

# **WIRELESS NETWORK TECHNOLOGIES IN TRANSPORT AREA: SECURITY AND E-LEARNING APPLICATIONS**

T.Rikure, A.Jurenoks

*Wireless technologies, security, wireless enabled teaching, application, IEEE 802.11b specification, LAN*

## **Abstract**

A wireless LAN is a method of linking computers together without using cables, but using radio signals or infrared light instead. This paper discusses the issues involved in determining whether a wireless LAN is appropriate for any institution (or part of an institution) including transport area enterprises, and the issues involved in implementing a wireless LAN. It also looks at the educational opportunities that the use of wireless LANs presents for these institutions, and covers the pedagogical, technical and security issues that wireless LANs raise.

## **Introduction**

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Risks are inherent, however, in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. This article provides an overview of wireless networking technologies most commonly used today, outlines the associated risks, and offers guidance for mitigating those risks.

Wireless technologies have become increasingly popular in our everyday business and personal lives. Cell phones offer users a freedom of movement unimaginable just over 10 years ago. Personal Digital Assistants (PDA) allow individuals to access calendars, e-mail, address and phone number lists, and the Internet. Some technologies even offer global positioning system (GPS) capabilities that can pinpoint the location of the device anywhere in the world. Wireless technologies promise to offer even more features and functions in the next few years.

An increasing number of government agencies, businesses, and home users are using, or considering using, wireless technologies in their environments. However, these groups need to be aware of the security risks associated with wireless technologies. They need to develop strategies that help mitigate those risks as they integrate these technologies in their computing environments.

## **IEEE 802.11b**

Wireless technologies enable one or more devices to communicate without physical connections – without requiring network cabling. Wireless technology aims to provide users access to information anywhere – it allows mobility.

Wireless Local Area Networks (WLAN) are often implemented as an extension to wired LANs within a building and can provide the final few meters of connectivity between a wired network and the mobile user. WLANs are based on the IEEE 802.11 standard [9]. The IEEE designed 802.11 to support medium-range, higher data rate

applications, such as Ethernet networks, and to address mobile and portable stations [2]. 802.11 is the original WLAN standard, designed for 1Mbps to 2Mbps wireless transmissions (table 1 shows comparison of 802.11 standards). The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications.

1. Table

Comparison of 802.11 standards

	<b>802.11b</b>	<b>802.11a</b>	<b>802.11g</b>
Frequency	2.4GHz	5GHz	2.4GHz
Speed	11Mbps	54Mbps	54Mbps
Accessibility	Worldwide	US	Worldwide

### Wireless Security Threats

Data security is a major issue for wireless due to the nature of the transmission mechanism (electromagnetic signals passing through the air). Threats can be classified into nine categories [10]:

- errors and omissions;
- fraud and theft committed by authorized or unauthorized users of the system;
- employee sabotage;
- loss of physical and infrastructure support;
- malicious hackers;
- industrial espionage;
- malicious code;
- foreign government espionage;
- threats to personal privacy.

These threats, if successful, place an organization's systems - and, more importantly, its data - at risk. Ensuring confidentiality, integrity, and network availability are (or should be) prime objectives of all government security policies and practices. Risks in wireless networks are equal to the sum of the risk of operating a wired network (as in operating a network in general) plus the new risks introduced by weaknesses in wireless protocols. The list below represents some of the more salient threats and vulnerabilities of wireless systems [10]:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an organization's computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.

- Viruses or other malicious code may corrupt data on a wireless device and be introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other organizations for the purposes of launching attacks and concealing their activity.
- Interlopers, from insider or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

## Security of 802.11 Wireless LANS

The IEEE 802.11b specification identified several services to provide a secure operating environment. The security services are provided largely by the WEP (Wired Equivalent Privacy) protocol to protect link-level data during wireless transmission between clients and access points. That is, WEP does not provide end-to-end security but only for the wireless portion of the connection. Security for the radio path is depicted in Figure 1.

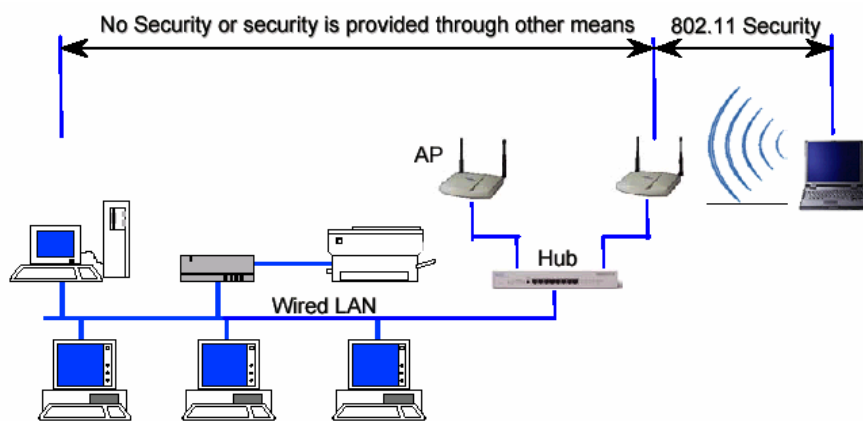


Figure 1. Wireless Security of 802.11b in Typical Network.

