Today

- Wireless Communication
- Group Key Establishment
- IEEE 802.11
- Routing in mobile networks

Communication Terminology

- Communicate
  - Send/receive
    - Physical
    - Signal
  - Intent/interpretation
    - Logical
    - Crypto

Communication Terminology

- Unicast
  - To one node
- Broadcast
  - To everyone that:
    1. Can hear one send
    2. Can hear however
- Multicast
  - To a select set of those that can hear

Communication Terminology

- Communication group
  - Everyone in the group can receive and understand
  - No one not in the group can receive and understand
  - It is OK if some not in the group
    - Receive as long as they cannot understand
    - Could understand if they receive, but are guaranteed not to receive

Line-of-Sight Transmissions

- Radio
- Microwave
- Satellite
- Infrared
- Lazer
Wireless Technology Issues

- Signaling ➢ Device to Device
- Multiplexing ➢ Multiple link users
- Routing ➢ Inter-network communication

Radio Signals

- Energy Emissions into the environment
- May be
  - Impulses (discrete)
  - Continuous (waves)

Frequency Bands

- VLF ➢ 3-30 kHz
- LF ➢ 30 - 300 kHz
- MF ➢ 300 kHz - 3 MHz
- HF ➢ 3-30 MHz
- VHF ➢ 30 - 300 MHz
- UHF ➢ 300 MHz - 3 GHz
- SHF ➢ 3-30 GHz
- EHF ➢ 30-300 GHz

Signaling

- Radio Signals
- Frequency
- Modulation

Frequency

- For a sin wave, frequency measures the distance between peaks
- Wireless bandwidth is split up between frequencies

Frequency Uses

- AM Radio ➢ 535 kHz - 1.7 MHz
- Short-wave/CB radio ➢ 5.9 - 27.4 MHz
- Garage Door Openers ➢ 40 - 50 MHz
- Cordless phone ➢ 75 MHz
- FM Radio ➢ 88 - 108 MHz
- Radio controlled cars ➢ 824 - 849 MHz
- Cell Phones ➢ 900 MHz
- New Cordless Phones ➢ 960 - 1215 MHz
- Air Traffic Control ➢ 1227-1575 MHz
- GPS ➢ 30-300 GHz
Wireless Duplex Techniques

- Time Division Duplexing
- Frequency Division Duplexing

Multiple Access Techniques

- Frequency Division Multiple Access
- Spread Spectrum
- Time Division Multiple Access

FDMA

- Assigns individual channels to individual users
- The channel cannot be shared concurrently
- Channel use must be scheduled
- Channel latency results in lower throughput

Spread Spectrum

- 2.4 GHz
- Data is sent in small pieces over a number of the discrete frequencies
- Frequency hopping
  - Send a short burst of data
  - Shift frequencies
  - Send another short burst
  - Because they use any given frequency for such a short time, FHSS devices are less prone to interference

TDMA

- The allocated frequency is partitioned into time slots that are scheduled for use.
- Each user is allocated one or more cyclical, repeating time slots
- The system operates in a "burst and buffer" mode

Wireless Paradigms

- Short range
  - Cordless phones
  - PDAs
  - Garage door openers
- Mid range
  - Paging Systems
  - Cellular phones
- Long Range
  - Microwave Communications
  - Satellite Communications
  - Etc
Paging Systems
- Emphasis on reliability
- Simplex
- Low bandwidth
- High power transmission
- Simulcast by base stations

Cordless Telephone Systems
- Full duplex
- Short range
- Low power
- Single base station per handset

Cellular Phone Systems
- Full duplex
- High power
- Multiple base stations
- FDMA
- Frequency Reuse

Frequency Cells

Infrared Communications
- Light waves of a lower frequency than human eyes can receive and interpret
- Used
  - in most TV remote control systems
  - to connect some computers with peripheral devices
  - Hand-held devices
- Signaling: Pulses of light
Infrared Pros/Cons

- Cons
  - Short range
  - One-to-one
  - Line of sight
  - Directional

- Pros
  - Reliable
  - Inexpensive
  - Directional

Wireless Networking Architectures

- Fixed Point to point
- Broadcast
- Base Station with fixed remotes
- Base Stations with random remotes
- Combinations

Power Considerations

- Fixed sites
  - Suitable infrastructure available
  - Generator required
    - Fuel availability
- Mobile units
  - Motor availability
  - Battery availability
    - Weight limitations
    - Size limitations
    - Battery life
    - Recharge capabilities

Group Communication

- Communication controlled
  - Only group members GET group messages
- Crypto controlled
  - Only group members UNDERSTAND the messages

Crypto Key Uses

- Authentication
- Session key
- Key distribution key
- Group Communications
- Etc.

