Chapter 16

Recent Advances
Outline

- Introduction
- Femtocell Network
- Ultra-Wideband Technology
- Push-to-Talk (PTT) Technology
- RFID
- Cognitive Radio
- Multimedia Services Requirements
- Wireless Heterogeneous Networks
- Mobility and Resource Management for Integrated Systems
- Multicast in Wireless Networks
- Directional and Smart Antennas
- WiMAX and Major Standards
- Low Power Design
- XML
- DDoS Attack Detection
Need for Femtocell

- Advanced cellular standards such as 3GPP’s UMTS and LTE; 3GPP2’s CDMA2000, 1x, EVDO and WiMAX
- High data rate and seamless coverage important objective
- Signal strength is weak inside buildings
- More than 50% voice call and more than 70% data traffic start from an indoor environment
- Easier solution is to deploy some indoor devices serving only the indoor users
- Femtocell Network is an effective way to remedy coverage holes
Femtocell

Telephony Core Network

Internet

M-BS

F-BS

MS

FGW

F-BS

MS

Wired Connection

Wireless Connection

F-BS: Femtocell Base Station
FGW: Femtocell Gateway
M-BS: Macrocell Base Station
MS: User Mobile Station
Femtocell Characteristics

- Femtocell Base Station (F-BS)
  - Wireless Interface
  - Internet Interface
- Internet Link
- Femtocell Gateway (FGW)
- Benefits of Femtocell Network
  - Better and seamless coverage
  - Enhanced capacity
  - Lower transmit power
  - Prolong handset battery life
  - Higher signal-to-interference-noise ratio (SINR)
- Hand off
- Synchronization
- Self-Configuration, Self-Operation and Location Tracking
- Security Issues

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Femtocell</th>
<th>Macrocell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air interface</td>
<td>Telecommunication standard</td>
<td>Telecommunication standard</td>
</tr>
<tr>
<td>Backhaul</td>
<td>Broadband Internet</td>
<td>Telephony network</td>
</tr>
<tr>
<td>Cost</td>
<td>$200/year</td>
<td>$60,000/year</td>
</tr>
<tr>
<td>UE</td>
<td>Power consumption low</td>
<td>high</td>
</tr>
<tr>
<td>Radio Range</td>
<td>10-50 meters</td>
<td>300-2000 meters</td>
</tr>
</tbody>
</table>
Ultra-Wideband Technology (UWB)

- **UWB Radio**: Radio System having large bandwidth.
  - Bandwidth > 25% of center frequency or > 1 GHz.
- Wide bandwidth makes it possible to share spectrum with other users with certain co-coverage sense.
- Wide band signals are naturally suited for location determination applications.
UWB Basics - TM-UWB

- Basic element: Ultra short monocycle wavelet
  - Wavelet pulse width between 0.2 and 1.5 nsecs
  - Center frequency between 5 GHz and 600 MHz
  - Pulse-to-pulse interval between 25 and 1000 nsecs
- System uses pulse position modulation
- No Intermediate frequency stage
  - Reduces complexity
- Single bit of information is spread over multiple monocycels
TM-UWB Modulation and DSC-UWB

- **Pulse position modulation**
  - Positions signal one quarter cycle early or late relative to the nominal PN coded location or pulse polarity
  - Modulation further smoothes the spectrum of the signal, thus making the system less detectable

- **DSC-UWB**
  - Wavelet pulse trains at duty cycles approaching that of a sine wave carrier are direct sequence modulated to spread the signal. A PN sequence provides spectrum spreading, channelization and modulation
UWB Signal Propagation

- Generally follow a free space propagation law
- Millions of coded pulses transmitted per second
- Emissions below conventional receiver noise floor and across an ultra wide bandwidth
- Very low extant RF signature, providing intrinsically secure transmissions
- Low probability of detection and interception
UWB Applications

- **Communications:**
  - Noise like spectral characteristics of UWB signals enables secure communication with less detection
  - Suitable for robust in-building communications

- **Advanced Radar Sensing:**
  - Through the wall radar, terrain mapping radar, ground penetrating radar

