Security Implications for Wireless Local Area Networks

Daniel Zentner

Carroll College, Helena, MT

Follow this and additional works at: https://scholars.carroll.edu/mathengcompsci_theses

Part of the Computer Sciences Commons, and the Electrical and Computer Engineering Commons

Recommended Citation

https://scholars.carroll.edu/mathengcompsci_theses/78

This Thesis is brought to you for free and open access by the Mathematics, Engineering and Computer Science at Carroll Scholars. It has been accepted for inclusion in Mathematics, Engineering and Computer Science Undergraduate Theses by an authorized administrator of Carroll Scholars. For more information, please contact tkratz@carroll.edu.
Security Implications

for

Wireless Local Area Networks

By

Daniel R. Zentner

Computer Science Honors Thesis

2003
This thesis for honors recognition has been approved for the
Department of Mathematics, Engineering, and Computer Science.

(Director)  
Date

(Reader 1)  
Date

(Reader 2)  
Date
# Table of Contents

Acknowledgements ................................................................. ii

Chapter 1 Introduction to Wireless Communication .................. 1
   1.1 History ............................................................................. 1
   1.2 Wireless Uses ................................................................. 3
   1.2.1 Home Uses ................................................................. 3
   1.2.2 Business Uses ............................................................. 4
   1.2.3 Educational Uses ........................................................ 5
   1.3 Benefits ........................................................................... 6
   1.4 Common Configurations .................................................. 7

Chapter 2 802.11b Protocol ..................................................... 9
   2.1 Physical Layer .................................................................. 9
   2.2 MAC Layer ...................................................................... 12
   2.2.1 CSMA/CA .................................................................. 12
   2.2.2 Air Scanning ............................................................... 14
   2.2.3 Authentication ............................................................. 14
   2.2.4 Association ................................................................. 15
   2.2.5 Power Saving Options ............................................... 15
   2.2.6 Fragmentation ............................................................. 16
   2.3 Types of 802.11b Frames ................................................ 16
   2.3.1 General Frame ........................................................... 16
   2.3.2 Control Frame ............................................................. 16
   2.3.3 Control Frames ........................................................... 17
   2.3.3.1 RTS Frame ............................................................. 17
   2.3.3.2 CTS Frame .............................................................. 17
   2.3.3.3 ACK Frame ............................................................ 18
   2.3.4 Frame Filed Descriptions ........................................... 18

Chapter 3 802.11b WEP Security ............................................. 21
   3.1 An Overview of the RC4 Algorithm ................................ 21
   3.2 How the RC4 Algorithm Works ....................................... 21
   3.3 Introduction to WEP ....................................................... 23
   3.3.1 How WEP implements the RC4 Algorithm ................. 23

Chapter 4 Problems with WEP Security ................................. 27
   4.1 Vulnerabilities ............................................................... 27
   4.2 Attacking WEP ............................................................... 29
   4.2.1 How to Crack WEP’s Implantation of RC4 .................. 31
   4.2.2 Simulated Attack ......................................................... 31
   4.3 Countermeasures .......................................................... 32
   4.3.1 Other Means of Securing a Wireless Network ............ 34
   4.3.2 VPN’s ....................................................................... 34
   4.3.3 Biometrics ................................................................. 35

Conclusion ............................................................................. 36

Bibliography .......................................................................... 37
Acknowledgments

I would like to thank my loving family and friends, who have helped me financially, spiritually, and encouraged me in all my educational endeavors.

I would also like to thank my most amazing thesis and educational advisor Darrell Hagen, as well as my tireless readers Phil Rose and Dr. Jeffery Morris.

And finally, to Carroll College for giving me an educational platform on which I have tried very hard to excel.
Chapter 1

Introduction to Wireless Communication

1.1 History

The first real wireless communication system was developed by a collection of scientists. Samuel Morse sent the first telegraph message in 1838. James Maxwell, a Scottish physicist, developed the first theoretical method of sending electromagnetic waves through a medium in 1873. He theorized that these waves could travel at the speed of light. In 1888 Heinrich Hertz discovered radio waves, which are a form of electromagnetic radiation. Guglielmo Marconi, in 1895, conducted the first real use of radio waves by sending a signal over 2 miles to show that radio communication does not have to be in a straight line. After successfully demonstrating radio communications, Marconi quickly put his work to practical use. In 1899, he used wireless telegraphy to send a distress signal from a shipwrecked ship to a station on land, resulting in the rescue of all the passengers. During this era, many scientists feverishly worked on new wireless communication devices and their possible applications.

Beginning in 1924, the U. S. patent office issued a patent on wireless communication to Alfred N. Goldsmith spread spectrum. The actress Hedy Lamarr, who has a patent for a spread spectrum radio system, improved upon Alfred N. Goldsmith’s work. This research helped the U.S. military configure wireless signals to transmit data securely over a long distance. This type of technology was first introduced during WW II when the Army began sending battle plans over enemy lines and when Navy ships instructed their fleets from shore to shore.
In 1971, networking and wireless communications came together at the University of Hawaii. They developed a wireless network research project called AlohaNet. This project enabled the University to communicate to several other campus sites on other islands. The Aloha Net offered a relatively cheap method of bi-directional communication between a centralized computer and its wireless remote stations.

