Security in SDR & cognitive radio

Ali Shamsizadeh

Summer 2009

Introduction

- Background on Network Security
- Security Concerns in Mobile Systems
- Security in SDR
- Secure Software Download in SDR
- Security in Cognitive Radio
- Security Threats in Cognitive Radio Networks

Background on Network Security

- **Authentication**:

  “Who are you?”

- **Authorization**:

  “Should you be doing that?”

- **Confidentiality**:

  “If someone gets the packets, can they recover the information?”

- **Integrity**:

  “Is what I get really what I should get?”

Background on Network Security

Hostile environment

- A third party might want to disturb communication
- Attacks might be against
  - confidentiality
  - integrity
  - originality
  - Or the service (denial of service)

Background on Network Security

Application security requirements

- Eavesdropping protection

(encryption)

- Impersonation and integrity protection

(authenticated and hashed messages)

- Denial of service protection
- Secure device configuration and user identification
- Security for an unreliable channel

Security Concerns in Mobile Systems

- User identification
- Secure storage
- A secure software execution environment
- tamper-resistant system
- Secure network access
- Secure data communications
- Content security

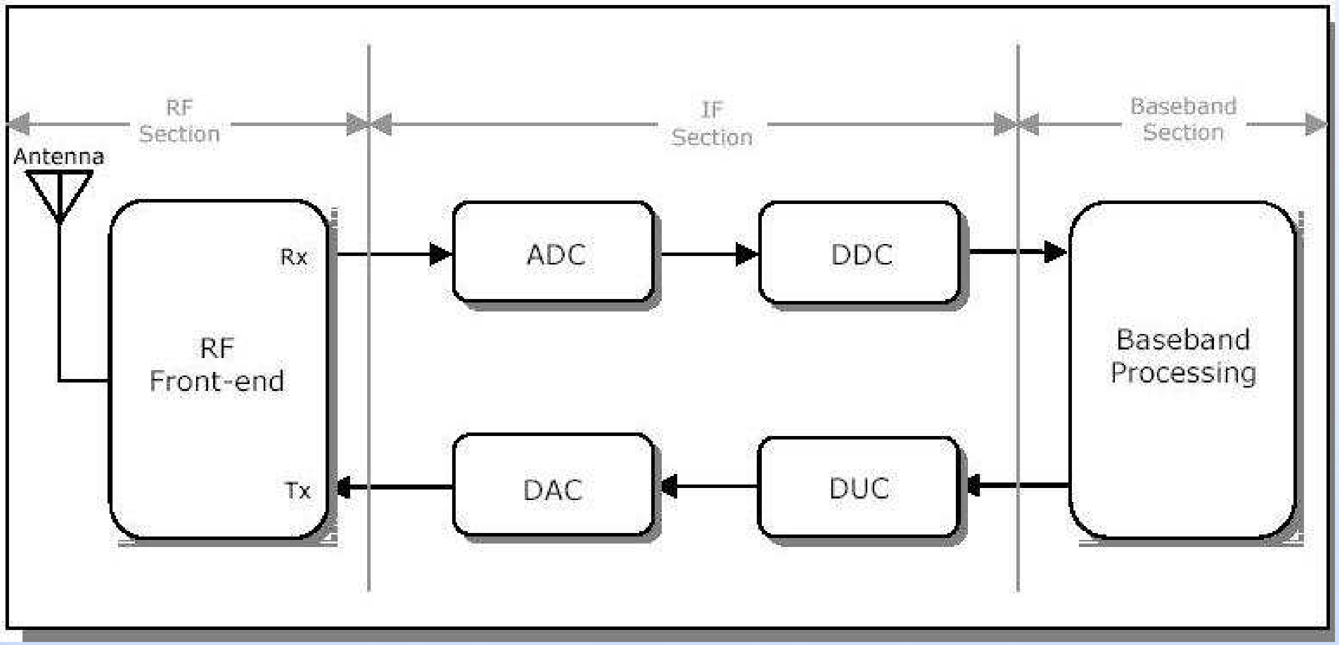
Security Concerns in Mobile Systems

Attack scenarios (third radio)

- Transmit noise at a frequency that might be in use
- Spread noise at available frequencies by jumping
- Listen for transmission and transmit noise at that frequency (may include jumping)
- Replay, modify, inject messages

Security in SDR

- **the functions of software-defined radio (SDR) can be changed by changing its software. Therefore, many security problems that have never been seen in the conventional fixed wireless terminals will arise.**



Security in SDR

Requirements

- **Policy-driven behavior**

  An SDR device SHALL enforce a device-specific SDR security policy that governs the behavior of the device at all times.

