

# An approach to WLAN Security

Satish Khatak\*, Parveen Singhal\*\*, Kamal Sardana\*\*\*  
Email: khatak1977@yahoo.co.in  
singhal.parveensinghal@rediff.com  
sardanakamal@indiatimes.com

## Abstract

*802.11b's low cost of entry is what makes it so attractive. However, inexpensive equipment also makes it easier for attackers to mount an attack. "Rogue" access points and unauthorized, poorly secured networks compound the odds of a security breach. The 802.11b standard shares unlicensed frequencies with other devices, including Bluetooth wireless personal area networks (PANs), cordless phones, and baby monitors. These technologies can, and do, interfere with each other. 802.11b also fails to delineate roaming leaving each vendor to implement a different solution. An approach to WLAN security using Pseudo Random codes promises to address such shortcomings.*

## 1. Introduction

Wireless LANs based on the 802.11 standard are the most likely candidate to become widely prevalent in corporate environments. Current 802.11b products operate at 2.4GHz, and deliver up to 11Mbps of bandwidth comparable to a standard Ethernet wired LAN in performance. The 802.11b standard shares unlicensed frequencies with other devices, including Bluetooth wireless personal area networks (PANs), cordless phones, and baby monitors. Security management administrators do not yet recognize wireless LANs as an approved technology. This paper focuses on the risk issues from a corporate network perspective; these same issues apply to home networks, telecommuters using wireless, and "public use" networks such as those being set up by Microsoft to allow wireless Internet access at select Starbucks locations. Remote users are now able to access internal corporate resources from multiple types of foreign networks. Even organizations without internal wireless networks must take wireless into account as part of their overall security practices.

## 2. Threats

Although attacks against 802.11b and other wireless technologies will undoubtedly increase in number and sophistication over time, most current 802.11b risks fall into seven basic categories:

- **Insertion attacks**
- **Interception and unauthorized monitoring of wireless traffic**

- **Jamming**
- **Client-to-Client attacks**
- **Brute force attacks against access point passwords**
- **Encryption attacks**
- **Misconfiguration**

These classifications can apply to any wireless technology, not just 802.11b. Understanding how they work and using this information to prevent their success is a good stepping stone for any wireless solution.

### 2.1 Insertion Attacks

Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review.

#### 2.1.1 Unauthorized Clients

An attacker who connect to an access point without authorization. Access points can be configured to require a password for client access. If there is no password, an intruder can connect to the internal network simply by enabling a wireless client to communicate with the access point.

#### 2.1.2 Unauthorized or Renegade Access Points

An organization may not be aware that internal employees have deployed wireless capabilities on their network. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources through a rogue access point. Organizations need to implement policy to ensure secure configuration of access points, plus an ongoing process in which the network is scanned for the presence of unauthorized devices.

### 2.2 Interception and Monitoring of Wireless Traffic

As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be within range of an access point (approximately 300 feet for 802.11b) for this attack to work, whereas a wired attacker can be anywhere where there is a functioning network connection. The advantage for a wireless interception is that a wired attack requires

the placement of a monitoring agent on a compromised system. All a wireless intruder needs is access to the network data stream. There are two important considerations to keep in mind with the range of 802.11b access points. First, directional antennae can dramatically extend either the transmission or reception ranges of 802.11b devices. Therefore, the 300 foot maximum range attributed to 802.11b only applies to normal, as-designed installations. Second, access points transmit their signals in a circular pattern, which means that the 802.11b signal almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings, or even through floors in multistory buildings. Careful antenna placement can significantly affect the ability of the 802.11b signal to reach beyond physical corporate boundaries.

### **2.2.1 Wireless Packet Analysis**

An attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of these tools capture the first part of the connection session, where the data would typically include the username and password. An intruder can then masquerade as a legitimate user by using this captured information to hijack the user session and issue unauthorized commands.

### **2.2.2 Broadcast Monitoring**

If an access point is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcasted out over the wireless network. Because the Ethernet hub broadcasts all data packets to all connected devices including the wireless access point, an attacker can monitor sensitive data going over wireless not even intended for any wireless clients.

### **2.2.3 Access Point Clone Traffic Interception**

An attacker fools legitimate wireless clients into connecting to the attacker's own network by placing an unauthorized access point with a stronger signal in close proximity to wireless clients. Users attempt to log into the substitute servers and unknowingly give away passwords and similar sensitive data.

## **2.3 Jamming**

Denial of service attacks are also easily applied to wireless networks, where legitimate traffic cannot reach clients or the access point because illegitimate traffic overwhelms the frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, corrupting the signal until the wireless network ceases to function. Devices operating on the 2.4 GHz band can disrupt a

wireless network using this frequency. These denials of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

## **2.4 Client-to-Client Attacks**

Two wireless clients can talk directly to each other, bypassing the access point. Users therefore need to defend clients not just against an external threat but also against each other.