To keep wireless networking alive, amateur radio enthusiasts across the United States and Canada built terminal node controllers (TNCs) to interface their computers through ham radio equipment. To help sponsor wireless networking, the American Radio Relay League and the Canadian Radio Relay League were created to encourage the development of wireless wide area networks (WANs). As a result, the first generation of wireless communication modems were created in the early 1980’s. These modems could reach a possible data rate of up to 9600bps (bits per second). In 1985, the FCC announced the release of experimental bands for civilians’ use that opened up many wireless communication possibilities.

After the initial computer use of wireless communications, people and companies needed a common foundation from which to work. The Institute of Electrical and Electronics Engineers (IEEE) organization created the 802.11 Wireless Access Methods and Physical Layer Standardization Committee for wireless local area networks.

The first IEEE workshop was designed for researchers, design engineers, computer scientists, students, and users who were interested in getting a general overview of technical aspects of wireless indoor radio networks. After the general information had been presented, the second day of the workshop consisted of small group tutorials on
implementation, and at the end of the day, the network administrators gave a panel
discussion on the applications regarding wireless LANs.

After five years, the IEEE committee on wireless communications meet for a
second time. During the intervening years, many new developments had taken place
such as notebook computers equipped with wireless technology to make the “wireless
classroom” a possibility, and much greater speeds and reliability for wireless connections
to make “any time, anywhere” applications a reality. The second workshop had
something for everybody in the technology field, which helped fuel the third IEEE
wireless workshop.

During the third IEEE workshop, the committee on wireless communications ad
hoc committee was slated to meet every five years to evaluate and discuss the future of
the technology. In the workshop, many new topics were discussed, such as enabling next
generation wireless communications, Bluetooth, IEEE 802.11b, and the presentation of
many new wireless devices.

1.2 Wireless Uses

There are many practical uses of wireless communication devices. This paper
will focus on devices utilizing the 802.11a,b wireless protocol. The most common uses of
the 802.11a,b protocol are wireless local area networks for Home, Business, and
educational purposes.

1.2.1 Home Uses

IEEE 802.11b is by far the least expensive, most easy to use, and most cost
effective means for home wireless communications. Many homes built before 1996 were
not built with computer networking in mind, so the networking cables and hardware were
not installed. This caused a minor dilemma for the homeowners who wanted to connect two or more computers for file sharing and high speed Internet access. The owner had to go through costly rewiring to be able to complete this seemingly simple task of computer networking. In 1999 when the IEEE approved the 802.11b protocol for use, the homeowner had new options in home networking. Home networking would finally be possible. The 802.11b protocol allows for an 11Mbps (Netgear WirelessInfrev4) connection that is sufficient for any home application. Not only is the protocol fast enough, but it is priced well within common users’ budgets. The average cost to connect three computers with wireless networking in a home using wireless technology is about $150 (www.pricewatch.com). Not only is wireless networking moderately inexpensive, but it is also very easy to setup and maintain a wireless network. With average home setup time of less than two hours, home wireless networking lends itself well to the average computer user. With its ease of use, good performance, and cost effectiveness, wireless networking should be considered whenever a homeowner wishes to network his or her house.

1.2.2 Business Uses

To quickly connect up to 64 computers with maximum speeds reaching 54Mbps, the IEEE 802.11a wireless protocol is well suited for business applications (Netgear WirelessInfrev4). There are many benefits in using 802.11a for dense business networks with bandwidth intensive applications. These benefits include freedom from interference, increased speed, good range, better density overlapping, cost efficiency, and much greater user capacity.
The 802.11a protocol operates in the 5GHz frequency range (5.725GHz to 5.850GHz) (Netgear Wirelesslnforev4). This makes the protocol free from interference from common wireless phones, microwave ovens, and other interfering devices. When using this frequency range, it allows other wireless communications protocols to coexist, such as Bluetooth™ and 802.11a devices.

When considering a new form of networking, the new solution must be able to effectively handle many different network intensive applications. The 802.11a protocol was designed to perform up to 54Mbps, so it can support such applications as voice and video transmissions.

Connect range using the 802.11a protocol in a typical office environment is up to 255 feet. Within this distance, up to eight wireless access points can be installed. This is a much greater available network than for the 802.11b protocol, which only allows for three access points. With the increased wireless network density of 802.11a, a maximum of 512 wireless connections are available.

The 802.11a devices’ “prices are higher, but increased density and throughput potentially lowers cost per user and price per Mbps” (Netgear Wirelesslnforev4). This makes the 802.11a protocol a good choice for business wireless networking over the slower 802.11b protocol.

1.2.3 Education Uses

As mobile computing devices get faster and more obtainable by college students, the need for wireless capabilities in the classroom is growing. There are many benefits in having wireless computers in the classroom. They add to the educational value of the lecture, aid in the students’ learning, and provide a cost-effective method for a
multimedia hands-on classroom. The 802.11a protocol would best meet the needs of an educational environment because it has a higher throughput, more available users per access point, and has less of a chance of interfering with other existing wireless devices.

1.3 Benefits:

There are many benefits to using wireless LAN’s. Listed below with descriptions are a few of the more popular reasons for using wireless LAN’s for home, business, and educational purposes:

- No wires:

  The whole idea of wireless LAN’s is to be able to communicate to a wired network without having to be physically connected.

- Ease of installation:

  With an average home installation time of one hour, and many available books and online sources, implementing a wireless network is a relatively easy task to perform. Just the time and money saved by not having to install wires makes the ease of installation much greater.

