Network Access Security Policies for Cognitive Radio

Mukul Khairatkar

Tulin Mangir

California State University Long Beach

Roadmap

- Introduction
- Types of Attack
- Initial Conditions
- Preventive Methods
  - 802.22 WRAN Topology
  - RF Cognitive Access Chip
  - Frequency Shift
- Comparison of Methods
- Conclusion

Software Defined Radio

- Fixed frequency operation
- Main components
  - Receiver Controlled by DSP
  - LNA and Mixer
  - A/D converter
  - Digitized Data
- Operation:- Filtering , Demodulation etc.
- Predefined Algorithm

Cognitive Radio

- Advanced form of Software Defined Radio (SDR)
- Covers defined spectrum of operation
- Used to overcome frequency spectrum shortage
- Flexible operation
- Transceiver selects RF front end of operation

Types of Attack

- MAC Spoofing
- Beacon based attacks
- Vulnerability attacks
- Flood attacks

MAC Spoofing

- MAC address is stolen and misused
- Station on same network with same privileges
- Cloning of MAC address
- Modification in Network access

Beacon Based Attacks

- Change in Beacon Frame
- Announcement of network existence
- Beacon frames are transmitted regularly for
  - Nodes to find existence of network
  - Paging a node
  - Clock synchronization
- Maintenance of the network

Vulnerability Attacks

- Advantage of wireless network protocol design error
- Related to CCA in DSSS
- Channel Busy message
- RF signal algorithm causing signal scrambling
- Improper modulation type
- Data mismatch

Flood Attacks

- Blocking operating channel
- SSID mask
- Destroying beacon frame
- Disconnecting other users from accessing network
- DoS

Preventive Methods

- Guard Access Point (802.22 WRAN Topology)
- RF Cognitive Access Chip
- Frequency Shift

Guard AP (802.22 WRAN)