- **Policy freshness**

  The SDR device SHALL ensure that its device-specific SDR security policy incorporates the SDR security policies of its stakeholders within the scope of their authority.

- **Device attestation**

  An SDR device SHALL provide trusted configuration information to its communications service providers on request.

- **Protected download**

  An SDR device SHALL provide confidentiality and integrity services for download of SDR-related software and configuration data.

Security in SDR

- **Policy-compliant installation and instantiation**

  An SDR device SHALL only install and instantiate SDR-related software and policy that have been appropriately certified to be compliant with the device's SDR security policy.

- **Run-time control**

  An SDR device SHALL at run-time prevent transmissions that violate its SDR security policy.

- **Resource integrity**

  An SDR device SHALL detect the unauthorized modification of its SDR-related resources and use that information to prevent additional unauthorized behavior.

- **Access control**

  SDR devices SHALL control access to each SDR-related resource on the device.

Security in SDR

- **Audit**

  An SDR device SHALL detect, log and notify specified processes of security related events.

- **Process separation**

  An SDR device SHALL have mechanisms to prevent SDR applications from compromising the security of non-SDR-related applications and data.

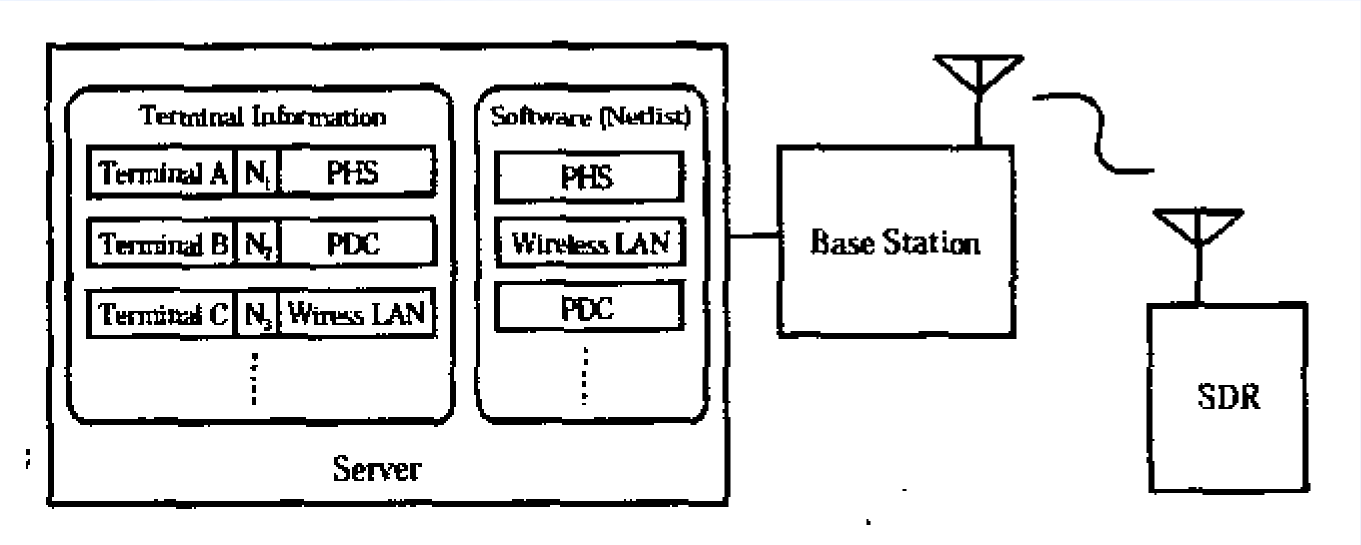
- **Implementation assurance**

  Information assurance mechanisms SHALL be based on industry standards and validated technology.