- Relatively inexpensive:

  To connect three laptops wirelessly using the 802.11a protocol, the estimated cost is $310. To connect three laptops wirelessly using the 802.11b protocol, the estimated cost is $150. All prices were estimated through www.pricewatch.com.

- Decent throughput:

  The maximum available throughput for the 802.11a protocol is 54Mbps and for 802.11b it is 11Mbps(Netgear WirelessInforev4).
• Mobility

The chart below describes the range versus throughput for the 802.11a,b protocols (Netgear).

### 802.11b Range Versus Throughput

<table>
<thead>
<tr>
<th>Outdoor Environment</th>
<th>Range</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1650 ft</td>
<td>1 Mbps</td>
</tr>
<tr>
<td></td>
<td>1320 ft</td>
<td>2 Mbps</td>
</tr>
<tr>
<td></td>
<td>1155 ft</td>
<td>5.5 Mbps</td>
</tr>
<tr>
<td></td>
<td>835 ft</td>
<td>11 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indoor Environment</th>
<th>Range</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>500 ft</td>
<td>1 Mbps</td>
</tr>
<tr>
<td></td>
<td>400 ft</td>
<td>2 Mbps</td>
</tr>
<tr>
<td></td>
<td>270 ft</td>
<td>5.5 Mbps</td>
</tr>
<tr>
<td></td>
<td>175 ft</td>
<td>11 Mbps</td>
</tr>
</tbody>
</table>

*Table 1.1*

### 802.11a Range Versus Throughput

<table>
<thead>
<tr>
<th>Outdoor Environment</th>
<th>Range</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1200 ft</td>
<td>6 Mbps</td>
</tr>
<tr>
<td></td>
<td>100 ft</td>
<td>54 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indoor Environment</th>
<th>Range</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>300 ft</td>
<td>6 Mbps</td>
</tr>
<tr>
<td></td>
<td>60 ft</td>
<td>54 Mbps</td>
</tr>
</tbody>
</table>

*Table 1.2*

### 1.4 Common Configurations

There are many possible 802.11a,b wireless LAN configurations for home, business and educational uses. Below are a few pictures of what a wireless LAN might look like:

#### Home Configuration

![Home Configuration Diagram](image)
Business and Educational Configuration

Figure 1.2
Chapter 2

802.11b Protocol

The IEEE 802.11b standard is defined by the bottom two layers of the OSI (Open Systems Interconnection) model, the Physical Layer (PHY) and the Data Link Layer (Medium Access Control, MAC sub layer). As described in figure 2.0.

![OSI Reference Model](image)

2.1 Physical Layer

The 802.11b physical layer describes how the protocol communicates through the wireless medium. It includes the specifications for the data rate, types of codes, and the different types of modulation in use by the 802.11b protocol.

The Physical layer splits up the 2.4-2.4835GHz bands into eleven separate sub channels. This is to allow multiple wireless network nodes to communicate at the same time. Figure 2.1 describing how Direct-Phase Sequence Spread-Spectrum (DSSS) modulation parses the channel into eleven different sub channels. DSSS is used to be able to obtain higher data rates of 5MHz to 11MHz. Frequency-Hopping Spread Spectrum (FHSS) is used in the 1MHz to 2MHz range. FHSS is not used in the higher speeds because it would violate FCC regulations.
FHSS works by splitting the band into several-sub channels. It uses a narrowband carrier that randomly changes into either 2 or 4 levels. This means that the signal hops around the frequency band. This actually adds a bit of security into the way the transmission is sent over the medium.

**IEEE 802.11b Data Rate Specifications**

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Code Length (in bits)</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>11-bit Barker Sequence</td>
<td>BPSK</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>11-bit Barker Sequence</td>
<td>QPSK</td>
</tr>
<tr>
<td>5.5 Mbps</td>
<td>8-bit (CCK)</td>
<td>QPSK</td>
</tr>
<tr>
<td>11 Mbps</td>
<td>8-bit (CCK)</td>
<td>QPSK</td>
</tr>
</tbody>
</table>
The table above describes the code length and modulation in use by each of the possible data rates. The Barker Sequence is an 11-bit mathematical sequence that is ideal for modulating data onto the wireless medium. “The basic data stream is exclusive OR’d with the Barker code to generate a series of data objects called “chips”. Each bit is encoded by the 11-bit Barker code, and each group of 11 chips encodes one bit of data” (Anatomy of IEEE).

- **BPSK**: Binary Phase Shift Keying uses one phase shift for each bit.
- **QPSK**: Quadrature Phase Shift Keying uses four rotations (0, 90, 180, and 270 degrees).
- **CCK**: Complementary Code Keying uses 4 bits per carrier for 5.5Mbps and 8 bits per carrier for 11Mbps.

The physical layer is then split up into two parts, the Physical Layer Convergence Protocol (PLCP) and the Physical Medium Dependent (PMD) sub-layers. The sub-layer takes care of the wireless encoding. The PLCP is the common interface between the MAC sub-layer, enables it to write, and allows for carrier sense and Clear Channel Assessment (CCA). CCA is the ability to tell if the wireless medium is in use or is clear, and it is okay to send data.

The PLCP is then broken up into two different substructures, a long and short preamble. All 802.11b devices must support both the long and short preambles. The short preamble provides improved efficiency when network throughput is important, for example, when using streaming video and audio.