The IEEE 802.11b specification defines two means to validate wireless users attempting to gain access to the wired network, as depicted previously. One means is based on cryptography and the other is not. For the non-cryptographic approach, there are essentially two different ways to identify a wireless client attempting to join a network. However, both of these approaches are identity-based verification mechanisms. The wireless stations requesting access simply respond with the Service Set Identifier (SSID) of the wireless network - there is no true "authentication." The two ways are referred to as Open System authentication and Closed System authentication. Taxonomy of the techniques for 802.11b is depicted in Figure 2.

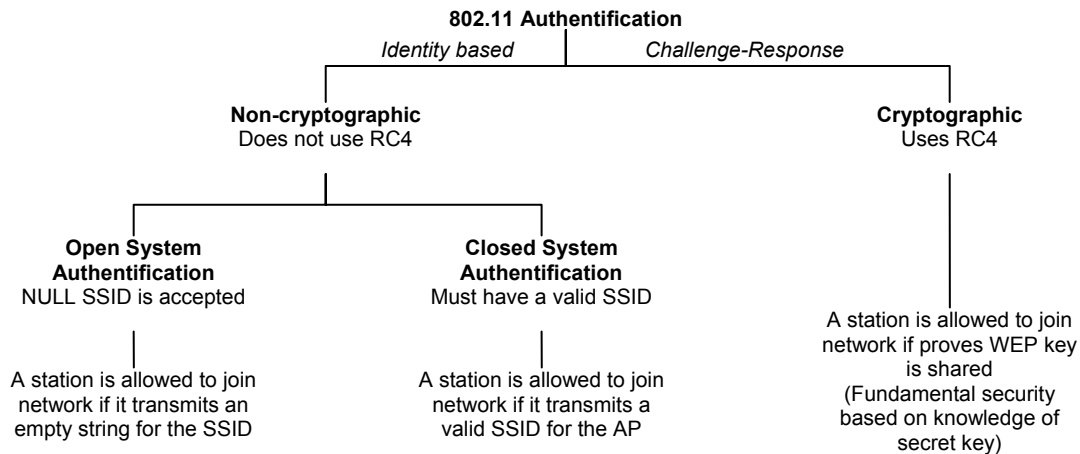


Figure 2. Taxonomy of 802.11b Authentication Techniques.

With Open System, a client is authenticated if it simply responds with an empty string for the SSID (Service Set Identifier) – hence, the name “NULL authentication”. With the second method, Closed Authentication, wireless clients must respond with the actual SSID of the wireless network. That is, a client is allowed access if it responds with the correct 0-byte to 32-byte string identifying the BSS of the wireless network. Again, this primitive type of authentication is only an identification scheme. Practically speaking, neither of these two schemes offers robust security against unauthorized access. To reiterate, both Open and Closed Authentication schemes are highly vulnerable to attacks – against even the most novice adversaries – and without enhancements, they practically invite security incidents.

Shared key authentication is a cryptographic technique for authentication. It is a simple “challenge-response” scheme based on whether a client has knowledge of a shared secret. In this scheme, as depicted in Figure 3, a random challenge is generated by the access point and sent to the wireless client. The client, using a cryptographic key (WEP key) that is shared with the AP, encrypts the challenge (or “nonce”, as it is called in security vernacular) and returns the result to the AP. The AP decrypts the result computed by the client and allows access only if the decrypted value is the same as the random challenge transmitted. The algorithm used in the cryptographic computation is the RC4 stream cipher developed by Ron Rivest of MIT. It should be noted that the authentication method just described is a rudimentary cryptographic technique, and it does not provide mutual authentication. That is, the client does not authenticate the AP and therefore there is no assurance that a client is communicating with a legitimate AP, and wireless network. It is also worth noting that simple unilateral challenge-response schemes have long been known to be weak. They suffer from numerous attacks including the infamous “man-in-the-middle” attack.