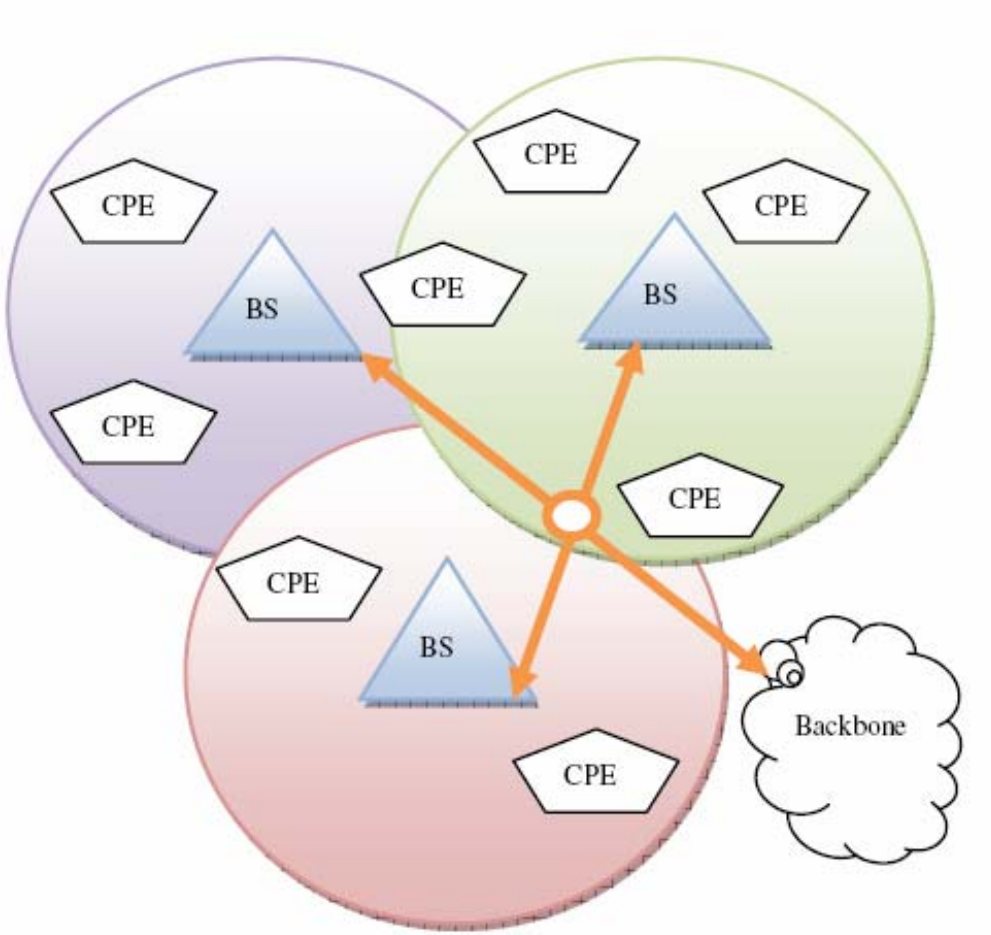

Fig. 1 802.22 WRAN Topology

Guard AP (802.22 WRAN)

- 802.22 Wireless Regional Area Network
- Uses white space in TV broadcasting spectrum
- Opportunistic way to decide channel
- First worldwide CR based standard
- Supports unlicensed operation in bands (54 MHz-862 MHz)

Operation

- Fixed Point-to-multipoint wireless air interface
- Base Station Manages its own cell and associated Customer premises equipment (CPEs)
- Base Station (BS) is a professionally installed entity
- BS controls the downstream to CPEs
- CPEs respond on upstream to BS
- Master/Slave Configuration
- NO CPE is active without authorization from BS
- Distributed Sensing for Incumbent protection

RF Cognitive Access Chip

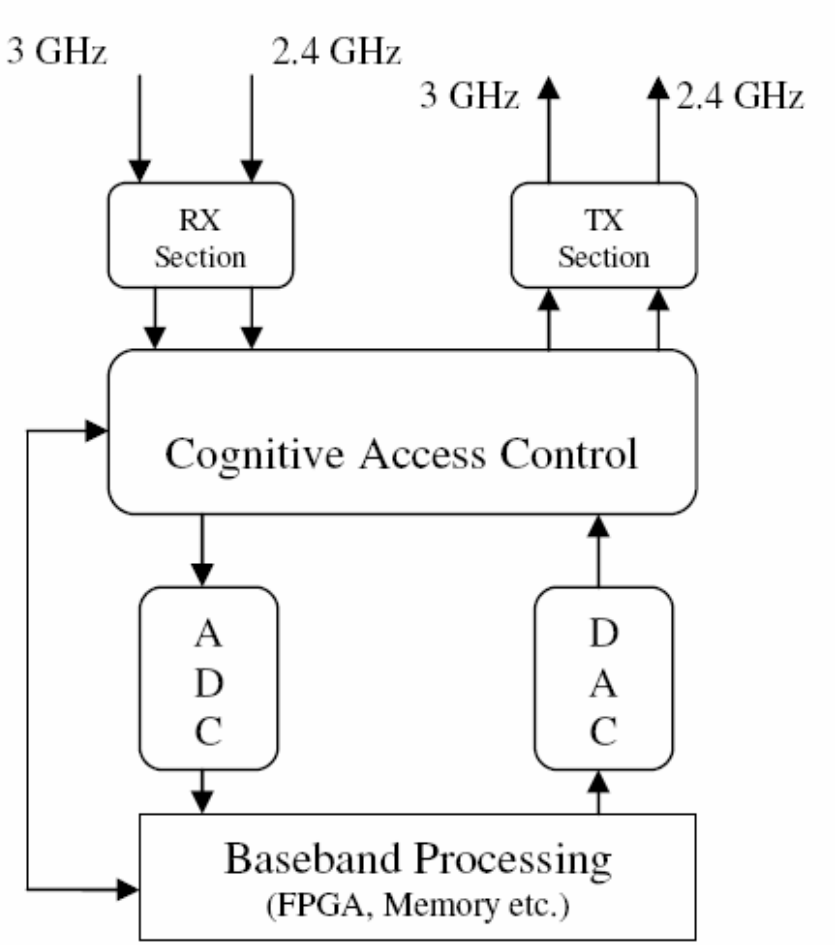

Fig. 2 RF Cognitive Access Method

RF Cognitive Access Chip

- RF access chip is on RF front end
- Can be a part of modulator and demodulator
- Hybrid chip with minimal processing capability
- Interacts with baseband processing unit
- Acts as a gate for dataflow from ADC/DAC
- Major responsibility with spectrum sensing