### **2.4.1 File Sharing and Other TCP/IP Service Attacks**

Wireless clients running TCP/IP services such as a Web server or file sharing are open to the same exploits and misconfigurations as any user on a wired network.

### **2.4.2 DOS (Denial of Service)**

A wireless device floods other wireless client with bogus packets, creating a denial of service attack. In addition, duplicate IP or MAC addresses, both intentional and accidental, can cause disruption on the network.

## **2.5 Brute Force Attacks Against Access Point Passwords**

Most access points use a single key or password that is shared with all connecting wireless clients. Brute force dictionary attacks attempt to compromise this key by methodically testing very possible password. The intruder gains access to the access point once the password is guessed.

## **2.6 Attacks against Encryption**

802.11b standard uses an encryption system called WEP (Wired Equivalent Privacy). WEP has known weaknesses, and these issues are not slated to be addressed before 2002. Not many tools are readily available for exploiting this issue, but sophisticated attackers can certainly build their own.

## **2.7 Misconfiguration**

Many access points ship in an unsecured configuration in order to emphasize ease of use and rapid deployment. Unless administrators understand wireless security risks and properly configure each unit prior to deployment, these access points will remain at a high risk for attack or misuse. The following section examines three leading access points, one each from Cisco, Lucent and 3Com. Although each vendor has its own implementation of

802.11b, the underlying issues should be broadly applicable to products from other vendors.

### 3. Security mechanisms and technologies

Wireless security technology is classified into three broad categories. Most vendors use a combination of technologies from these categories to build a secure system. The first category is authorization. Which includes the mechanisms for determining whether or not a client is an authorized user of the WLAN and which authorizations the user should have. It also includes the mechanisms for stopping an unauthorized user from using the WLAN. The second category includes those mechanisms for maintaining the privacy of the session once a user is authenticated into the WLAN. Normally, the privacy is maintained by some use of encryption. The final category contains those mechanisms that verify the integrity of the information. [1]

#### 3.1 Authentication

These are the technologies used to authenticate an individual client into the WLAN. Once authenticated, the client usually owns an authenticated session that continues until the client or WLAN terminate the session. When WLAN networks are deployed Service Set Identifiers (SSIDs) that act as a crude password and Media Access Control (MAC) addresses that act as personal identification numbers are often used to verify that clients are authorized to connect with an access point [2].

##### 3.1.1 Service Set Identifier (SSID)

This is the most basic security authentication mechanism for 802.11 networks. The SSID can be used as a shared secret; however, as a security mechanism it is virtually worthless. In reality, the SSID is transmitted unencrypted. An attacker can use passive eavesdropping to discover the SSID, or if she is impatient, she can use an active attack. To actively attack a WLAN using SSID as a shared secret the attacker sends a forged disassociates message to the target and then eavesdrops as the target automatically begins to reassociate with an authentication transaction. this security mechanism is only effective against the most unskilled attacker.[6]

##### 3.1.2 Media Access Control (MAC) Address

Access Points can be programmed to allow access to the WLAN by MAC address. This security mechanism is designed to deny access to all clients except those explicitly authorized to use the WLAN. The effort required to implement and maintain access lists is large. This mechanism does not scale well and is only useful for small WLANs. An attacker with minimal tools can easily defeat

access list. It provides no protection from the insider, who is an authorized user of the network. An outsider who obtains a wireless network access card that is authorized entry into the WLAN is effectively an insider. An outsider can also sniff the traffic between the AP and the client collecting a valid MAC address.

Access Points can be programmed to allow access to the WLAN by MAC address. This security mechanism is designed to deny access to all clients except those explicitly authorized to use the WLAN. The effort required to implement and maintain access lists is large. This mechanism does not scale well and is only useful for small WLANs. An attacker with minimal tools can easily defeat access list. It provides no protection from the insider, who is an authorized user of the network. An outsider who obtains a wireless network access card that is authorized entry into the WLAN is effectively an insider. An outsider can also sniff the traffic between the AP and the client collecting a valid MAC address.

#### 3.2 Packet Authentication

Packet Authentication is different from the session authentication that the previous paragraphs address. Once an authenticated session is established and the keys are exchanged most schemes rely on the privacy of an encrypted tunnel and integrity checking on the payload to imply the identity of the sender. This is an effective scheme, however, the addition of packet authentication adds an additional mechanism that an attacker must defeat. We do not believe replay, session high jacking and man-in-the-middle attacks are possible when packet authentication is added to strong session authentication. The individual packets that are transmitted, as part of an authenticated session must all come from the sender and arrive at the intended recipient. The receiver must be sure that the individual packets of a session did in fact come from the sender or else the session is subject to man-in-the-middle, replay or session high jacking attacks. These attacks all can succeed because the attacker fools the receiver into believing the packets sent by the attacker are from the target, hence destroying the session integrity of the system. These all rely on breaking an authenticated session. Per-packet authentication adds another layer of defense that an attacker must defeat. She cannot just take over an authenticated session without the ability to authenticate the packets that she generates or modifies. By itself packet authentication does not offer much defense; however, when combined with mutual session authentication it is very effective. This is an example of how properly integrated partial security mechanisms can form a defense-in-depth.

