Spread Spectrum
and
Wi-Fi Basics

Syed Masud Mahmud, Ph.D.
Electrical and Computer Engineering Dept.
Wayne State University
Detroit MI 48202
Spread Spectrum

- Spread Spectrum techniques are used to deliberately spread the frequency domain of a signal from its narrow band domain.
- These techniques are used for a variety of reasons such as:
  - establishment of secure communications,
  - increasing resistance to natural interference and jamming
Spread Spectrum Techniques

- Frequency Hopping Spread Spectrum (FHSS)
- Direct-Sequence Spread Spectrum (DSSS)
- Orthogonal Frequency-Division Multiplexing (OFDM)
The FHSS Technology

- FHSS is a method of transmitting signals by rapidly switching channels, using a pseudorandom sequence known to both the transmitter and receiver.
- FHSS offers three main advantages over a fixed-frequency transmission:
  - Resistant to narrowband interference.
  - Difficult to intercept. An eavesdropper would only be able to intercept the transmission if they knew the pseudorandom sequence.
  - Can share a frequency band with many types of conventional transmissions with minimal interference.
The FHSS Technology

- If the hop sequence of two transmitters are different and never transmit the same frequency at the same time, then there will be no interference among them.
- A hopping code determines the frequencies the radio will transmit and in which order.
- A set of hopping codes that never use the same frequencies at the same time are considered orthogonal.
Application of FHSS

- Bluetooth uses FHSS technology.
- In US there 79 channels in Bluetooth technology.
- The protocol operates in the unlicensed ISM band at 2.4-2.4835 GHz.
- The Bluetooth protocol divides the band into 79 channels (each 1 MHz wide) and changes channels 1600 times per second.
The DSSS Technology

- The DSSS is the same technology used in GPS satellite navigation systems.
- The data stream is combined via an XOR function with a high-speed pseudo-random numerical sequence (PRN).
- For 1 and 2 Mbps DSSS the PRN code is the 11-chip Barker sequence, which is 10110111000.
An Example of DSSS Coding

Data Bits

\[
\begin{array}{c}
0 \\
1 \\
\end{array}
\]

Barker Sequence

11 Chips 11 Chips

Data

PRN

Output

10110111000010110111000

101101110000100100011

Out
A “0” and a “1’ in DSSS Coding

<table>
<thead>
<tr>
<th>Data Bit</th>
<th>DSSS Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>101101111000</td>
</tr>
<tr>
<td>1</td>
<td>010010000111</td>
</tr>
</tbody>
</table>
Binary and Quadrature Phase Shift Keying Modulation

- XOR output is modulated onto a carrier frequency using BPSK and QPSK for 1 and 2 Mpbs signals, respectively.

### BPSK Encoding

<table>
<thead>
<tr>
<th>XOR Output</th>
<th>Phase Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>$\pi$</td>
</tr>
</tbody>
</table>

### QPSK Encoding

<table>
<thead>
<tr>
<th>2-Bit (d0,d1) XOR Output (d0 is the first bit in time)</th>
<th>Phase Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>$\pi/2$</td>
</tr>
<tr>
<td>11</td>
<td>$\pi$</td>
</tr>
<tr>
<td>10</td>
<td>$3\pi/2$</td>
</tr>
</tbody>
</table>
Complementary Code Keying is used for 5.5 and 11Mbps

- Complementary Code Keying (CCK), is a set of 64 eight-bit code words used to encode data for 5.5 and 11Mbps.
- The code words have unique mathematical properties that allow them to be correctly distinguished from one another by a receiver even in the presence of substantial noise and interference.
DSSS Code Length, Modulation and Symbol Rate

<table>
<thead>
<tr>
<th>Data rate</th>
<th>Code length</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>11 (Barker sequence)</td>
<td>BPSK</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>11 (Barker sequence)</td>
<td>QPSK</td>
</tr>
<tr>
<td>5.5 Mbps</td>
<td>8 (CCK)</td>
<td>QPSK</td>
</tr>
<tr>
<td>11 Mbps</td>
<td>8 (CCK)</td>
<td>QPSK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data rate</th>
<th>Symbol rate</th>
<th>Bits/Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>1 MSps</td>
<td>1</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>1 MSps</td>
<td>2</td>
</tr>
<tr>
<td>5.5 Mbps</td>
<td>1.375 MSps</td>
<td>4</td>
</tr>
<tr>
<td>11 Mbps</td>
<td>1.375 MSps</td>
<td>8</td>
</tr>
</tbody>
</table>
Effect of PRN Sequence on Transmit Spectrum

