Cognitive Radio Network Security

Yao Zheng

Outline
- A taxonomy of CR security threats
- Primary user emulation attacks
- Byzantine failures in distributed spectrum sensing
- Security vulnerabilities in IEEE 802.22

Introduction
- Successful deployment of CR networks and the realization of their benefits will depend on the placement of essential security mechanisms
- Emergence of the opportunistic spectrum sharing (OSS) paradigm and cognitive radio technology raises new security implications that have not been studied previously
- Researchers have only recently started to examine the security issues specific to CR devices and networks

COGNITIVE RADIO TECHNOLOGY

Some Recent Publications on CR Security
A Taxonomy of CR Security Threats

- Off-network security threats
- Spectrum access related security threats
- Threats to incumbent coexistence mechanisms
- Threats to self-coexistence mechanisms
- Radio software security threats

The Importance of Distinguishing Primary Users from Secondary Users
- Spectrum usage scenario for a secondary user
  - Periodically search for spectrum “white spaces” (i.e., fallow bands) to transmit/receive data
  - When a primary user is detected in its spectrum band
    - Immediately vacate that band and switch to a vacant one
      → “vertical spectrum sharing”
  - When another secondary user is detected in its spectrum band
    - When there are no better spectrum opportunities, it may choose to share the band with the detected secondary user
      → “horizontal spectrum sharing”
    - CR MAC protocol guarantees fair resource allocation among secondary users

Primary User Emulation Attacks

Existing Technique (1): Using Energy Detection to Conduct Spectrum Sensing
- Trust model
  - An energy detector measures RF energy or the RSS to determine whether a given channel is idle or not
  - Secondary users can recognize each other’s signals and share a common protocol, and therefore are able to identify each other
  - If an unidentified user is detected, it is considered a primary user

Existing Technique (1): Using Energy Detection to Conduct Spectrum Sensing
- Problem: If a malicious secondary user transmits a signal that is not recognized by other secondary users, it will be identified as a primary user by the other secondary users
  - Interference to primary users
  - Prevents other secondary users from accessing that band

Decision statistic Y follows Chi-square distribution
\[ Y \sim \chi^2_{2M} \] if Hypothesis \( H_0 \) holds.
\[ Y \sim \chi^2_{2N}(\gamma) \] if Hypothesis \( H_1 \) holds.
Existing Technique (2): Matched Filter and Cyclostationary Feature Detection

- Trust model
  - Matched filter and cyclostationary feature detectors are able to recognize the distinguishing characteristics of primary user signals
  - Secondary users can identify each other’s signals
- Problem: If a malicious secondary user transmits signals that emulate the characteristics of primary user signals, it will be identified as a primary user by the other secondary users
  - Interference to primary users
  - Prevents other secondary users from accessing that band

Advantages: Better detection performance and less time to achieve processing gain
Disadvantages: Prior knowledge of primary signal is required (such as pilots, preambles or synchronized messages).

Existing Technique (3): Quiet Period for Spectrum Sensing

- Trust model
  - Define a “quiet period” that all secondary users stop transmission. It is dedicated for spectrum sensing.
  - Any user detected in the quiet period (using energy detector, matched filter or cyclostationary feature detector) is a primary user
- Problem: If a malicious secondary user transmits signals in the quiet period, it will be identified as a primary user by the other secondary users
  - Interference to primary users
  - Prevents other secondary users from accessing that band

Transmitter Verification for Spectrum Sensing

- Transmitter verification for spectrum sensing is composed of three processes:
  - Verification of signal characteristics
  - Measurement of received signal energy level
  - Localization of the signal source

A Flowchart of transmitter verification
Challenges in PST Localization

• Primary signal transmitter (PST) localization is more challenging than the standard localization problem due to two reasons
  o No modification should be made to primary users to accommodate the DSA of licensed spectrum. This requirement excludes the possibility of using a localization protocol that involves the interaction between a primary user and the localization device(s).
      • PST localization problem is a non-interactive localization problem
  o When a receiver is localized, one does not need to consider the existence of other receivers. However, the existence of multiple transmitters may add difficulty to transmitter localization

A solution to PST Localization

• Magnitude of an RSS value typically decreases as the distance between the signal transmitter and the receiver increases
• If one is able to collect a sufficient number of RSS measurements from a group of receivers spread throughout a large network, the location with the peak RSS value is likely to be the location of a transmitter.
• Advantage of this technique is twofold,
  o Obviates modification of primary users and
  o Supports localizing multiple transmitters that transmit signals simultaneously

Byzantine failures in distributed spectrum sensing

• Cause of Byzantine failures in distributed spectrum sensing (DSS)
  o Malfunctioning sensing terminals
  o Spectrum sensing data falsification (SSDF) attacks
    • A malicious secondary user intentionally sends falsified local spectrum sensing reports to the data collector in an attempt to cause the data collector to make incorrect spectrum sensing decisions

SSDF Attacks

Modeling of DSS as a parallel fusion network

• We can model the DSS problem as a parallel fusion network

Data fusion algorithms for DSS

• Decision fusion
• Bayesian detection
• Neyman-Pearson test
• Weighted sequential probability ratio test (WSPRT)
The Coexistence Problem in CR Networks

- Incumbent coexistence
  o Avoid serious interference to incumbent users
  o Ex: spectrum sensing for detecting incumbent signals
  o Ex: dynamic frequency hopping to avoid interfering with detected incumbents

- Why is self-coexistence important in CR networks?
  o Minimize self-interference between neighboring networks
  o Need to satisfy QoS of networks’ admitted service workloads in a DSA environment
  o Ex: 802.22 prescribes inter-cell dynamic resource sharing mechanisms for better self-coexistence

- CR coexistence mechanisms can be exploited by adversaries
  o Threats to incumbent coexistence mechanisms
  o Threats to self-coexistence mechanisms

Operating Environment of 802.22 Networks

- Incumbent services: TV broadcast services
- Part 74 devices (wireless microphones)
- TV transmitters

PHY-Layer Support for Coexistence

- Two-stage spectrum sensing in quiet periods (QPs)
  o Fast sensing stage: a quick and simple detection technique, e.g., energy detection.
  o Fine sensing stage: measurements from fast sensing determine the need and duration of fine sensing stage.