Operation

- Minimum Dual band radio (licensed and unlicensed)
- Cognitive Access chip senses the medium on licensed band
- If senses primary active then looks for another channel for white space
- Signal and whitespace decision taken by algorithm in RF access chip
- It indicates baseband unit about availability and transmission
- Periodic sensing for primary
- Presence of primary reverts the operation

Frequency Shift (Buck-Boost)

- Change of frequency up or down

- CR Classes for buck or boost frequency shift
- Avoids unwanted spectrum sensing

Operation

- Certain shift for CR when primary is absent
- CR can only look for white space lower than its default center frequency (buck frequency shift)
- CR with higher classes look for white space upper than its default frequency (boost frequency shift)
- Multiple radio support
- Certain CR can do both (boost and Buck) frequency shift
- Limited hardware, size and power requirement

Comparison Parameters

- Implementation
  - Feasibility
  - Power requirement
- Complexity
  - Development
  - Operation
  - Debugging
- Network Structure
  - WAN/WRAN/Mobile/Ad-hoc
- Cost
  - Development
  - Implementation
  - Maintenance

Comparison Table

Methods / Metrics	**Guard AP**	**RF access Chip**	**Frequency Shift**
Implementation	Additional Device	Additional Chip	Additional Rules
Complexity	Complex	Complex	Simple
Power Requirement	More	Less	*NA*
Cost	Costly	Costly	Less costly
MAC Spoofing	Preventive	Preventive	Less Preventive
Beacon based Attacks	Preventive	Preventive	Less Preventive
Vulnerability Attack	Less Preventive	Preventive	Preventive
Flood Attacks	Preventive	Less preventive	Less Preventive

Conclusion

- Wireless Attacks can disrupt CR operation
- Security and operational rules are mandatory
- Spectrum Sensing is important and must be secured
- Three methods for secure spectrum sensing
- 802.22 WRAN method is effective in large power communication
- RF access chip is more efficient and robust
- Frequency shift is effective in CR classification

References

[1] FCC, "Spectrum Policy Task Force Report (ET Docket no. 02-135)," Nov. 2002

[2] Ian F. Akyildiz, Won-Yeol Lee, "A Survey on Spectrum Management in Cognitive Radio Networks, IEEE Communications Magazine, IEEE 2008.

[3] Ruiliang Chen, Jung-Min Park, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks, IEEE Communications Magazine, IEEE 2008.

[4] Amir Ghasemi, "Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-offs", Communications Research Center Canada, University of Toronto, IEEE 2008.

[5] Nicola Baldo and Michele Zorzi, University of Padova Italy, "Fuzzy Logic for Cross-layer Optimization in Cognitive Radio Networks", IEEE Communications Magazine, IEEE 2008.

[6] R. Venkatesha and Przemyslaw, Delft University of Technology, "Cognitive Functionality in Next Generation Wireless Networks: Standardization efforts" IEEE Communications Magazine, IEEE 2008.

[7] Samer Fayssal, Salim Hariri, and Youssif Al-Nashif, electrical and Computer Engineering Department ,The University of Arizona Tucson, "Anomaly-Based Behavior Analysis of Wireless Network Security" Fourth Annual International Conference for Mobile communication, 2007.

[8] BorkoFurht, Auerbach Publications "Encyclopedia of Wireless and Mobile Communications" Volume -1, Page 230- Page 252. , Taylor and Francis Group, 2008.

[9] Carlos Cordeiro, Kiran Challapali, Dagnachew Birru, "IEEE 802.22: The First Worldwide Wireless Standard based on Cognitive Radios", Philips Research USA, IEEE 2007

[10] Asier Mart´ınez_, Urko Zurutuzayz, Roberto Uribeetxeberriay, Miguel Fern´andez, "Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks", Mondragon University, Computer Science Department, IEEE 2008.

Thank You