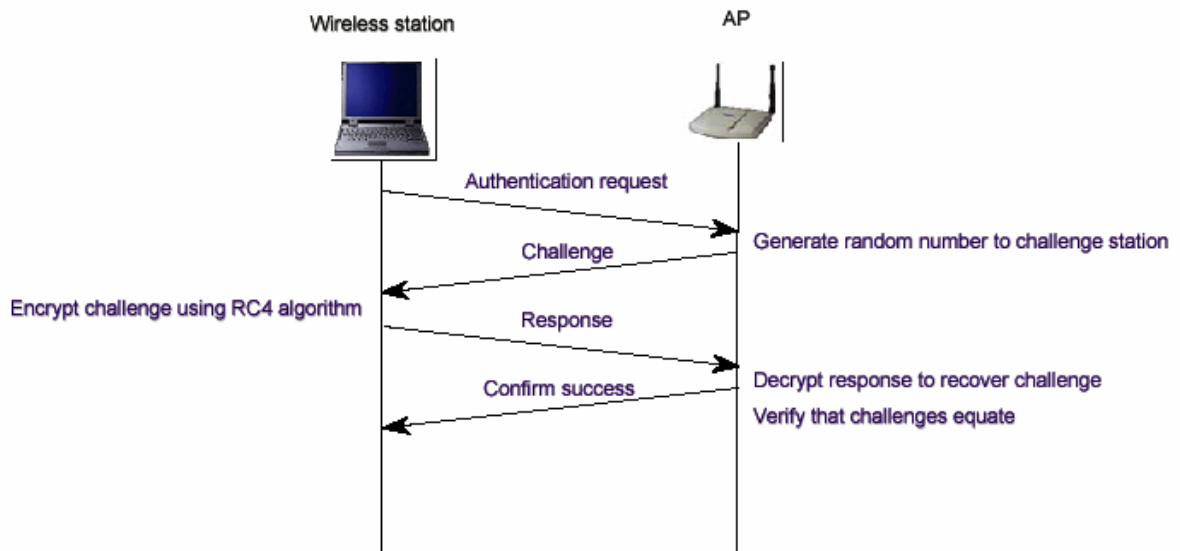


Figure 3. Shared-key Authentication Message Flow.

### Wireless enabled teaching

Wireless LANs provide great flexibility, especially in conjunction with laptops because between them they allow computers to be used anywhere. The computers go to the teaching rather than the teaching to the computers so that anywhere - including laboratories, classrooms and even outdoors - can be used to teach with computers.

This has several advantages. Firstly, as already suggested the computer can be used where the teacher wants. Secondly, laptops used where they are needed not where they happen to have been installed or can be plugged in are much less intrusive into the rest of the teaching. Thirdly, it allows more efficient use of resources because computers can be used in the number needed - not the number that have been installed in a room, and special rooms do not need to be set aside for when computers are needed in teaching and training. So a wireless network enables you to create a more dynamic and cost efficient architecture to support the rapid changes and flexible management.

Implementation of wireless LAN support for training rooms is beginning to be considered a part of normal operations at many enterprises and institutions. In general, wide range institutions are better positioned to make use of wireless technology. Employees have better access to personal computers and the internet, and the institutions generally have a stronger technology infrastructure and support staff available to them.

Security is a tough challenge these days in any IT environment. In any enterprise keeping data and systems secure is even tougher. That's true for several reasons: learning environments encourage open atmospheres that are conducive to security vulnerabilities; funds and personnel are usually spread thin; and many enterprises run heterogeneous environments with a range of hardware and software, some owned by the institution, some by employees. Adding wireless to the mix, as many enterprises now have done, compounds the problem. The challenge is to lock down the institutions environment even under those conditions - while keeping all constituents reasonably happy with their access to information and services.

### Conclusions

Wireless LANs have an important part to play in the development of IT infrastructure in transport area institutions over the next few years. It will be especially important for those enterprises which are in the process of extending the reach of their network, whether this is to increase the area covered by the network or to improve availability to employees and other users. Wireless LANs are likely to be the most cost effective way of extending the reach of the institution network both to new areas and to increase the number of people who can be using it simultaneously. Cost savings are likely to be especially great in areas that are hard to wire because of the nature of the existing buildings, this includes listed buildings where permission to put the wiring in can be difficult and the controls on where it can go make it even more expensive. Also, buildings with asbestos or reinforced walls can be very difficult to wire and here wireless LANs can be especially beneficial.

Besides the economic advantages wireless LANs also provide for greater flexibility than wired LANs for three reasons:

1. They provide physical flexibility in that it does not matter where within the space the user is working they are still able to use the network. With a wired network it is necessary to decide where computers will be used and install the ports there. Often the use of space changes with time, and then either the space has to be rewired or long trailing cables are used to get from the computer to the port.
2. With a wired network the maximum number of users has to be determined when the space is wired and a suitable number of ports installed. This tends to mean either that too many ports are installed, so wasting money, or that there are times when demand exceeds supply and some users are unable to use the network. With a wireless network the performance of the network will deteriorate as the usage increases but unless there is very high demand all users will be able to access the network.
3. The network can reach places that wired networks cannot, this includes out of doors where up to several hundred meters from buildings the signal can be reached. Also, it is relatively easy to set up an access point linked back to the organization network for use in remote premises.