Data Spectrum

XOR with PRN Code

Transmit Spectrum

01001000111

1

Spread Spectrum and Wi-Fi Basics by Syed M. Mahmud
DSSS Receiver

• The receiver processing of DSSS signals begins with de-spreading the signals.
• This is done by mixing the spread signal with the same PRN sequence that was used for spreading.
DSSS Receiver

Demodulator

Barker Sequence

Correlating Process

Raw bit stream

Data Bits

Spread Spectrum and Wi-Fi Basics by Syed M. Mahmud
Received Signal is Correlated with the PRN Sequence to Recover Data and Reject Interference.
Properties of DSSS Signals

Immune to certain amount of noise

Signal & Noise on the Air:

DSSS Receiver
Properties of DSSS Signals

Immune to certain amount of interference

Signal, Noise & Interference on the Air:

DSSS Receiver
Properties of DSSS Signals
Multiple access using different PRN codes

Multiple Signals and Noise on the Air:
## DSSS versus FHSS

<table>
<thead>
<tr>
<th></th>
<th>DSSS</th>
<th>FHSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Higher cost</td>
<td></td>
<td>Lower cost</td>
</tr>
<tr>
<td>Higher power consumption</td>
<td></td>
<td>Lower power consumption</td>
</tr>
<tr>
<td>Higher data rates</td>
<td></td>
<td>Lower data rates</td>
</tr>
<tr>
<td>Lower aggregate capacity using multiple physical layers.</td>
<td></td>
<td>Higher aggregate capacity using multiple physical layers.</td>
</tr>
<tr>
<td>More range</td>
<td></td>
<td>Less range</td>
</tr>
<tr>
<td>Smaller number of geographically separate radio cells due to a limited number of channels.</td>
<td></td>
<td>Most tolerant to signal interference</td>
</tr>
</tbody>
</table>

Spread Spectrum and Wi-Fi Basics by Syed M. Mahmud
One version of Wi-Fi (IEEE 802.11b) Uses DSSS Technology

<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412 MHz</td>
</tr>
<tr>
<td>2</td>
<td>2417 MHz</td>
</tr>
<tr>
<td>3</td>
<td>2422 MHz</td>
</tr>
<tr>
<td>4</td>
<td>2427 MHz</td>
</tr>
<tr>
<td>5</td>
<td>2432 MHz</td>
</tr>
<tr>
<td>6</td>
<td>2437 MHz</td>
</tr>
<tr>
<td>7</td>
<td>2442 MHz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>2447 MHz</td>
</tr>
<tr>
<td>9</td>
<td>2452 MHz</td>
</tr>
<tr>
<td>10</td>
<td>2457 MHz</td>
</tr>
<tr>
<td>11</td>
<td>2462 MHz</td>
</tr>
<tr>
<td>12</td>
<td>2467 MHz</td>
</tr>
<tr>
<td>13</td>
<td>2472 MHz</td>
</tr>
<tr>
<td>14</td>
<td>2484 MHz</td>
</tr>
</tbody>
</table>

- U.S. allows the use of channels 1 thru. 11.
- U.K. can use channels 1 through 13.
- Japan allows the use of all 14 channels.
Three Non-Overlapping DSSS Channels

Each Channel Bandwidth is about 22 MHz.
The OFDM Technology

- Orthogonal frequency division multiplexing (OFDM) divides a communication channel into a number of equally spaced subcarriers (sub-channels).
- Each subcarrier carries a part of the user information.
- Each subcarrier is orthogonal (independent of each other) to every other subcarrier.
Orthogonal Vectors

- Two vectors are orthogonal to each other if their dot product is zero.
- Assume that \( V=(v_1,v_2) \) and \( W=(w_1,w_2) \) are two vectors. These vectors will be orthogonal to each other if their dot product \( V.W=v_1*w_1+v_2*w_2 = 0 \).
- Example: \( V=(1,1) \) and \( W=(1,-1) \) are orthogonal to each other because \( V.W=1*1+1*(-1)=1-1=0 \).
Orthogonal Frequencies