- **Precision Location and Tracking:**
  - Remote, secure and real time tracking system
Difference Between UWB and Spread Spectrum Techniques

- **UWB uses an extremely wide band of RF spectrum to transmit more data in a given period of time, which is a time-domain concept**

- **Spread spectrum technique, including direct sequence spread spectrum or frequency hopping spread spectrum, is a transforming technique in frequency domain**
UWB Advantages & Limitations

- UWB radio systems have large bandwidth ( > 1 GHz).
- UWB has potential to address today’s “spectrum drought”
- Emissions below conventional level
- Single technology with 3 distinct capabilities
- Secure transmission, low probability of interception or detection and anti-jam immunity
- Not appropriate for a WAN (Wide Area Network) deployment such as wireless broadband access
- UWB devices are power limited
Push-to-Talk (PTT) Technology

- PTT is a “walkie-talkie-type” service implemented over cellular networks (P2T, PoC)
- PTT terminal have a PTT button that a user presses to start a direct conversation with each other
- PTT is a quick, short and spontaneous communication from user’s perspective
- PTT is an add-on feature to normal cell phones, also considered as a front-runner in peer-to-peer service over IP
PTT Technology

- Two kinds of PTT, one is iDEN by Motorola and Nextel and the other is in non-iDEN (PoC)

- iDEN
  - Has its own network that has its own frequencies and equipment
  - Uses TDMA
  - A direct connect call uses only a single frequency

- PoC
  - Uses GPRS network to send packetized speech
  - Signaling architecture is based on SIP

- Limitation of current services
  - Latency
  - Cost, new handset required
  - Quality of PTT service needs to be improved
PoC Architecture

It: Floor control and media
In: Proxy to proxy session signaling
In: Proxy to proxy session signaling
Itn: Floor control and media
Is: PoC client to proxies session signaling
Im: Group mgmt to PoC client
Ik: Group mgmt to PoC server
Igs: Group mgmt to PoC server
Ips: Group mgmt to PoC server
Ie: GLMS management/administration

Interface(s)

Copyright © 2011, Dr. Dharma P. Agrawal and Dr. Qing-An Zeng. All rights reserved.
RFID

- Radio Frequency Identification Tag (RFID) is a bar code with encoded intelligent data waiting to be read
- Many applications such as tracking items in a supply chain, embedded RFID tag in a passport, any generic access control like entry to a building or an office or an elevator or a parking area
- Receives energy from the electromagnetic waves that a card reader emits
- Passive has a detection range of about 20 feet
- Active and Semi-passive RFIDs can be detected from farther away as much as up to 100 feet or more away
- Already deployed on a large scale such as by Wal-Mart, Sam’s club, and the Department of Defense
- Tasks such as checking in, finding the location of books in a particular shelf, checking out books at the library or groceries at the counter
- Development of smart surgical sponges
RFID Tag and Scanner

RFID Tag

RFID Scanner
Cognitive Radio

- Constrained bandwidth poses a serious hindrance to communication networks
- Television bands exhibit stretches of white spaces
- These white spaces seem to be a panacea for increasing spectrum utilization
- CR is to sense white spaces and opportunistically allocate unused spectrum to unlicensed users
- Spectral occupancy by primary users exhibit dynamical spatial and temporal properties

Spectrum Utilization in 700-800 MHz band in Hoboken, NJ over 14 hours period
Cognitive Radio

- Adaptive spectrum sensing implies that the spectrum sensing is performed selectively and with a-priori data information
- Spectrum sensing techniques focus on reducing probability of misdetection and probability of false alarm
- Cooperative sharing of spectrum among secondary users leads to maximum utilization of licensed spectra

Functionality of Cognitive Radio for Secondary users
Multimedia Service Requirements

- Two trends distinguish multimedia requirements with respect to telecommunications – increasing demand for bandwidth, and a transparent support for user mobility
- On today’s internet, 90% of the traffic uses TCP, while 80% of the networking is done over the IP network
- Hence, multimedia streaming over IP has become a major issue
- The QoS of a network is defined by various parameters such as bandwidth, latency, jitter, packet loss and packet delay
Multimedia Service Requirements