Wireless LANs can be especially useful in training rooms as these are constantly being re-arranged for different purposes - for training in one session and then for actual work in another. This is not possible if the desks are wired as they then have to be secured to the floor. With wireless LANs this issue does not arise. Institutions which are looking at employees' ownership and use of laptop PCs and personal digital assistants (PDAs) need to find ways to provide access to the internet for employees' own machines. Wireless LANs are an easy way to manage this.

There are a number of problems with wireless LANs as well. The three most significant are the security, the rapid evolution of the technical standards and the sharing of bandwidth so that the available bandwidth will be much lower than for wired networks.

Wireless LAN is a relatively young technology and we are only just beginning to find the educational advantages that it can offer, either with or without ubiquitous computing. It is already clear that there are a number of things that it enables including better collaborative working among learners.

In conclusion then, wireless LANs will have a growing place in the IT infrastructure of institutions in transport area over the next few years and enterprises will begin to make use of it to enhance their employees knowledge level.

## References:

1. Wheat J., Hiser R., Tucker J., Neely A. and McCullough A. Designing a Wireless Network. Syngress Publishing, Inc., 2001.

2. Barnes Ch., Bautts T., Lloyd D., Ouellet E., Posluns J., Zendzian D. M. and O'Farrell N. Hack Proofing your Wireless Network. Syngress Publishing, Inc., 2002
3. Flickenger R. Building Wireless Community Networks. O'Reilly, 2002.
4. Basgall M. Experimental Break-Ins Reveal Vulnerability in Internet, Unix Computer Security. <http://www.dukenews.duke.edu/research/encrypt.html>, 1999.
5. Cardwell A. and Woollard S. Clinic: What are the biggest security risks associated with wireless technology? What do I need to consider if my organization wants to introduce this kind of technology to my corporate LAN?, [www.itsecurity.com](http://www.itsecurity.com), 2001.
6. Marek S. Identifying the Weakest Link. Wireless Internet Magazine, [www.wirelessinternetmag.com](http://www.wirelessinternetmag.com), 2001.
7. Jackson R.H. Defining e-Learning – different shades of “Online”, 2003.
8. Collier G. E-learning application infrastructure. Sun Microsystems Inc., 2002.
9. 3Com, 11 Mbps Wireless LAN Access Point 6000 User Guide. Version 2.0., 2001.
10. The NIST Handbook, Special Publication 800-12, An Introduction to Computer Security.
11. The NIST Handbook, Special Publication 800-30, Risk Management Guide for IT Systems.
12. ZDNet India Magazine website – provides white papers, surveys, and reports on wireless network security, [www.zdnetindia.com](http://www.zdnetindia.com)
13. SC Magazine website, an information security online magazine – provides information on wireless security issues, [www.scmagazine.com](http://www.scmagazine.com)
14. SANS Institute website – maintains articles, documents, and links on computer security and wireless technologies, [www.sans.org/newlook/home.htm](http://www.sans.org/newlook/home.htm)
15. Network World Fusion website – provides white papers, surveys, and reports on wireless network security, [www.nwfusion.com](http://www.nwfusion.com)
16. NIST, Computer Security Resource Center, <http://csrc.nist.gov/publications>

**Tatiana Rikure**, Riga Technical University, Division of Applied Systems Software, Meza 1/3, Riga, LV 1048, Latvia, PhD student, [rikure@cs.rtu.lv](mailto:rikure@cs.rtu.lv)

Tatiana Rikure is a master of science in computer science (MSCS). Now she is a PhD student at RTU Division of Applied Systems Software. She is a researcher in mobile and e-learning, Intelligent Tutoring Systems, web technologies and security. She is an author of three educational books and many instructional materials for teaching different courses in the computer science field. Now she takes part in IST 6FP project IST4Balt (Information Society Technologies Promotion in Baltic States).

**Alexey Jurenoks**, Riga Technical University, Division of Applied Systems Software, Meza 1/3, Riga, LV 1048, Latvia, PhD student, [alex@eskola.lv](mailto:alex@eskola.lv)

Alexey Jurenoks is a master of science in computer science (MSCS). Now he is a PhD student at RTU Division of Applied Systems Software. He is a researcher in wireless technologies, mobile learning, and web technologies. He is an author of four educational books and many instructional materials for teaching different courses in the computer science field. Now he takes part in IST 6FP project eLONGMAR-M (Web-based and Mobile Solutions for Collaborative Work Environment with Logistics and Maritime Applications).