- Two sinusoids of frequencies $f_1$ and $f_2$ are orthogonal to each other if $f_1$ and $f_2$ can be expressed as $f_1=n*f_0$ and $f_2=m*f_0$ where $n$ and $m$ are integers.
- In other words, all harmonics of $f_0$ are orthogonal to each other.
- Let $S_1=A_1\sin(2\pi nf_0 t+a_1)$ and $S_2=A_2\sin(2\pi mf_0 t+a_2)$. Then, it can be shown that the area under the curve $S_1*S_2$ for one cycle of $f_0$ is zero. This concept is similar to the dot product of two vectors being zero.
- Thus, $S_1$ and $S_2$ are orthogonal to each other.
Orthogonal Frequencies Don’t Interfere with Each Other

- Two orthogonal vectors are independent of each other.
- Similarly two orthogonal frequencies are independent of each other and they don’t interfere with each other.
- This is the reason why orthogonal sub-channels are used in OFDM technology so that signals going through different sub-channels don’t interfere with each other.
Data Transmission using OFDM

- In OFDM technology, the bit string to be transmitted is broken down into $N$ ($N > 1$) bit strings. The $N$ bit strings are then transmitted in parallel through $N$ orthogonal sub-channels.

- An effective bit rate of $B$ bits/sec is achieved by sending the bit strings at $B/N$ bits/sec through each one of the $N$ sub-channels.
Data Transmission using OFDM

- Assume that 110101001110 is the bit stream to be transmitted. It is converted into four bit patterns: 101, 111, 001 and 100 via a serial-to-parallel converter and then sent through four sub-channels (N=4). *(1 bit/symbol)*

**Diagram:**
- **Bit String To Be Transmitted:** 110101001110
- **Serial to Parallel:**
  - 1st Sub-Channel: 101
  - 2nd Sub-Channel: 111
  - 3rd Sub-Channel: 001
  - 4th Sub-Channel: 100
- **Parallel to Serial:**
  - Received Bit String: 110101001110

**Legend:**
- **Transmitter**
- **Receiver**
Data Transmission using OFDM

The following figure shows that the original bit pattern 110101001110 is broken down into four bit patterns: 101, 111, 001 and 100 and then sent through four orthogonal sub-channels C1, C2, C3 and C4. (1 bit/symbol)
Advantages of OFDM

- Narrow bits are susceptible to various types of noise and multi-path effect resulting in high Bit Error Rate (BER).
- OFDM technology converts narrow bits into wider bits. Thus, BER is reduced.
Effect of Inter-Symbol Interference

- If data is transmitted using one channel, then BER will be high due to noise and inter-symbol interference. OFDM reduces BER by transmitting data over multiple sub-channels.

![Diagram showing Bit Patterns sent through orthogonal sub-channels and their BER](image)

BER: Bit Error Rate

Spread Spectrum and Wi-Fi Basics by Syed M. Mahmud
Wi-Fi Basics

- Wi-Fi is a wireless technology developed mainly for high-speed internet access.
- Today Wi-Fi units are installed in computers, cell phones, printers, scanners and many other peripheral devices.
- Wi-Fi devices are designed based on IEEE 802.11 standards.
Versions of IEEE 802.11 Standards

- **802.11a** uses OFDM technology and operates in the 5 GHz band with a maximum net data rate of 54 Mbits/sec.
- **802.11b** uses DSSS technology and operates in the 2.4 GHz band with a maximum net data rate of 11 Mbits/sec.
- **802.11g** uses OFDM technology and operates in the 2.4 GHz band with a maximum net data rate of 54 Mbits/sec.
- There are many more versions of 802.11.
802.11 Medium Access Control

- The 802.11 Medium Access Control (MAC) protocol has been designed to take care of the following needs:
  - reliable delivery mechanism for user data over noisy and unreliable wireless media
  - requires participation of all nodes
  - fair distribution of wireless bandwidth among all nodes
  - dealing with hidden node problem
Minimum Communication Requirements

- MAC protocol requires at least two frames: a frame sent from the source to the destination and an acknowledgment (ACK) from the destination.
- If the source does not get ACK, it tries to transmit again based on the algorithm of the MAC protocol.
- Retransmissions are necessary for reliable communications over noisy media.
The Hidden Node Problem

- The following figure shows that Node B is within the communication range of both nodes A and C but A and C aren’t within the range of each other. Since A and C are hidden from each other, they may try to send data to B at the same time.