### 3.3 Integrity Checking

Another aspect that must be considered is integrity checking. Integrity is normally implemented separately from the encryption and indicates whether or not the packet has been altered from when the sender created it. A cryptographic checksum is a necessity. The question is whether to protect the message itself or the meaning of the message. The integrity check mechanism can encrypt the message and authenticate the encrypted message or it can authenticate the plaintext message and encrypt the authentication and the message. Authenticating the encrypted message leaves the session vulnerable to potential attack as documented by Ferguson and Schneier. [3]

#### 3.3.1. WEP CRC-32 Checksum

The WEP Checksum is a linear function of the message. Taking the plaintext as input the CRC- 32 checksum calculates a 32-bit number based on the content of the message. Any modification of the message should result in a different checksum when the CRC-32 function is used. This would indicate to the receiver that the message has been modified. The function does not map just one message to each of the 429 million possible values. There are far more than 429 million possible messages, so each value actually has many possible messages that can have the CRC-32 function applied to result in that value. A clever attacker can modify the message and leave the checksum unchanged. Because both the RC4 stream cipher and the CRC-32 checksum are linear the attacker can actually modify the message without even knowing the entire contents of the message, just the change she wants to make.

#### 3.3.2 Message Integrity Codes (MIC)

When encrypting the message a technique called Cipher Block Chaining (CBC) can be part of the encryption algorithm. In fact it is used in most modern algorithms. CBC calculations result in a residual value that does not have to be transmitted to decrypt the message; however, the residue can only be computed by using the secret key. Hence it insures the message is intact. This technique does not work when the message is encrypted.

#### 3.3.3 Secure Hash Algorithm SHA-1

SHA-1 is an algorithm for computing a condensed representation of a message. The SHA-1 algorithm computes a 160-bit output called a message digest from the original message. It is virtually impossible to find a message to match a given digest or two separate messages

that produces the same digest; therefore, a modified message will be detectable as such by the receiver, thus maintaining the integrity of the message.

There are other cryptographic hash algorithms that provide message integrity. MD4 and MD5 are older algorithms that have demonstrated vulnerabilities with published attacks.

It clarifies that existing encryption standards are not foolproof, knowledgeable intruders can pick off approved SSIDs and MAC addresses to connect to a WLAN as an authorized user with ability to steal bandwidth, corrupt or download files and wreak havoc on entire network. Wireless communications use air interface to carry the electromagnetic waves that carry the information. The air interface has the security concern that anyone in the range of the communication can intercept the data being transferred through it. And it is much easier than intercepting communications in fixed network as the waves in air go all over but in the fixed line they do not leak out of the cables. [4]

Other security problem with the air interface has been the fact that the radio waves will not stop to certain borders like organization's physical premises. This is serious problem with WLAN implementations as in the cities many offices are building their own WLAN networks near to each other as one might think the possible concerns in a office building where in every floor resides a different company with its own and different WLAN. This is basically equivalent to leaving an open network connection for everybody to peruse without the need to physically plug in a cable. To a certain degree, this issue is addressed by a standard security function called Wired Equivalent Privacy (WEP). In many cases this technology alone is not sufficient, so additional security options need to be developed for WLANs to enhance the protection provided by WEP. [2 & 4]

Another problem is that the other networks on the same frequency bands or near to each other can interfere each other's communications. (e.g. IEEE 802.11b, Home RF, Bluetooth). For data security reasons almost all wireless networks have to have some degree of network security with their own security algorithms. We can see clearly that data security considerations impact the entire network architecture. And while these data security considerations apply equally to wireless networks, the technology used in the physical layer (airspace) of wireless networks actually increases overall network security,

Objective of this paper is to suggest an algorithm based upon spread spectrum technology that uses a PN Sequence Code to secure the MAC address and only an authorized

user who knows that secret code will be able to use the WLAN Network.

Spread spectrum technology was first introduced about 50 years ago by the military with the objective of improving both message integrity and security. Spread-spectrum systems are designed to be resistant to noise, interference, jamming, and unauthorized detection. Many spread spectrum techniques are currently available. For example, there is direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), time hopping spread spectrum [3]. In Direct Sequence Spread Spectrum (DSSS) transmissions, another element than original data introduced is called pseudo-noise (PN) code sequence.