- **Supportive operations**

  Operational practices supporting information assurance mechanisms SHALL be consistent with and supportive of the SDR security policy.

Secure Software Download in SDR



Download Model in SDR

Secure Software Download in SDR

- **Verification of integrity**

  Must be a method of ensuring that the software downloaded is intact and has not been modified

- **Authentication**

  It has obtained government approval

- **Furthermore**

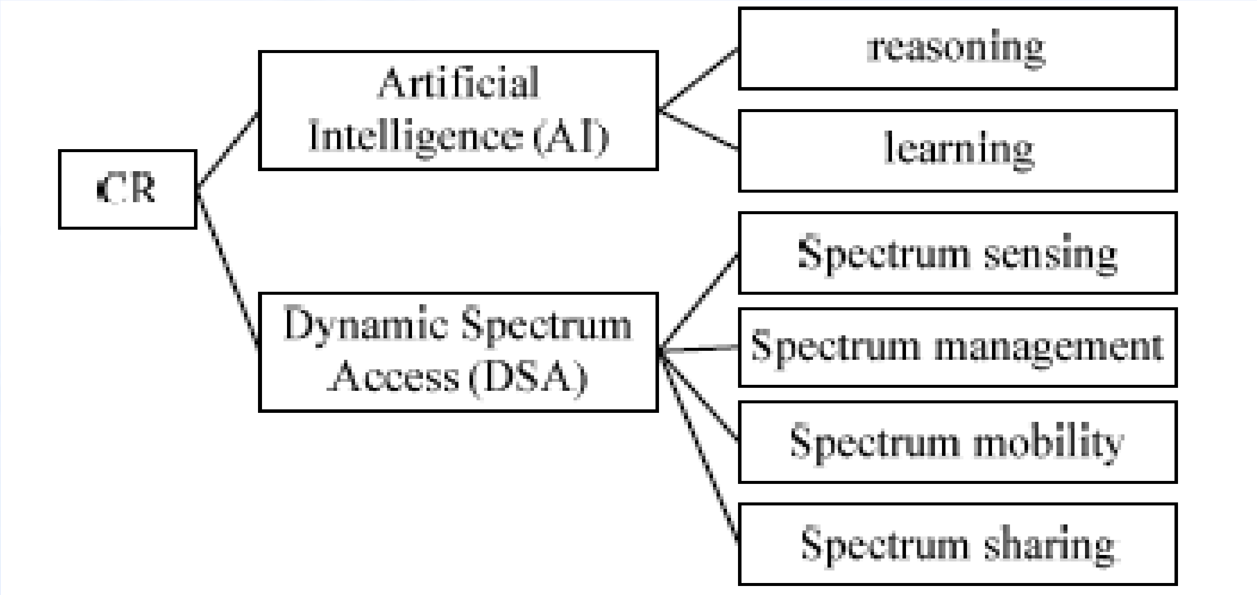
  - In the event that some illegally modified software is created, there should be some mechanism to prevent the spread of that illegal software.
  - For the introduction of a software downloadable SDR system, the software should be protected against theft by people or companies who would like to know the details of the software employed by a rival company

Secure Software Download in SDR

- Secret key encryption
- Public key encryption
- A technique for cryptographic hashing
- A technique for cryptographic signature