The data at node B is unreadable as it is corrupted due to simultaneous transmissions from nodes A and C.
Solution to the Hidden Node Problem

- 802.11 MAC protocol addresses this problem by adding two additional frames called the *Request to Send* (RTS) and *Clear to Send* (CTS) frames. RTS and CTS frames are very short compared to a normal data frame.
- If A wants to send data to B, it will first send an RTS frame to B and then will wait for a CTS frame from B.
Solution to the Hidden Node Problem

- If both A and C send RTS frames to B at the same time, then there will be a collision. However, since RTS is a very short frame compared to a data frame, the collision will be for a short period of time.
- If B sends a CTS frame to A after receiving an RTS from A, node C will also detect that CTS frame.

As a result, node C will wait until the end of ACK frame from B after B received data from A.
Effects of RTS and CTS

- When node A sends an RTS frame, all nodes within the communication range of A hold their transmission until the communication between A and B is completed.
- Similarly when node B sends a CTS frame, all nodes within the range of B hold their transmission until the end of ACK frame from B.
RTS and CTS aren’t Always Necessary

- If all nodes are within the communication range of each other, then the hidden node problem doesn’t exist. As a result, RTS and CTS frames are not necessary.

Similarly, if the demand for the bandwidth from each node is low and the media is not frequently accessed by the nodes, then there is very little chance for collision. Thus, RTS and CTS are not necessary.
The MAC layer parameter *dot11RTSThreshold* indicates the minimum required length of a frame for the frame to be preceded by RTS and CTS frames. The default value of *dot11RTSThreshold* is 2347.

- If the length of a frame is shorter than *dot11RTSThreshold*, then it is a short frame. Otherwise, it is a long frame.
- Short frames are not preceded by RTS and CTS frames.
Retransmission of Frames

- A node transmits a frame several times before it receives an **ACK** frame.
- Short frames are transmitted fewer times than long frames as the probability of a long frame getting corrupted by noise and interference is high.
Retry Counters

- A frame is associated with two retry counters: a *short retry counter* and a *long retry counter*.
- A short retry counter is used for short frames and a long retry counter is used for long frames.
- Two MAC layer parameters: `dot11ShortRetryLimit` and `dot11LongRetryLimit` indicate how many times a frame is to be transmitted before it is discarded.
Retry Counters

• Every time the transmission of a frame fails, the corresponding retry counter is incremented by 1.
• If a retry counter reaches its limit (\texttt{dot11ShortRetryLimit} or \texttt{dot11LongRetryLimit}), the frame is discarded.
• The higher layer of the network is notified that the transmission failed.
### General Frame Format

<table>
<thead>
<tr>
<th>FC</th>
<th>Duration /ID</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Sequence Control</th>
<th>Address 4</th>
<th>DATA</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>0-2312</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>

- **NAV information**
  - Or
  - Short Id for PS-Poll

- **Upper layer data**
  - 2048 byte max
  - 256 upper layer header

- **Protocol Version**
- **Frame Type and Sub Type**
- **To DS and From DS**
- **More Fragments**
- **Retry**
- **Power Management**
- **More Data**
- **WEP**
- **Order**

- **IEEE 48 bit address**
  - Individual/Group
  - Universal/Local

- **46 bit address**

- **MAC Service Data Units (MSDU)**
  - Sequence Number
  - Fragment Number

- **BSSID – BSS Identifier**
- **TA - Transmitter**
- **RA - Receiver**
- **SA - Source**
- **DA - Destination**

- **CCIT CRC-32 Polynomial**

---

*Spread Spectrum and Wi-Fi Basics by Syed M. Mahmud*
### RTS and CTS Frame Formats

#### RTS Frame:

<table>
<thead>
<tr>
<th>FC</th>
<th>Duration /ID</th>
<th>RA</th>
<th>TA</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>4</td>
</tr>
</tbody>
</table>

Duration = CTS + Data or Management Frame + ACK + 3 SIFS

#### CTS Frame:

<table>
<thead>
<tr>
<th>FC</th>
<th>Duration /ID</th>
<th>RA</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>4</td>
</tr>
</tbody>
</table>