The PLCP Frame Format:

1. The PLCP Preamble
• Synchronization Field: Consists of a 128-bit field for the long preamble and a 56-bit field for the short preamble.

• 16-bit Start Frame Delimiter (SFD) Field: This field is used to mark the start of each new frame.

2. The PLCP Header

• 8-bit Signal or Data rate field: An indication of the transmission data rate.

• 8-bit Service Field: Not currently in use.

• 16-bit Length Field: Length of the future Medium Access Control sub-layer’s Protocol Data Unit (MAC PDU).

• 16-bit Cyclic Redundancy Code (CRC) Field: this is used for error detection.

2.2 Medium Access Control Sub-Layer (MAC)

The IEEE 802.11b MAC layer is the interface between the physical layer and the host device or application. It supports both ad hoc and infrastructure operation modes. The MAC layer has many responsibilities including managing Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), air scanning, authentication, association, power saving options, and packet fragmentation.

2.2.1 CSMA/CA

The heart of the 802.11b protocol is how it accesses and transmits information over the wireless medium. CSMA/CA is also referred to as Distributed Coordination
Function (DCF). DCF is a connection-based protocol assuring that the medium is clear before transmitting information. The main goal is to avoid having stations transmit at the same time, which results in collisions and corresponding retransmissions.

First, each station listens on the medium. The first station that finds the medium clear begins to transmit. If the station senses that the medium is currently occupied, it then waits a random amount of time and then retries to connect.

Problems could arise if there are many stations connected to the same access point, but are out of communication range from one another. This problem is commonly known as the “hidden node problem”. For example: assume that there are three stations A, B, and C. Station A can hear B, and B can hear C, but A cannot hear station C, and all stations can communicate with the Access point. To handle this problem, the following algorithm was developed. It is also explained in figure 2.2.

1. If A wants to send a message to the access point, it sends a RTS (Request To Send) packet, which station C can hear.
2. The access point sends back a CTS (Clear To Send) packet.
3. A then transmits the data to the access point.
4. An ACK (Acknowledgment) packet is then sent to confirm this transmission.

![Diagram showing the hidden node problem and the 4-way handshake.](image_url)
2.2.2 Air Scanning

There are two types of scanning, active and passive. Passive scanning is when the Network Interface Card (NIC) scans individual channels randomly to try to find the access point with which to communicate. The NIC listens on the channels for the access points’ periodic broadcast beacon. This beacon contains signal strength, service set identifier, supported data rates, and location. The NIC uses this information to determine which access point is the best choice.

Active scanning is when the NIC actively communicates with all possible access points. The NIC broadcasts a probe frame to all available access points. This method of scanning allows the NIC to immediately contact access points, instead of waiting for an access point beacon transmission. Active scanning, if allowed, consumes network resources, but makes sure the best possible access point is in use.

2.2.3 Authentication

Authentication is the method of checking to make sure the device or user is who he or she proclaims they are.

There are two types of authentication defined by the 802.11b protocol, open system and shared key authentication. Open system authentication is required and it is described by a two-step process. First the NIC sends an authentication packet to the access point. Then the access point responds with either an approval or disapproval authentication packet.

The shared key method of authentication is a four-step process that is based on authenticating the NIC’s WEP (Wired Equivalent Privacy) key. First the NIC sends a request for authentication packet to the access point. The access point then sends the
station a challenge packet. The station then encrypts the challenge packet and sends it back to the access point. The access point decrypts the packet with the correct key and compares it to the original challenge packet. The access point sends the NIC either an approval or disapproval authentication packet.

2.2.4 Association

After the authentication, the NIC must then associate with the access point before it is to transmit data. Association is important, so that the NIC stays in constant synchronization with the most optimal access point. The association process is when the NIC requests information regarding the access point. This information includes the Service Set Identifier (SSID), supported data rates, and other important information regarding the access point. The NIC analyzes all available access points and then chooses the best available access point in which to associate with. Only when the NIC and the access point have finished associating can the flow of data begin.

2.2.5 Power Saving Options

When power utilization is a factor in wireless communication, then the NIC is set to PAM (Polled Access Mode). This is when the NIC goes into a “sleeping” mode; the card will then “wake up” at a designated time to listen for a special packet called a TIM (Traffic Information Map) from the access point. In between TIMs, the NIC shuts off its radio and thus conserves power. All the devices on the network share the same wake-up period, as they must all wake up at exactly the same time to hear the TIM from the access point (Anatomy of IEEE).

If the NIC has information waiting at the access point it stays “awake” long enough for the access point to transmit the buffered data.
2.2.6 Fragmentation

The packet fragmentation option enables the 802.11b protocol to break up large packets into smaller, more manageable packets. This is done to minimize the need to retransmit large packets in the occurrence of an error. Errors are more likely to affect large packets than smaller ones, thus requiring the packet to be resent.

In addition to the topics above, the 802.11b MAC layer is also responsible for identifying the source and destination address of the packet being sent, as well as the data payload and a CRC.