- ETSI has introduced four classes of services with class 1 being best service and class 4 being QoS guaranteed service.
- Some standards need to be defined in the following areas to form complete streaming systems – media codecs, transport protocols, media control, file formats, capability exchange, and metadata.
- Media codecs are comprised of MPEG-1, MPEG-2, and MPEG-4.
- MPEG-1 and MPEG-2 are limited to audio/video compression.
Multimedia Service Requirements

- MPEG-4 on the other hand describes the coded representation of natural and synthetic multimedia objects
- The objects may include images, video, audio, text, graphics, and animation
- MPEG-4 audio capabilities include tools for speech, audio, voice synthesis, composition and scalability
- Two file formats are found in MPEG-4. One is based on the Apple quick time format and the other is based on the Microsoft ASF (Advanced Stream Format)
Multimedia Service Requirements

- HTTP (Hyper Text Transfer Protocol) is a very simple and widely used way to stream media files.
- Works with regular web servers and does not require a special media server.
- In MPEG-4 systems, the transport streams is divided into 4 layers – compression layer, synchronization layer, flexmux layer and transport layer.
- A media control protocol needs to support issues of file seek, bandwidth scalability and live streaming.
Some Multimedia Protocols

- The Real-time streaming protocol (RTSP) establishes and controls time synchronized streams of continuous media such as audio and video.
- The Session initiating protocol (SIP) is an application-layer control protocol for creating, modifying and terminating sessions with one or more users.
- IP broad-band networks have also caught the attention of researchers in recent times.
Multimedia Messaging Service (MMS)

- MMS is significant enhancement to current SMS service, which allows only text
- MMS allows text, sound clips, video clips etc
- Although MMS is targeted toward 3G network, it has been deployed on network using WAP
- Possible application: next generation voicemail, immediate messaging, choosing how, when, and where to view the messages, mobile fax, sending multimedia postcards
Multimedia Transmission in MANETs

- Varying bandwidth capacity, different end-to-end delay, and path lifetime channels introduce real challenges in realizing desired QoS
- Major limitation for real-time video information over MANETs is the link reliability
- QoS routing in MANET can be supported by employing a dynamic channel assignment
Effect of Route change on Video Frame in a MANET

(Switched P-frame prediction option)

Encoded frame Prior to link failure

Link failure occurs within this frame

Link failure is detected

New route Is formed

Next coding frame

RTP Video data

RTP Redundant

RTP Redundant

RTP Redundant

RTP Video data

RTP Video data

RTP Redundant

RTP Redundant

RTP Video data
Heterogeneous Networks

- Rapid developments is creating new possibilities of integrating existing networks to provide seamless service to users.
- Future networking environment will be heterogeneous using different access technologies, like WWAN, WMAN, WPAN, etc.
Heterogeneous Network

- To provide an “Always Best Connected”
- Migrating current technologies to suit the requirements of the future is a challenging task
- Salient features of forthcoming heterogeneous wireless networks:
  - Multi-network
  - Architecture
  - Multi-mode terminal
  - Multi-service

Specific challenges are:
- Network Discovery
- Network Selection
- Mobility
- Network Infrastructure
- Security
- Billing
- Quality of Service
Mobility and Resource Management for Integrated System

- The next generation of wireless mobile networks have been designed to support both real-time and non real-time service.

- Mobility management has to be taken into consideration while designing the infrastructure.

- Mobility management features two tasks - location management and handoff management.

- Efficient handoff design schemes are essential in ensuring good QoS in integrated wireless networks.

- Criteria for handoff initiation need to be selected carefully.
Mobility Management

- Some handoff criteria currently in use are word error indicator, received signal strength and quality indicator.

- Handoff strategy for integrated wireless networks has to be different for different services. As an example, handoff interruptions in real-time services are very undesirable.

- On the other hand, interruptions are not so critical in non real-time applications.