Secure Groups in Ad hoc Networks

- Cryptographic protocols
- Requirements
  - Distributed
  - Efficient
  - Contributory

No Structure Required
Group Key Establishment

- “Key Agreement in Dynamic Peer Groups” by Michael Steiner, Gene Tsudik, and Michael Waidner, August 2000
- “A Secure and Efficient Conference Key Distribution System”, M. Burmester and Y. Desmedt, 1995

A Family of Secure Group Protocols for Ad hoc Networks

- Foundational Protocol
- Member Join
- Member Exclusion
- Authenticated member join

Key Management

- Generation
- Distribution
- Replacement/change

Foundational Protocol

\[ K = g^{F \cdot z}, \text{ where} \]
\[ F = f(g^{x_1}, ..., g^{x_n}) \]

C -> Gm: e[z]g^{x_1}, ..., e[z]g^{x_n}  
Gm -> C: g, p, gx_0  
C -> bc: e[z]gx_0, ... , e[z]gx_n

Number of Messages

- Coordinator: 2
- Group Members: 1 each
- For n members: n + 2

Protocol Strength

- Diffie-Hellman Key (g^x \mod p)
- x must be:
  - Random
  - Contributory
  - Computable by all members
Functions $f$ and $g^{f(x_1...x_n)} z \mod p$

1. $f = \text{secure hash, and}$
   $= \text{multiplication}$
2. $= \text{exclusive-or and}$
   $f = \text{multiplication mod } p$

Member Exclusion

$K = g^F z$, where
$F = f(g^{x_1}, ..., g^{x_n}) \text{ (less } g^{x_i})$

C-> be: $g^{x_i}, e[z]g^{x_1}, \ldots, e[z]g^{x_n}$

Excluded node

CLIQUES

- M4 will compute and broadcast intermediate values to group
- M4 $\rightarrow$ M1 ($g^{n_2n_3n_4n}$)
- M4 $\rightarrow$ M2 ($g^{n_1n_3n_4n}$)
- M4 $\rightarrow$ M3 ($g^{n_1n_2n_4n}$)

$M_n$ will have the last cardinal value and therefore is the first member to compute the key $K$

802.11

- Provides mechanisms to provide a secure wireless network environment
- Introduced Wired Equivalency Privacy (WEP)
  - Protects link-level data during wireless transmission
  - Protects data confidentiality against passive eavesdropping
  - Attempted to make wireless privacy = wired/ethernet privacy

802.11- WEP

- Security Goals
  - Confidentiality
    • prevent casual eavesdropping
  - Access Control
    • protect access to wireless network infrastructure
  - Data Integrity
    • prevent tampering with transmitted messages
    • integrity checksum used for this purpose
  - In all 3 cases, security lies in difficulty of discovering key through brute-force attack

802.11- WEP

- WEP relies on a secret key $k$
  - shared between communicating parties
  - used to protect body of transmitted frame of data
- Encryption of the frame is:
  - Checksumming
  - Encryption
  - Transmission
802.11-WEP Picture

Plaintext

\[
\begin{array}{|c|c|}
\hline
\text{Message} & \text{CRC} \\
\hline
\end{array}
\]

\[\text{Keystream} = \text{RC4}(v,k)\]

\[v \quad \text{Ciphertext}\]

Transmitted Data

802.11-WEP

- WEP standard only specifies 40 bit key
  - makes brute-force attacks rather simple
  - there are extensions
- Many attacks are not based on the size of the key

802.11 Modes

- Works in two modes:
  - ad-hoc mode
    - Independent Basic Service Set (IBSS)
    - client communicates directly with other clients
    - only clients within transmission range (cell) of each other can communicate
  - infrastructure mode
    - Basic Service Set (BSS)
    - client communicates with central station which forwards communication

802.11 Security Association

- Prior to communication, entities must establish an association
  - Three states
    - Unauthenticated and unassociated
    - Authenticated and associated
    - Authenticated and associated
  - To transition between states using frames
    - management
    - data

802.11 Flaws

- Allows eavesdropping
- Allows tampering
- Provides limited confidentiality
- Allows misuse of network
802.11 - RC4 Flaw

- RC4 is the stream cipher used in the encryption of data in 802.11
- Weaknesses:
  - existence of large classes of weak keys
  - small part of secret key determines a large number of bits in initial permutation
  - key vulnerability
    - when part of the key is exposed to attacker

802.11 - Effectiveness

- None of the three security goals attained
  - Practical attacks allow eavesdropping
  - It is possible to subvert the integrity checksum field (modify messages)
  - New traffic can be injected into the network

802.11 - Summary

Problems:
- Use of RC4 stream cipher
- Link-layer difficult to protect
- Use of checksum instead of MAC
- No key management specified
- Keystream reuse is common

802.1X

- After the problems with 802.11, 802.1X was developed
  - Is used in combination with 802.11
  - Provides architectural framework for authentication methods
- 802.1X introduced the Robust Security Network (RSN)
  - control access
  - provide authentication
  - key management