2.3 Types of 802.11b Frames

2.3.1 General Frame

- Frame Control: 2 bytes
- Duration Field: 2 bytes
- Address Field 1: 6bytes
- Address Field 2: 6bytes
- Address Field 3: 6bytes
- Sequence and Control Field: 2bytes
- Address Field 4: 6bytes
- Data/Payload: 0-2312bytes
- Frame Check Sequence: 4bytes

2.3.2 Frame Control Frame

- Protocol Version: 2bits
- Type: 2bits
- Subtype: 4bits
• To DS: 1bit
• From DS: 1bit
• More Fragments: 1bit
• Retry: 1bit
• Power Management: 1bit
• More Data: 1bit
• WEP: 1bit
• Order: 1bit

2.3.3 Control Frames

2.3.3.1 RTS Frame

• Entire Control Frame
• Duration: 2bits
• RA: 6bits
• TA: 6bits
• FCS: 4bits

2.3.3.2 CTS Frame

• Entire Control Frame
• Duration: 2bits
• RA: 6bits
• FCS: 4bits

2.3.3.3 ACK Frame

• Entire Control Frame
• Duration: 2bits
2.3.4 Frame Field Descriptions:

- **Duration ID Field:** This 16-bit field represents the number of microseconds that the medium is expected to remain busy for the transmission.

- **Address Fields:** There are up to 4 addresses contained in each 802.11b MAC frame. They are numbered 1 through 4 and are used for different purposes depending on the frame and subtype. Typically, Address 1 is used for the receiver; Address 2 is used for the transmitter, and Address 3 for filtering (by receiver).

- **Sequence and Control:** This 16-bit field is broken up into two sections, a 12-bit sequence number and a 4-bit fragment number. Higher-level packets are broken into different sequence numbers and if those packets need to be fragmented, they are broken up and the fragments are assigned a fragmentation number.

- **Data Field:** This is the actual information from the higher levels. Each frame supports up to 2304 bytes.

- **FCS:** The Frame Check Sequence uses a CRC (Cyclic Redundancy Check) to make sure the header is not corrupted during transmission.

- **Protocol Version:** The protocol field is 2 bits long. It declares the version of 801.11 that is in use.

- **Type and Sub-type:** The frame type and sub-type fields identify the function of the frame and which other MAC header fields are present in
the frame. There are three types of frames: control, data, and management frames. There are several subtypes within each frame type.

- **To and From DS:** The to and from DS (Distribution System) fields are 1-bit in length. It is always set to 1 if the frame is intended for the access point.

- **More Fragments:** This one-bit field is set to 1 if there are more fragments coming and is set to 0 if this is the final fragment.

- **Retry:** This one-bit field is set to 0 to indicate that this is the first time this frame has been sent and is set to 1 if the frame has been transmitted before.

- **Power Management:** The power management field is one bit in length. It is set to 1 to indicate that the mobile device is going into “sleep mode”, and is set to 0 to indicate that the device is “awake” and active.

- **More Data:** The More Data sub field is a single bit used by the access point to tell a mobile device that there is at least one frame buffered at the access point for the device. When this sub field is 1, there are no frames buffered. When this sub filed is 0, there is at least one more frame remaining.

- **WEP:** When this one-bit field is set to 1, the data in the frame has been encrypted with the WEP algorithm.
• **Order:** The order field is one bit in length and is set to 1 if when the content of the frame is in a strictly ordered group. For example, a larger transfer of important data will use the order field.

• **RA:** The Receiver Address field is 48 bits long. It indicates the address of the wireless station that needs to process the data.

• **TA:** The Transmitter Address is a 48-bit address used to identify the wireless device that is transmitting the frame onto the medium.
Chapter 3

802.11b WEP Security

Computer security is the process of making all digital data on a computer secure from any and all possible attacks or intrusions. The methods of preventing such attacks is a very important topic in the wired and wireless computing world.

The IEEE 802.11b standard defines the Wired Equivalent Privacy, or WEP, encapsulation of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network. WEP implements a 40-to-128bit RC4 encryption algorithm to try to provide data security.

3.1 An Overview of the RC4 Algorithm

The RC4 is a variable-key-size stream cipher developed in 1987 by Ron Rivest for RSA Data Security, Inc. For seven years it was proprietary, and details of the algorithm were only available after signing a nondisclosure agreement. RC4 is not necessarily an insecure weak algorithm, but there are errors in many of the applications that use RC4, which will leave the application vulnerable to attack. The RC4 key is often limited to 40 bits, because of export restrictions, but it sometimes uses a 128-bit key. It has the capability of using keys between 1 and 2048 bits in length. RC4 is used in many commercial software packages such as Lotus Notes and Oracle Secure SQL.

3.2 How the RC4 Algorithm works

The RC4 algorithm works in two phases, key setup and ciphering. The first phase of the RC4 algorithm is the most difficult to understand. Below is a description of how to
set up the keys for the RC4, which is the creation of the S-box. The example uses an 8-bit keyword.

1. Allocate a 256-element array of 8-bit bytes to be used as an S-box, label it
   \[ S[0], \ldots S[255] \].

2. Initialize the S-box by filling each entry with its index number:
   \[ S[0] = 0, S[1] = 1, \ldots, S[255] = 255; \]

3. Fill another array of the same size (256) with the key, repeating bytes as necessary.
   As the value I is \(< 256\) DO:
   \[ S2[I] = \text{key}[I \mod \text{the Key Length}] \]
   Add one to I
   End Do

4. Set the index j to zero and initialize the S-box as follows:
   As the value I is \(< 256\) DO:
   Make \( J = (J + S1[I] + S2[I]) \mod 256 \)
   Set temp = S1[I]
   Set S1[I] = S2[j]
   Set S2[j] = temp
   Add one to I
   End Do