- Synchronization of overlapping BS’ QPs

Cognitive MAC (CMAC) Layer (1)

- Two types control messages
  o Management messages: intra-cell management
  o Beacons: inter-cell coordination

- Inter-cell synchronization
  o Frame offset is contained in beacon payload
  o The receiver BS performs frame sliding to synchronize with the transmitter BS.

Cognitive MAC (CMAC) Layer (2)

- Inter-BS dynamic resource sharing
  o Needed when QoS of admitted service workload cannot be satisfied
  o 802.22 prescribes non-exclusive & exclusive spectrum sharing

- On-demand spectrum contention (ODSC) protocol
  o Select a target channel to contend
  o Each BS selects a Channel Contention Number (CCN) from [0,W].
  o BS with a greater CCN wins the pair-wise contention procedure.
  o BS wins the channel if it wins all pair-wise contention procedures with all co-channel BSs.
  o Inter-cell beacons used to carry out ODSC

Cognitive MAC (CMAC) Layer (3)

- Protection of Part 74 devices (wireless microphones)

- Class A solution
  o A separate beacon device deployed
  o Transmit short wireless microphone beacons (WMB)
  o Use WMBs to notify collocated 802.22 cells about operation of Part 74 devices

- Class B solution
  o A special type of CPE is deployed
  o Class B CPEs detect Part 74 device operations and notify other 802.22 systems
Overview of 802.22’s Security Sublayer

• 802.22 security sublayer provides confidentiality, authentication and integrity services for intra-cell management messages
  o PKM (Privacy Key Management) protocol
  o Encapsulation protocol
• It fails to protect inter-cell beacons used in coexistence mechanisms

Potential Security Threats

• DoS attacks
  o Insertion of forged management messages by rogue terminals
  o Prevented by use of mutual authentication and MACs
• Replay attacks
  o Management messages: Prevented by use of nonces in challenge/response protocols
  o Data packets: Thwarted using AES-CCM & packet numbers
• Threats against WMBs
  o Class B CPEs possess pre-programmed keys that enable the use of authentication mechanisms to prevent WMB forgery/modification
  o Spurious transmissions in QPs: Interfere with various coexistence-related control mechanisms
  o Primary user emulation: Adversarial radio transmits signals whose characteristics emulate those of incumbent signals

Security Vulnerabilities in Inter-Cell Coexistence Mechanisms

• Inter-cell beacons are not protected by 802.22’s security sublayer!
• Beacon Falsification (BF) attack
  o Two types of BF attacks
    o Tx of false/forged inter-cell beacons to
      • disrupt spectrum contention processes ➔ Network throughput drop
      • interfere with inter-cell synchronization ➔ Undermine the accuracy of spectrum sensing

Disrupting Inter-cell Spectrum Contention

• Objective of BF attacks
  o Disrupt self-coexistence mechanisms (spectrum contention processes)
• Attack method
  o Forge inter-cell beacons with arbitrarily large CCN value (e.g., select CCN from \([W/z, W]\), where \(z \geq 1\))
  o Tx beacons that contain large CCN to neighboring BSs
• Impact of BF attacks
  o Legitimate victim BSs lose the target channels.
  o Drop in network throughput

Countermeasures

• To thwart the forgery of inter-cell beacons, an inter-cell key management scheme is needed
  o Utilize the backhaul infrastructure that connects multiple cells
  o Employ a distributed key management scheme

Interfering with Inter-cell Synchronization

• Objective of BF attack
  o Undermine efficacy of incumbent coexistence mechanism (spectrum sensing)
• Attack method
  o Forge inter-cell beacons with spurious Frame Offset
• Impact of BF attack
  o Victim BS performs frame sliding according to the spurious Frame Offset, which causes asynchrony of QPs.
  o Asynchrony causes self-interference that degrades accuracy of spectrum sensing during QPs.
  o Impact on misdetection probability (for energy detector)
    o An incumbent signal is detected if \(Y > r\) (estimated Rx signal power, \(Y\), is greater than threshold \(r\)).
    o Under BF attacks, self-interference in QPs causes the threshold to increase to a larger value, \(r^*\).
    o Miss detection probability increases by \(\Pr(Y < r^*) = \int_{r^*}^{\infty} f_Y(x)dx\)
Summary

• Emergence of the opportunistic spectrum sharing (OSS) paradigm and cognitive radio technology raises new security implications that have not been studied previously.
• One countermeasure for primary user emulation attacks is transmitter verification; it is composed of 3 processes:
  o Verification of signal characteristics
  o Measurement of received signal energy level
  o Localization of the signal source
• We can model the distributed spectrum sensing problem as a parallel fusion network to deal with Byzantine failures.
• IEEE 802.22 is vulnerable to attacks because its inter-cell beacons are not protected.