- In order to provide better QoS with limited frequency spectrum reuse, various handoff schemes have been proposed.
Resource Management

- Some guard channels in each BS are reserved for handoff request calls. Such a request will have a higher priority over an originating call.
- The guard channels are subject to availability.
- In a queuing based priority handoff scheme, each BS has one or more queuing buffers for all incoming calls. A call is serviced immediately if there is an available channel.
- Otherwise, the call is stored in a queue and is not dropped/blocked.
- When a channel is released, the first call in the queue is picked.
The queue operates on a first-in-first-out basis

Current issues of interest are: How many queues should be allocated to a BS, and what kind of service call should be included into the queue?

One way of giving priority reservation to real-time service handoff requests is to reserve a number of channels for real-time service handoff requests

Queues are allowed for real-time service handoff requests and non-real-time service handoff requests

A non-real-time request can be transferred to another queue when the MS moves out of the cell
A service dependent priority handoff scheme for integrated wireless networks has been proposed.

Calls are divided into four different service types: originating real-time service calls, originating non-real-time service calls, non real-time service handoff request calls and real-time service handoff request calls.

Correspondingly, the channels in each cell are divided into three groups, one each for real-time service calls, non real-time service calls and overflowed handoff requests from the previous two groups.
Resource Management

- Some channels are reserved exclusively for real-time service handoff requests
- Hence, real-time service handoff requests have priority over non-real-time service handoff requests and all handoff requests have priority over originating calls
- Current issues of interest include the introduction of a preemptive priority procedure that gives real-time service handoff requests a higher priority over non-real-time service handoff requests
- Individual queues will be added for both real-time and non-real-time requests
Resource Management

The non real-time service handoff requests waiting in the queue can be transferred from the current base station to one of the target base stations when the mobile user moves out of the current cell before it gets service.
Multicast in Wireless Networks

- IETF has proposed two methods to support multicast over Mobile IP: remote subscription and bidirectional tunneling (BT)
- Enhancement of MoM, called range-based MoM (RBMoM), provides a tradeoff between the shortest delivery path and the frequency of the multicast tree reconfiguration
- It selects a router, called the multicast home agent (MHA), which is responsible for tunneling multicast packets to the MS’s currently subscribed FA
Multicast in Wireless Networks

- **Range Based MoM (RBMoM)**
  - An enhancement of MoM
  - RBMoM provides a trade off between the shortest delivery path and the frequency of the multicast tree reconfiguration
  - It selects a router called multicast home agent (MHA), which is responsible for tunneling multicast packets to FA to which the MH is currently subscribed within its service range
  - If a mobile host is out of service range, then an MHA handoff will occur
  - Every MH can have only one MHA, which changes dynamically as per the location of the MH, whereas the HA of an MH never changes
Multicast in Wireless Networks

- Multicast for Mobility Protocol (MMP):
  - It combines Mobile IP and CBT where the former controls communication up to the foreign network, and the latter manages movement of hosts inside them
  - It assumes the foreign domain to form a hierarchy of multicast supporting routers
  - Similar to the concept of FA, base stations acting as a multicast router transmit periodic beacons, which include one multicast care-of address
Multicast in Wireless Networks

- Mobicast
  - Designed for an inter-network environment with small wireless cells
  - Assume that a set of cells are grouped together and are served by a domain foreign agent (DFA)
  - DFA serves as multicast forwarding agents and isolate the mobility of the mobile host from the main multicast delivery tree
  - Mobicast is based on an IETF proposed method to support multicast over Mobile-IP
Handling Multicast with Source Movement

- Remote subscription (receiving packets)
- Reverse tunnel (sending packets)

(a) Initial multicast tree
(b) Tree after source movement
Multicast in Wireless Networks

- Reliable Multicast Data Distribution Protocol (RMDP):
  - Uses Forward Error Correction (FEC) and Automatic Retransmission reQuest (ARQ) information to provide reliable transfer. Redundant information is inserted into the FEC, often enabling a receiver to reconstruct the original packet.
  - In the event that such information is not enough, an ARQ is sent to the multicast source which in turn, multicasts the requested packet to all receivers.
Reliable Multicast Data Distribution Protocol (RMDP) (cont’d):

- In RMDP, a data object to be transmitted is a file, identified by a unique name, say its Uniform Resource Locator (URL).