5. Initialize i and j to zero. If it is suspected that the wireless communications are compromised, then set the S2 array and the key-array to zero also. That gives slightly better protection since it is believed to not be feasible to calculate the key after it had been zeroed and thus forgotten.
Once the encrypting variable is produced from the key setup, the key is then XORed with the plaintext message to create the encrypted message. When the receiver gets the encrypted message, they XOR the message with the same encrypting key to reveal the plaintext message. There are some possible design flaws in the algorithm using this method of key creation and encryption in WEP. Below is a description of how the RC4 is implemented of the binary representation of the ASCII characters “HI”:

Assume that the RC4 algorithm generated the binary key of (00000010)

<table>
<thead>
<tr>
<th>Binary Representation</th>
<th></th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>XORed with the Key</td>
<td>01001000</td>
<td>01001001</td>
</tr>
<tr>
<td>Encrypted Results</td>
<td>00000010</td>
<td>01001010</td>
</tr>
</tbody>
</table>

### 3.3 Introduction to WEP

“The 802.11b design community generally concedes that the WEP encapsulation fails to meet its design goals, but widely attributes this failure to WEP’s use of 40-bit RC4 as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP could meet its design goals by migrating from 40-bit to 104 or 128-bit RC4 keys instead” (Unsafe At Any Key).

It has been found and widely accepted that no matter the size of the RC4 key, WEP’s implementation will always be insecure. The main problem with WEP is the way it is designed to encapsulate data using the RC4 algorithm. The RC4 algorithm it is poorly suited for WEP.

### 3.3.1 How WEP implements the RC4 Algorithm

The IEEE 802.11 protocol defines WEP as a method for encrypting the contents of the 802.11 data frames. Below is a list of six general WEP concepts:

1. A key is shared between the all the clients and the access points.
2. WEP implements the RC4 stream cipher as its main encryption algorithm. The RC4 algorithm is used to generate a key, which is XORed with the plaintext to create the ciphertext.

3. WEP also uses the RC4 algorithm as its main ciphertext decryption algorithm.

4. A 24-bit initialization vector (IV). WEP appends the IV to the shared key. WEP uses this combined key and the IV to generate the RC4 key schedule. WEP selects a new IV for each packet.

5. An encapsulating packet is sent to the receiver to decrypt the ciphertext.

6. WEP also uses a CRC of the frame payload plaintext in its encapsulation. The CRC is computed over the data payload and then appended to the payload before encryption. WEP encrypts the CRC with the rest of the data payload. Below is a description of how WEP goes about encrypting and sending packets:

**Sender**

1. First each member wanting to encrypt data must gain access to the shared key. This is done via an unspecified out-of-band transmission mechanism.

2. The sender then calculates the CRC of the frame payload and appends it to the end of the encapsulated frame.

3. The sender then selects a new IV, appends this to the shared key to form a "per-packet key", and uses the results to generate the RC4 key schedule.

4. The sender then uses the RC4 algorithm to encrypt the payload plus the CRC.

5. The IV is then placed in the appropriate field in the encapsulated frame header and sets the WEP encryption bit to true.

6. Now the frame is encapsulated with WEP and is ready to be sent.
Receiver

1. The receiver first checks to see if the WEP encryption bit is set to true in the header.

2. If the bit is set, then the receiver extracts the IV from the frame header and concatenates it onto the shared key. The receiver then generates the RC4 “per packet” key schedule.

3. The encrypted payload plus the “per packet” key schedule are placed in the RC4 deciphering algorithm to reveal the original plain text.

4. Finally, the receiver uses the CRC of the decrypted payload data to verify that the frame data was correctly decrypted.

Figure 3.1 taken from Wireless Network Security

Several problems and concerns with WEP send and receive processes are:

1. If the first bit in the packet is lost during transmission, it will cause the RC4 algorithm to be off by one bit, resulting in the loss of all the following data in that
packet. This then requires the WEP algorithm to have to resynchronize the RC4 decryption process. This is done by reinitializing the cipher key schedule on every new data frame.

2. Stream ciphers have a bad property of being able to use a particular key only once.

3. The cipher stream is publicly known, and it is presumed that possible attackers will buffer the entire transmission.
Chapter 4

Problems with WEP Security

Now that we have a better understanding of how WEP uses the RC4 algorithm to encrypt data, we now must point out that it is widely accepted that there are many security flaws with in WEP’s implementation of the RC4 algorithm. This chapter will discuss the current problems facing wireless security, how to attack WEP, and possible countermeasures to try to make WEP, and wireless networking as a whole, more secure.

4.1 Vulnerabilities

There are a number of security vulnerabilities within the 802.11b protocol. Listed below are some of security problems:

1. The 802.11b uses static WEP keys: All the users connecting through the same access point need to have the same key. This key could be used for a long period of time. This lack of key management causes a very large potential security hole. For example, if a laptop computer using a secure wireless connection was stolen, then every computer on that particular network would be compromised. Additionally, since every device uses the same key, if a large amount of traffic was transmitted, it could then lead to eavesdropping for an analytical attack.

2. The IV in WEP is a 24-bit field sent in the cleartext part of the WEP frame. When the IV is reused, it will produce exactly the same encryption key. A short IV results in the reuse of the key in a relatively short amount of time on busy networks. Because the 802.11 standard does not specify
how or when the IV is changed, it is left up to the individual wireless NIC

card. Depending on the vendor, the IV could be randomly generated or
the same IV could be constantly used. As a result, attackers could record
network traffic to determine the key and then decrypt the ciphertext.