Security in Cognitive Radio

- **Characteristics of cognitive radio**



Security in Cognitive Radio

- **Security threats in CR**

- **Artificial intelligence behavior threats**

  - Policy threats
  - Learning threats
  - Parameters threats

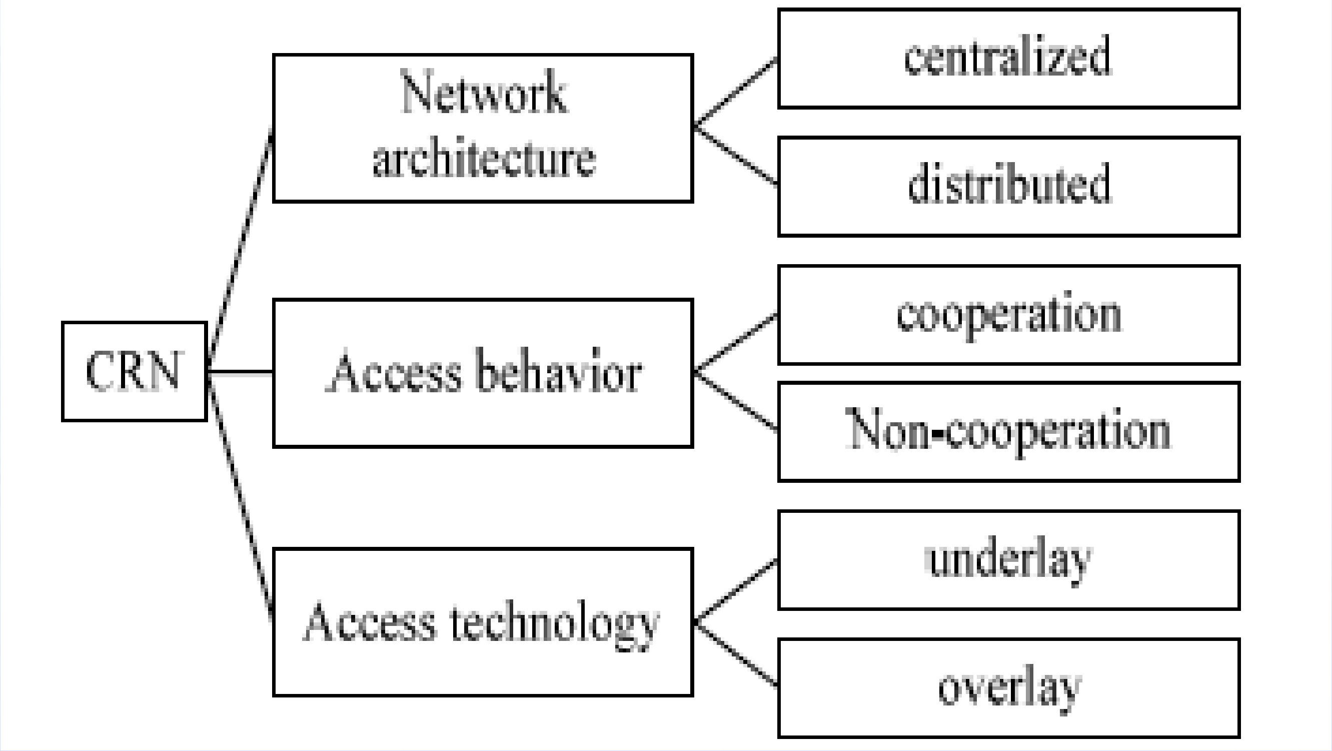
Security in Cognitive Radio

- **Security threats in CR**

- **Dynamic spectrum access threats**
  - Spectrum sensing threats
  - Spectrum management threats
  - Spectrum mobility threats

Security Threats in Cognitive Radio Networks

- **Characteristics of cognitive radio network**



Security Threats in Cognitive Radio Networks

threats to a cognitive radio network

- sensory input statistics can be altered
- faulty sensory input statistics can lead to belief manipulation
- manipulated individual statistics and beliefs may be distributed through a cognitive radio network
- behavior algorithms based on manipulated statistics and beliefs can result in suboptimal performance or maliciousbehavior

Security Threats in Cognitive Radio Networks

To mitigate the effectiveness of previous attacks, cognitive radios should:

- always assume sensory input statistics are “noisy” and subject to manipulation;
- be programmed with some amount of “common sense” to attempt to validate learned beliefs;
- compare and validate learned beliefs with other devices on the network;
- expire learned beliefs to prevent long-term effects of attackers
- attempt to perform learning in known-good environments

FUTURE RESEARCH

- Understanding Identity
- Earning and Using Trust
- Trust in Networking and Routing

Thanks For Your Attention