- The file has a finite size, and is split into packets of \( s \) bytes each. RMDP uses an \((n, k)\) encoder with \( n >>> k \) to generate packets for transmission, and assumes the existence of a multicast network which provides unreliable, but efficient delivery of data packets.
Reliable Multicast Data Distribution Protocol (RMDP) (cont’d):

- Limitations:
  - In RMDP, data encoding/decoding is done through software resulting in a processing overhead and, therefore, performance degradation
  - In case of burst errors, a lot of ARQ packets are generated. This triggers a substantial amount of retransmission packets, which are multicast to all receivers
Reliable Mobile Multicast Protocol (RM2):

- RM2 is a hierarchical protocol, which divides a multicast tree into sub-trees where subcasting within these smaller regions is applied using a tree of retransmission servers (RSs)

- RS have a retransmission subcast address shared by its members and which may be dynamically configured using IETF’s MADCAP (Multicast Address Dynamic Client Allocation Protocol)
Reliable Mobile Multicast Protocol (RM2) (cont..):

- In order to guarantee end-to-end reliability, the receivers are required to send NACKs, pointing out the packets to be retransmitted. In other words, RM2 implements selective packet retransmission.

- RM2 adopts a retransmission algorithm that dynamically switches between unicast and multicast modes to save network and wireless resources.
### Multicast in Wireless Networks

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Optimal Routing</th>
<th>Reliability</th>
<th>Packet Redundancy</th>
<th>Multicast Protocol Dependency</th>
<th>Join &amp; Graft delays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Subscription</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Independent</td>
<td>Yes</td>
</tr>
<tr>
<td>Bi-directional Tunneling</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Independent</td>
<td>No</td>
</tr>
<tr>
<td>MoM</td>
<td>No</td>
<td>No</td>
<td>Minimal</td>
<td>Independent</td>
<td>No</td>
</tr>
<tr>
<td>MMP</td>
<td>No</td>
<td>No</td>
<td>Minimal</td>
<td>CBT</td>
<td>No</td>
</tr>
<tr>
<td>Mobicast</td>
<td>Yes</td>
<td>No</td>
<td>Minimal</td>
<td>Independent</td>
<td>Yes</td>
</tr>
<tr>
<td>RMDP</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Independent</td>
<td>Yes</td>
</tr>
<tr>
<td>RM2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Independent</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Broadcasting in a cellular network is relatively easier than in an ad hoc network

Only one channel is used in CSMA/CA mode for communication

It is relatively hard to have a global knowledge of ad hoc network topology

When a device transmits a message to all its neighbors within its transmission distance, then the question is which receiving device ought to be allowed to rebroadcast

This selection is difficult and requires a global network connectivity information
Broadcasting steps in Ad hoc Networks

Step 1

Coverage Area For node A

Green area covered by device A in step 1

Step 2

Coverage area for node F

Copyright © 2011, Dr. Dharma P. Agrawal and Dr. Qing-An Zeng. All rights reserved.
Ad hoc Connectivity for Broadcasting

Device Connectivity and Comparison with Neighboring Devices for Broadcasting

<table>
<thead>
<tr>
<th>Device</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighboring Devices</td>
<td>BCD</td>
<td>EF</td>
<td>ACF</td>
<td>GH</td>
<td>AB</td>
<td>DH</td>
<td>ACE</td>
<td>JK</td>
<td>ADF</td>
<td>L</td>
<td>ABE</td>
<td>GO</td>
<td>BF</td>
<td>HO</td>
<td>Q</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connectivity</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Connectivity as compared to neighboring devices</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Very Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>
Directional and Smart Antennas

- Directional antennas in MANETs can reduce the coverage of silence zones and allow neighboring nodes to communicate simultaneously, thereby enhancing system throughput.