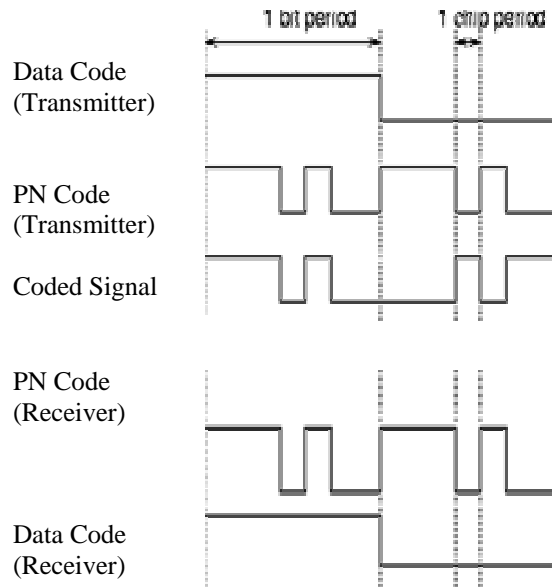
At the receiver end, in a process known as "correlation", a similar pseudo-noise code sequence matching exactly the one used by the transmitter is generated in order to "decode" the transmission by reconstituting the spread spectrum signal into intelligible information again. Without this code sequence, the spread spectrum signal is useless. Therein lies the security-enhancing feature of DSSS transmissions, which explains why there is military interest in the technology. Because DSSS transmissions are harder to detect, there is a lower probability of interception. And because it employs binary code sequences to "encrypt" the transmitted data, it makes it hard for unauthorized parties to "listen in", or to spoof or imitate network members. [5,6]

Consider a address of 10 bit length (1000 0010 11) & PN sequence Code is 0111 1000 11.

True Address (Original)	1000 0010 11	
	+	
PN Coding	0111 1000 11	
New Address	1111 1010 00	1111 1010 00
	+	+
PN Decoding Sequence	0111 1000 11	0100 1000 11
Result (True Address)	1000 0010 11	1011 0010 11

As it is clear from the above explanation that if the true address decoded by wrong code sequence (Blue colour) doesn't match with Original True Address. The algorithm spreads the original true address over the Bandwidth as decided by PN Sequence Code. So like spread spectrum multiple access scheme all users can transmit simultaneously on the entire available bandwidth using a pseudorandom code that is unique for each user. These PN codes are random sequences generated by means

of a multistage shift register, where some selected outputs are added modulo 2 and fed back to the input of the shift register. Such a PN code generator is shown in fig 1. The code sequences repeat themselves after a finite, although usually quite long, period and behave as random functions for all practical purposes. The receiver separates the different users by correlating the received signal with these codes.



It should be clear from the discussion above that wireless networks can take advantage of all the security measures available on wire-line networks, and then add additional security features not available in the wire-line world. As a result, wireless networks can be as secure, and in fact more secure, than their wire-line counterparts. Developments of new technologies the cost of securing WLAN using above spread spectrum technique can be reduced to a much lower value.

#### 4 Conclusion

Security is not a state, but a process of risk management. To develop, run, and maintain a secure network, the administrators and responsible leaders must know the value of the information and the threats against them. They must then consider the functionality their organizations need for mission accomplishment and the resources they have at their disposal. The algorithm presented here provides the best security method against unauthorized air channel access.

## 5 References

- [1]. Colonel D.J. Welch, Major S.D. Lathrop, "Department of Electrical Engineering and Computer Science United States Military Academy ITOC-TR-2003-101 West Point, New York 1996"
- [2]. F. Tanzella, "IT Toolbox wireless"
- [3]. F. Niels and B. Schneier, "A Cryptographic Evaluation of IPsec." Counterpane Internet Security White Paper, 1999. Webpage online available at [www.counterpane.com/ipsec.html](http://www.counterpane.com/ipsec.html) last accessed 3 October 2002.
- [4]. Air Defense, Wireless LANs: Risks and Defenses. White Paper available at [www.airdefense.net/company/whitepaper/Risks\\_Defenses\\_0802.pdf](http://www.airdefense.net/company/whitepaper/Risks_Defenses_0802.pdf) last accessed 20 September 2002. 2002 AirDefence, Inc.
- [5] Wireless LAN Security: 802.11b and Corporate Networks. ISS Technical White Paper. Webpage online available at [http://documents.iss.net/whitepapers/wireless\\_LAN\\_security.pdf](http://documents.iss.net/whitepapers/wireless_LAN_security.pdf) last accessed 20 September 2002
- [6]. V.Garg, "IS-95 & CDMA 2000" Pearson Education, pp 24-30