
- Intrusion Detection and Prevention

(iii) Mis-Configured Access Points:

Just as dangerous as an unauthorized "rogue" access point is an access point that has been legitimately connected to the wired network, but improperly or insufficiently configured. For instance, if no security settings were configured, then such an access point would provide open network access to anyone.

(iv) Ad Hoc Wireless Networks:
Operating systems like Windows allow the creation of networks consisting of multiple wireless clients, without an access point in between. If one of these computers is configured to participate in an ad hoc network as well as connect to the corporate WLAN via an access point, they could be inadvertently creating an opening for a hacker to exploit.

(v) Client Mis-associations:
In cases where companies are physically near one another, it is very possible for two wireless networks to have the same network information. In such a case, a wireless client will associate with the first access point that it contacts, and if it belongs to the neighboring WLAN, a security threat can exist.

(vi) Rogue access points:
An unauthorized access point that has been connected to the wired network, which can provide malicious or unauthorized users with open access to the LAN.

(vii) Honey pot APs:
Some hackers will be able to determine the configuration settings of the wireless LAN, and will plant an access point with the same settings within range of the network. Through mis-association, clients can connect to these honey pots assuming that they are legitimate. Clever hackers can then exploit this by connecting decoy network resources to the AP so that users login, after which the hacker can steal passwords or even confidential documents.

(viii) AP MAC Spoofing:
Wireless client computers can be configured to behave like legitimate participants in the network. In this manner, a hacker can mimic an authorized user or even act as a honey pot AP.

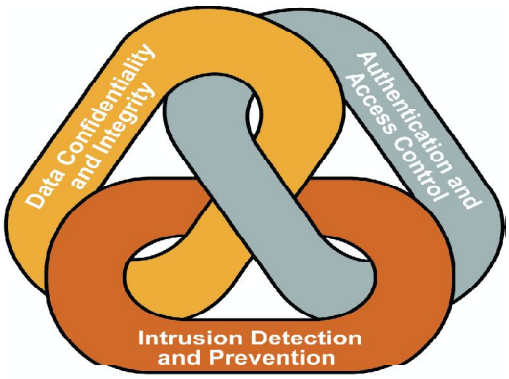
(ix) Unauthorized Client Access:
If a network has a weak user authentication Hackers continually probe areas for open wireless scheme – or none at all – it is very easy for a hacker to obtain access to the corporate network and take information or launch attacks on resources in order to cause disruptions.

(x) Denial of Service (DoS):
Because of the way networking devices work, they need to respond to any client requests. Hackers are able to exploit this by inundating a network resource with more requests than it is able to handle. Distributed DoS attacks magnify this problem by enlisting a number of unknowing computers through hidden code to simultaneously launch denial of service attacks on a potentially massive scale.

(xi) Man in the Middle:
If data is unprotected, hackers can intercept messages and change the content to mislead parties that are communicating, making it seem as if the hacker is actually one of the parties.

(xii) IP Spoofing:
By modifying the source IP address contained in the packet header, a hacker can intercept traffic coming from a legitimately authenticated user and make it appear that the user is actually using the hacker's computer. As a result, all data and messages coming from a server would go back to the hacker.

VIII.SECURITY IN WLAN

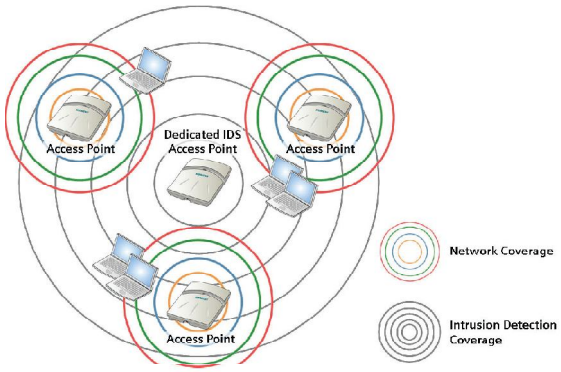


An effective WLAN security policy should:

- Identify who may use WLAN technology and what type of access is required,
- Describe who can install access points and other wireless infrastructure equipment,
- Describe the type of information that can and cannot be sent over wireless links,
- Describe conditions under which wireless devices are allowed and how they may be used,
- Describe the hardware and software configuration for any access device,
- Provide guidelines on reporting losses of wireless devices and security incidents,
- Provide guidelines on the use of encryption and other security software; and,
- Define the frequency and scope of security assessments, audits and report generation

8. A) Intrusion Detection and Prevention:

Data confidentiality and authentication are addressed through industry standards, but no standards exist for wireless intrusion detection and prevention (WIDS/WIPS). Instead, WLAN equipment vendors and/or specialty wireless security vendors provide enterprise WIDS/WIPS solutions. Different vendors implement WIDS in their own way, but the basic principles and required equipment are the same. All WIDS systems need; remote sensors distributed throughout the monitored network, and management software often called an IDS server. When the system is initially deployed, a detailed description of the network is programmed into the IDS server as a baseline. In a WIDS solution sensors passively observe wireless activity and network configuration, reporting any exception back to the central IDS server. That IDS server is responsible for analyzing reported activity, generating intrusion alarms and an event log. WIPS solutions take this information and act upon it directly, without requiring manual intervention, by sending disassociation commands to the client, they effectively disconnecting any access to identified threats such as rogue or honey-pot APs. A WIPS solution needs to be chosen with care. Many solutions not only fail to detect many types of threats, but can also deliver false positive detections. This false positive, can cause unnecessary effort for the IT security team but can also lead to a general distrust of the identification of real threats and thus complacency.