Duration = Data or management frame + ACK + 2 SIFS
Basic Access Mechanism

- The basic access mechanism is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
- This requires each station to listen for other users.
- If the channel is idle for a certain time, the station may transmit.
- If the channel is busy, each station waits until transmission stops.
Network Allocation Vector (NAV)

- The Network Allocation Vector (NAV) is a virtual carrier sensing mechanism used with the 802.11 protocol.
- It limits the need for physical carrier sensing in order to save power.
- The MAC layer frame headers contain a **Duration** field that specifies the transmission time required for the frame, during which the medium will be busy.
Network Allocation Vector (NAV)

- The stations listening on the wireless medium read the Duration field and set their NAV, which is an indicator for a station on how long it must defer from accessing the medium.
- Wireless stations are often battery powered, so in order to conserve power the stations may enter a power-saving mode.
- A station decrements its NAV counter until it becomes zero, at which time they wakeup to sense the medium again.
Network Allocation Vector (NAV)

These nodes set NAV after hearing RTS

These nodes set NAV after hearing CTS
Inter Frame Space (IFS)

- **SIFS** - Short IFS, is used to separate transmissions belonging to a single dialog (e.g. RTS-CTS or Data-ACK), and is the minimum Inter Frame Space.
- The SIFS is long enough such that the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming packet.

![Diagram showing RTS-CTS and Data-ACK sequences with SIFS intervals.](Image)
Inter Frame Space (IFS)

- **DIFS** - Distributed IFS, is the Inter Frame Space used for a station willing to start a new transmission, which is calculated as SIFS plus two time slots.

\[
\text{DIFS} = \text{SIFS} + \text{Two Times Slots}
\]
Inter Frame Space (IFS)

- **PIFS** - Point Coordination IFS, is one time slot shorter than DIFS and it is used by the Access Point (or Point Coordinator), to gain access to the medium before any other station.

  \[
  \text{PIFS} = \text{DIFS} - \text{One Time Slot} \\
  = \text{SIFS} + \text{One Time Slot}
  \]

- Since all stations except the Access Point are required to wait for DIFS before they can transmit, the Access Point can get the medium before other nodes as PIFS < DIFS.
Inter Frame Space (IFS)

- **EIFS** - Extended IFS, which is a longer IFS used by a station that has received a packet that it could not understand. This is needed to prevent the station (which could not understand the duration information for the Virtual Carrier Sense) from colliding with a future packet belonging to the current dialog.
Distributed Coordination Function (DCF)

- A station (STA) having a packet to transmit checks the state of the medium.
- If the station senses a busy medium, it determines a random back-off period by setting an internal timer to an integer number of slot times.
- The back-off period is a randomly chosen integer over the interval \([0, CW]\). CW, known as the *Contention Window*, is restricted to lie between \(CW_{\text{min}}\) and \(CW_{\text{max}}\).
Distributed Coordination Function (DCF)

- The station defers until the medium is idle for one DIFS period.
- After that the internal back-off timer is decremented by 1 at every slot time during which the medium is idle.
- If the timer reaches zero, the station begins transmission.
- However, if the channel is seized by another station before the timer reaches zero, the timer setting is retained at the decremented value for subsequent transmission.
Distributed Coordination Function (DCF)

- After every successful transmission the value of CW is reset to $CW_{\text{min}}$.
- After every unsuccessful transmission the value of CW is doubled until CW reaches $CW_{\text{max}}$, and the retry counter of the frame is incremented by 1.
- The station attempts to retransmit the unsuccessful frame as long as its retry count does not reach retry count limits ($\text{dot11ShortRetryLimit}$ or $\text{dot11LongRetryLimit}$).
Timing of the 802.11 DCF

STA 3 is hidden to both STAs 1 and 2, and STA 6 is hidden to STA 2
(The following figure is a modified version of Fig. 2.3 of IEEE 802.11 Tutorial by Mustafa Ergen, June 2002)
Timing of the 802.11 DCF with EIFS

(This slide is made using Figure 2.7 of the Ph.D. Thesis of Mustafa Ergen, UC Berkley, Fall 2004)
Point Coordination Function (PCF)

- This Point Coordination Function enables the Access Point to access medium before other stations by the use of a smaller Inter Frame Space (PIFS).
- By using this higher priority access, the Access Point issues polling requests to the stations for data transmission, hence controlling medium access.