- Types of antennas
  - Omnidirectional antenna
  - Directional antenna
  - Smart antenna
Communication with Directional Antenna

Range of node B

Range of node F

Silenced nodes
Communication with Directional Antennas

Not possible with omni-directional antennas
Smart Antenna

- **Beamforming**
  - Antenna system focuses the maxima gain toward the desired user while minimizing the impact of noise, interference, and other effects from undesired users

- **Switched-beam and Adaptive Beam**
  - Switched-beam consists a set of predefined beam which have a narrow main lobe and small sidelobes
  - Adaptive-beam can steer the main lobe of the beam in the direction of the desired user and nulls in the direction of interference users

- **SDMA (Space division multiplexing access)**
  - Spatial multiplexing and demultiplexing
Basic function of Smart Antenna

Omni-directional Transmission of RTR packet by R

Directional Reception of RTS packets by R

Directional Transmission of CTS packets by R

Directional Reception of DATA packets by R

Directional Transmission of ACK packets by R
WiMAX and Major Standards

- IEEE 802.16 is a set of standards on broadband wireless access
- Offers an alternative to cable based access networks without any costly infrastructure
- Designed to evolve as a set of air interfaces based on a common MAC protocols but with
- Physical layer specifications depend on used spectrum and associated regulations
- Developed with five criteria:
  - Broad market potential
  - Compatibility
  - Distinct identity
  - Technical feasibility
  - Economic feasibility
IEEE 802.16j

- It offers many economic benefits:
  - Wireless backhaul
  - Better trunking efficiency at aggregate points
  - Lower site acquisition costs
  - Lower cost and complexity of RS
  - Faster deployment
IEEE 802.16m

- It provides an advanced air interface for operation in licensed bands
- Operating frequencies:
  - 450-470 MHz
  - 698-960 MHz
  - 1710-2025 MHz
  - 2110-2200 MHz
  - 2300-2400 MHz
  - 2500-2690 MHz
  - 3400-3600 MHz
- Operating bandwidths: supports from 5 to 40 MHz
- Duplex schemes
- Support for advanced antenna techniques
- Support for government mandates and public safety
Need for Low Power Design

- Limited energy of ad hoc and sensor network nodes.
- Not easily replaceable after deployment in forests and oceans.
- Slow progress in battery technology.
- Most of the times wireless devices are in a idle state or doing very trivial work.
Power Conservation Approaches

- Turning off hardware if not in use (display screens etc)
- Going to sleep during idle periods
- Reducing the voltage supply during periods of low power operations
Dynamic Voltage Scaling (DVS)

- For a sensor node processor consumes 30-50% of the battery power
- DVS is conserving processor power without significant performance degradation
- \( P_{\text{dynamic}} \propto CV_{dd}^2 f \)
  where, \( C \): capacitance, \( f \): frequency, \( V_{dd} \): supply voltage
- Therefore, reducing voltage reduces power consumption
- Transmeta TM5400 or the “Crusoe” is the one of the few processors which supports voltage scaling
Future Applications

- The need for the power conservation will increase for future video processing applications by wireless nodes
- Other applications such as image processing and sound processing will also need more power
- Therefore, conserving power is one of the important research areas today
XML

- Programming versus Markup Language
  - One Process data and other Presents Data
- SGML
- Why XML, Why not Html?
  - Html instructs Web Browser
  - XML is low level syntax for representing structured data and this simple syntax could be used to support a wide variety of applications
WML

- XML Application
- Designed for low bandwidth and small display devices
- Deck of cards concept
- Multiple Screens in single retrieval
- Predefined set of elements
DDoS Attack Detection

- Due to its dynamic topology, security issues in MANETs, WSNs, and WMNs are multidimensional
- DoS attack flow incessantly pumps traffic into the network to cause congestion
- Distributed DoS (DDoS) attack is a more virulent model; where an attack is launched synchronously from several compromised innocent hosts piloted by a remotely hidden attacker
- Correlations among its features which provide additional information to flag changes between normal and attack conditions
DDoS Attack Detection