WIDS/WIPS solutions can function in one of two different modes – time slicing or always on. These two modes offer varying degrees of security for the enterprise. In a time slicing mode the WIPS solution does not require dedicated sensors distributed throughout the enterprise, but rather "borrows" slices of time from existing access points to take a snap shot listen of the environment. This mode offers the advantage of lower cost security to the enterprise but also offers a lower level of security. Sophisticated hacking routines have been known to identify listening patterns and intersplice their activities between the listening slots, effectively going undetected. This is similar to the escaping prisoner avoiding the searchlight and thus going undetected.

The more costly, but more effective mode, is to use dedicated sensors on full time listening mode to detect (and with WIPS prevent) threats. This is the equivalent of leaving all the lights on, so no matter when the prisoner attempts to escape, he will be seen. Both modes offer their benefits and can even be used at the same time in different physical parts of the enterprise (depending on risks of say visitor or customer traffic). A well thought out plan and risk assessment is needed when deciding how to best implement WIPS for an enterprise.

Enterprises generally have two alternatives when deploying intrusion detection and prevention solutions. The first is to deploy an "overlay" solution, which is a specialized network of dedicated equipment completely separate from the WLAN. These solutions tend to provide the most comprehensive security and the best performance. However, overlay solutions have the disadvantages of adding operational complexity and cost, forcing the deployment of two wireless networks with no management integration or hardware economies. The other alternative is to accept the integrated IDS/IPS functionality which most WLAN infrastructure vendors offer with their solution. The problem with this alternative is that what the IDS solution vendors offer is generally inferior to over-lay products, if not in features then certainly in performance. WLAN Vendors are now starting to address this discrepancy.

For example, Siemens has fully integrated the industry leading Airtight WIPS solution into its Hi Guard product; deliver world-class WIPS security along with the benefit of reduced overhead and maintenance associated with an overlay solution.

IX. CONCLUSION

The general idea of WLAN was basically to provide a wireless network infrastructure comparable to the wired Ethernet networks in use. It has since evolved and is still currently evolving very rapidly towards offering fast connection capabilities within larger areas. However, this extension of physical boundaries provides expanded access to both authorized and unauthorized users that make it inherently less secure than wired networks. Wireless Networks do offer an additional physical layer of security when deployed in an all wireless office environment. By effectively eliminating employee or guest physical access to the network elements – jacks and cables – the hidden network becomes more physically secure. Employees can no longer plug in access points from home, guests can't erroneously misconnect LAN connections in a board room while trying to secure external access. The securing of the WLAN has become an enabler of the all-wireless future.

REFERENCES

1. Air Defense™, Inc. "Wireless LAN Security: Intrusion Detection and Monitoring for the Enterprise." 4 Dec. 2002. http://www.airdefense.net/products/index.shtml (30 Oct. 2002)
2. Borisov, Nikita, Goldberg, Ian and Wagner, David. "Security of the WEP Algorithm." 13 Dec. 2002. URL: http://www.isaac.cs.berkeley.edu/isaac/wepfaq. html (3 Dec. 2002).
3. Computer Security Research Centre, National Institute of Standards and Technology. "Announcing the Advanced Encryption Standard (AES)."Federal Information Processing Standards Publications 197. 13 Dec. 2002. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (3 Dec. 2002).
4. Eaton, Dennis." Diving into the 802.11i Spec: A Tutorial." 3 Jan. 2003. URL: http://www.commsdesign.com/design_corner/OEG20021126S0003 (18 Dec.2002).
5. Geier, Jim. "Guarding Against WLAN Security Threats." 2 Dec. 2002. URL: http://www.80211-planet.com/tutorials/article.php/1462031 (28 Oct. 2002).
6. Geier,Jim."802.11 Security Beyond WEP". 2 Dec. 2002. URL: http://www.80211 planet.com/tutorials/article.php/1377171 (28 Oct. 2002).
7. IBM Corporation. "Wireless Security Auditor (WSA)." 4 Dec. 2002. URL: http://researchweb.watson.ibm.com/gsal/wsa/ (30 Oct. 2002).
8. Isomair.com. "Isomair Security for Wireless World" 4 Dec. 2002. URL: http://www.isomair.com/products.html (30 Oct. 2002).
9. Knowledge Systems (UK) Ltd. "Wireless LAN Security Issues." 2 Dec. 2002. URL: http://www.ksys.info/wlan_security_issues.html (28 Oct. 2002).