3. “The IV is part of the RC4 encryption key. The fact that an eavesdropper
knows 24-bits of every packet, combined with a weakness in the RC4 key
schedule, leads to a deadly analytical attack that recovers the key, after
intercepting and analyzing only a relatively small amount of traffic. This
attack has been reduced to a script” (Wireless Network Security).

4. The 802.11 WEP standard does not include data integrity for the encrypted
information; however, the MAC layer provides a CRC to make sure that
packets and acknowledgments arrived correctly. “The combination of
noncryptographic checksums with stream ciphers is dangerous and often
leads to unintended “side channel” attacks, as is the case for WEP”
(Wireless Network Security).

5. When a user gets a new product, added security features are often turned
off to aide in the ease of installation. Users need to make sure to read all
device documentation, so that they may optimize all possible security
features.

6. The 40-bit WEP key is inadequate for any security application. Most
encryption keys range from 80 to 256 bits, so the longer the key, the less
likely it is to be vulnerable to a brute force attack.
7. Keys are shared between all wireless devices, which can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.

8. Keys cannot be updated easily. To prevent a brute force attack, keys should be changed frequently. This means that every wireless device on the network will have to have their keys manually changed by the security administrator.

9. “RC4 has a weak key schedule and is inappropriately used in WEP. The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 key stream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries”(Wireless Network Security).

10. Packet integrity is poor, because the frame check sequence or cyclic redundancy check (CRC) is only used to make sure the header of each packet is correct. This can then lead to the possibility of the message being modified and increases the risk of a “man-in-the-middle” attack.

11. No user authentication: There is only device authentication with wireless networks. So if a device is stolen, the thief will have full access to the wireless network.
4.2.1 Attacking WEP

It has been shown above that the implementation of WEP by the 802.11 protocol has many possible security flaws. There are two main types of attacks against WEP, passive and active attacks. Both methods of attack have different attributes associated with them.

- **Passive attack:** Passive attacks come in two forms, eavesdropping and traffic analysis. Passive attacks can only occur after the attacker has gained access to the network in some way, such as stealing a wireless device, or cracking the encryption key. The passive attack methods are:
  
  o **Eavesdropping:** The attacker simply monitors all transmissions for message content. For example, the attacker is within the wireless communication range and listens in on all the transmissions being broadcast.
  
  o **Traffic analysis:** The attack gains intelligence in a very subtle way to gain access to the network by analyzing the flow of traffic between the device and the access point to try to determine a possible network flaw.

- **Active Attack:** This is where the attacker modifies a message, file, or data stream. There are four types of active attacks: masquerading, replay, message modification, and Denial-of-Service (DoS).
  
  o **Masquerading:** When the attacker impersonates an authorized user to gain access to unauthorized privileges.
Replay: This is also called the “man-in-the-middle” attack. The attacker intercepts the information and retransmits the data as the legitimate user.

Message modification: The attacker alters a legitimate message by deleting, adding to, changing, or reordering the message.

Denial-of-Service: The attacker prevents or prohibits the normal use or management of the communication facilities (Wireless Network Security).

4.2.2 How to crack the WEP’s implementation of RC4

The first step in being able to successfully attack WEP encryption is to capture the encrypted packets from the wireless network. There are a number of very expensive commercial software titles that are available, such as NAI’s “Snifter” and Wildpack’s “AiroPeek”. They have the ability to capture and decode 802.11 packets. To conserve on money, there is a free, packet-sniffing program available called Ethereal, that will capture the raw WEP-encrypted packets and when the coded attack program runs, it will decrypt the packet.

4.2.3 Simulated attack

All accounts of the simulated attack were taken from Stubblefield, Loannids, and Rubin paper on cracking WEP using the Using the Fluhrer Mantin, and Shamir attack methods.

To simulate an attack, we must first use our understanding of the weakness of the RC4 algorithm to determine how many packets will need to be collected to make the attack successful. In a simulated attack, the attack code was able to recover the full key
when given 256 probable resolved cases. The problem is being able to find the first bit in each of the encrypted packets to be able to analyze each individual packet. To start the attack, a large number of packets must be collected from the wireless network. After finding the IVs in the collected packets, it is discovered that the wireless NIC uses a simple counter to increment IVs, where only the first byte is incremented. It is determined that 5,000,000 to 6,000,000 packets are needed to compute the IV.

After being able to derive the IVs, all that is needed now is the key bytes. The easiest way to obtain the key bytes is to exploit the human factor of the algorithm and the poor key management available in WEP implementations. “Since WEP keys have to be entered manually, it is assumed that instead of giving clients a long string of hex digits, a user memorable pass-phrase would be used. After examining the test wireless card, it is determined that the user-memorable pass-phrase is simply used raw as the key (i.e. the ASCII is used; no hashing is done)”(Using the Fluhrer Mantin). Hashing does not protect against, a dictionary attack however. This is just one example of how an attack could be performed. There are many possible methods of hacking into a wireless network because there is no direct way to stop attackers from listening in on a wireless communication.