The steps are:

1. Assume there are \( p \) features, \( f_1 \ldots f_p \), which compose a random vector 
   \( X = (f_1, \ldots, f_p)^T \)

2. \( x_1, \ldots, x_n \) are the \( n \) observed vectors, \( x_i = (f_1^i, \ldots, f_p^i) \) is the \( i \)th 
   observed vectors

3. \( f_{ij}^l \) is the value of \( f_i \) in the \( j \)th observation during the \( l \)th time interval \( T_l \)

4. Define a new variable \( y \) and the covariance matrix \( M \) to characterize the 
   variable \( y \)

\[
\begin{bmatrix}
  f_1^{l,1} & \ldots & f_p^{l,1} \\
  f_1^{l,2} & \ldots & f_p^{l,2} \\
  \vdots & & \vdots \\
  f_1^{l,n} & \ldots & f_p^{l,n}
\end{bmatrix}
\]

\[
\begin{bmatrix}
  \sigma & \sigma & \ldots & \sigma \\
  \sigma & \sigma & \ldots & \sigma \\
  \vdots & \vdots & & \vdots \\
  \sigma & \sigma & \ldots & \sigma
\end{bmatrix}
\]

Copyright © 2011, Dr. Dharma P. Agrawal and Dr. Qing-An Zeng. All rights reserved.
The steps are:

5. Define variable $z_l$ as the distance between two matrices $M_{yl}$ and the mean of $M_{yl}$ or $E(M_{yl})$ as $z_l = \| M_{yl} - E(M_{yl}) \|$, where $z_l$ measures the anomaly.

6. To simplify the problem description, the distance between the two matrices is calculated as

$$\| M_1 - M_2 \| = \sqrt{\sum_{i,j \leq p} (a_{i,j} - b_{i,j})^2}, \quad \forall a_{i,j} \in M_1, \quad \forall b_{i,j} \in M_2, l \leq i, j \leq p$$

7. In the normal situation, one can find a point $c$ and a constant $a$ for $z_l$ in step (5), which satisfies $|z_l - c| < a$, $\forall l \in Z$.

8. The constant $a$ is selected as the upper threshold of the i.i.d. $|z_l - c|$.

9. Calculate the corresponding $z_l$ for the observed data gathered during the $l$th time interval, if $|z_l - c| > a$, the abnormal behaviors could be determined. Assume there are $p$ features, $f_1 \ldots f_p$, which compose a random vector $X=(f_1, \ldots, f_p)^T$. 

Copyright © 2011, Dr. Dharma P. Agrawal and Dr. Qing-An Zeng. All rights reserved.
DDoS Attack Detection

- **SYN flooding detection**
  - Use of the covariance of each pair of six flags detects the SYN flooding attacks

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URG</td>
<td>The value of urgent pointer field is valid</td>
</tr>
<tr>
<td>ACK</td>
<td>The value of acknowledgement field is valid</td>
</tr>
<tr>
<td>PSH</td>
<td>Push the data</td>
</tr>
<tr>
<td>RST</td>
<td>The connection must be reset</td>
</tr>
<tr>
<td>SYN</td>
<td>Synchronize sequence numbers during connection</td>
</tr>
<tr>
<td>FIN</td>
<td>Terminate the connection</td>
</tr>
</tbody>
</table>

- **Mobile Agent Intrusion Detection System: A Non-overlapping Zone Approach**
  - Light-weight mobile agent (MA) is used as an alternative hierarchical distributed model
  - MA’s can collect and analyze along with the alert and alarm messages
  - Dependency and de-centralized administration of MANET gives a chance to adversaries to exploit new type of attacks
DDoS: Zone-Based IDS

- Two levels of hierarchical structure are defined by dividing into non-overlapping geographically partitioned zones.
- Two major components for each IDS, that is, GIDS (Gateway Intrusion Detection System) and LIDS (Local Intrusion Detection System).
- Every mobile node runs a LIDS locally to perform local data collection and anomaly detection.
- Zone manager agent.