Even if the key length was increased to 104 or even 128bits, this does nothing to increase WEP’s resistance to attack. “This is because the deficiencies are related to how WEP uses cryptography, not the key size. WEP’s design attempts to adapt RC4 to an environment for which it is poorly suited, with potentially catastrophic consequences for its intended users. Thus, to meet its goal of wired equivalent privacy, the WEP encapsulation needs significant reconstruction”(Unsafe At Any Key Size).
4.3.1 Countermeasures

To make sure any network is secure, a large number of administrative security policies need to be in place to make sure network security and integrity is in place before a wireless LAN is implemented. A wireless LAN should be able to do the following:

1. Be able to identify who may connect to the wireless LAN.
   If possible, a secondary authentication server should be installed to help manage and account for all wireless users trying to access the wireless network.
2. Does the user require Internet access?
   Have a well laid-out inventory of each user’s needs to tailor security and network permissions for each user.
3. Where and who may install access points and other wireless devices?
   Make sure that all user permissions are set correctly and updated frequently.
   Also, have only a specific person or team do and make all wireless additions and updates to make sure there are uniform network settings and guidelines.
4. Limit the location of wireless access points.
   A location assessment of access points needs to be taken into consideration. If wireless communications are used on a large campus, the administrator should look at the available range of the access point to try to cut down on users outside of the campus trying to access the wireless network.
5. Limit the type and kind of information that can be sent over the wireless link.
   There should be guidelines in place restricting the transfer of security or top security data across a wireless network to prevent a possible security breach.
6. Have well-defined security settings for access points.
7. Have a forum for reporting lost or stolen wireless devices.

8. Provide guidelines on the use of encryption and other security software.

   Make sure that the highest available encryption is properly implemented and installed on the wireless network to insure the security of the wired and wireless network.

9. “Another management countermeasure is to ensure that all critical personnel are properly trained on the use of a wireless technology. Network administrators need to be fully aware of the security risks that wireless LANs and devices pose. They must work to ensure security policy compliance and to know what steps to take in case of an attack. Finally, the most important countermeasures are trained and aware users” (Wireless Network Security).

### 4.3.2 Other Means of Securing a Wireless Network

There are several possible means to securing data on a normal LAN that can be implemented on a wireless LAN in accordance with the WEP encryption. For example, security can be achieved by using Virtual Private Network (VPN) technology and also with biometrics.

### 4.3.3 Virtual Private Networks (VPN’s)

Virtual Private Networks use cryptographic techniques to protect information as it passes from one network to another. In a sense, the VPN creates a virtual “tunnel” from one station to another. It does this by encapsulating one packet inside another, which separates it from other normal network or Internet traffic.

Wireless LAN’s would implement the VPN technology when they are located outside the main firewall of the organization. This would create a “VPN overlay” where
the wireless device would have its data encrypted twice, first by the VPN software and then next by the WEP protocol. In doing this, it would create a direct “tunnel” to the main organization. Even if the WEP part of the encryption was broken, the data inside WEP packet would then still be protected by the VPN’s encryption method which is much more secure and reliable than WEP. The figure below describes one possible VPN connection possibility. Figure taken from *Wireless Network Security*.

![Diagram](image)

**Figure 4.1**

### 4.3.4 Biometrics

There are many methods of securing a network but biometrics is the most foolproof way of making sure a user is who they say they are. Biometrics is the method of using our bodies (Fingerprint, facial scan, iris scan…) or secure smart cards to identify the user. Biometrics has two main advantages: one, the user must be present to gain access to the network and two, the method of access is very hard to duplicate because everybody is unique.
Conclusion

There are many security hardships facing wireless LAN’s, most undeniably is that WEP use of the RC4 algorithm for securing data over the wireless medium. In addition, to the poor encryption algorithm, using wireless devices, leads to hackers being able to listen into any communications sent wirelessly.

In my general assessment of the 802.11a,b wireless LANs, I have found that they are inherently insecure. Only with drastic changes to the WEP protocol would the 802.11a,b standard even become possibly secure. If a user still wishes implement a wireless network, they should make sure to find out about other security options available such as: VPN’s, firewalls, authenticating servers, and a developed network security policy.
Bibliography

Borisov Nikita, “Security of the WEP algorithm”

Cárdenas, Roberto Gómez. “The Algorithm (Stream Cipher) RC4 (ARC-4)”
November 01, 2001 http://webdia.cem.itesm.mx/ac/rogomez/TareasCripto/RC4-2.doc

Conover, Joel “Anatomy of IEEE 802.11b Wireless”

Geier, Jim “Medium Access Methods”

Grogans Candance, Bethea Jackie, Hamdan Issam. “RC4 Encryption Algorithm”
March 5, 2000 http://www.ncat.edu/~grogans/main.htm

Johns Hopkins School of Public Health. “History of Wireless”
http://wireless.jhsph.edu/history.html


Netgear Corp, “Wireless Comparison Information”

www.cwins.wpi.edu/wlans91/scripts/preface.html

Routt, Bill “FRAME TYPES AND FORMATS IN IEEE 802.11A, 802.11B AND 802.11G WIRELESS LOCAL AREA NETWORKS”

Sarinnapakorn, Kanoksri “High Rate Wireless Local Area Networks”
March 15, 2001 http://alpha.fdu.edu/~kanoksri/IEEE80211b.html


Stubblefield Adam, Loannids John, Rubin Aviel D., “Using the Fluhrer Mantin, and Shamir Attack to Break WEP”
August 6, 2001 AT&T Labs Technical Report TD-4ZCPZZ

Walker, Jesse “Unsafe At Any Key Size; An Analysis of the WEP Encapsulation”
October 27, 2000 Intel Corp