Copyright Transfer Agreement: The following Copyright Transfer Agreement must be included on the cover sheet for the paper (either email or fax)—not on the paper itself.

"The authors represent that the work is original and they are the author or authors of the work, except for material quoted and referenced as text passages. Authors acknowledge that they are willing to transfer the copyright of the abstract and the completed paper to the SDR Forum for purposes of publication in the SDR Forum Conference Proceedings, on associated CD ROMS, on SDR Forum Web pages, and compilations and derivative works related to this conference, should the paper be accepted for the conference. Authors are permitted to reproduce their work, and to reuse material in whole or in part from their work; for derivative works, however, such authors may not grant third party requests for reprints or republishing."

Government employees whose work is not subject to copyright should so certify. For work performed under a U.S. Government contract, the U.S. Government has royalty-free permission to reproduce the author's work for official U.S. Government purposes.

NETWORK ACCESS SECURITY POLICIES FOR COGNITIVE RADIO

Mukul Khairatkar, Tulin Mangir
(Dept. of Electrical Engineering California State University Long Beach CA 90840)
(mkhairat@csulb.edu, temangir@csulb.edu)

ABSTRACT

In this paper we explore security access methods and techniques for Cognitive Radio (CR) and compare different methods for complexity of implementation, effectiveness and applicability. In Cognitive radio (CR), which changes frequency band of operation with software while technology is being developed and actually fielded in certain tactical applications and operations, security of accessing the spectrum is still undefined. With the cognitive approach any radio spectrum can be accessed with certain hardware and software combination. In order to use the spectrum efficiently, spectrum of use must be well defined for specific radio operation. Here, we first discuss different attacks in wireless communication at the physical layer. These generalized attacks apply to CR communications. The types of attacks are physical layer attacks which can cause network operation to malfunction or to stop completely. We then present three different methods for secured cognitive access over a defined spectrum. We conclude by comparing these methods over different parameters and for different networks.

1. INTRODUCTION

Wireless access has become an integral and vital component of the society with the ubiquitous use of wireless devices in all aspects of our daily lives. This ubiquitous use is filling up the available channels in the specific spectrum making it difficult to accommodate more users. The spectrum used is broadly divided into two sections as licensed and unlicensed spectrum. The defined spectrum for different services was variable when it was started. However, now there is an imbalanced use of this region causing "Spectrum scarcity". A recent survey shows that, the licensed spectrum is less utilized continuously across time and space than unlicensed spectrum [1]. The low utilization of licensed spectrum shows that spectrum scarcity is mainly due to inefficient frequency allocation than any physical shortage of spectrum [2]. This fact has resulted in a new spectrum allocation paradigm called Dynamic Spectrum Allocation (DSA), where devices in unlicensed band can temporarily access unoccupied bands of licensed spectrum while respecting the rights of licensed spectrum users. This permission allows any user to access any licensed band for certain amount of time. With this permission attacker can create forbidden conditions on a licensed band which will turn down operation of entire networks. To avoid such cases, some network access policies must be defined which will restrict certain users from accessing licensed spectrum. In the following sections we first describe type of attacks by unauthorized users, after defining the initial conditions of use, we describe the preventive techniques. We conclude by comparing these techniques and making recommendations for secure access implementation.

2. TYPE OF ATTACKS

The network is accessed mainly for three reasons. One, when a device is in sheer need of communication. Second, when device does not want to communicate but just wants to interfere or disable the network operation - this is called an attack, and third reason can be both where it uses the network, interferes and prevents others from communicating and using the network. Based on above need we can briefly classify these operations into four categories [7].

1) MAC Spoofing
2) Beacon based attacks
3) Vulnerability attacks (DSSS)
4) Flood attacks

MAC spoofing is a type of attack in which MAC address of a particular device is stolen and misused by somebody else to access network. MAC spoofing occurs when a hacker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Beacon based attacks are related to access of network and association with access point. A beacon frame is used for several functions. It is used to synchronize the clock of the nodes and to announce the existence of the network as well as to transmit some necessary configuration parameters to join it. Other important functions of beacon frames are related to the maintenance of the network. Beacon frames are transmitted at regular intervals to allow the nodes find and identify a network. An attacker could spoof beacon frames using false clock values. Those values would produce maladjustment in the contention periods of the stations, causing a Denial of Service [10]. Vulnerability

Proceedings of the SDR '08 Technical Conference and product Exposition, Copyright © 2008 SDR Forum, Inc. All Rights Reserved

attacks take advantage of the wireless network protocol design errors; greedy behavior can fall in this category. The Clear channel assignment (CCA) algorithm used in conjunction with Direct Sequence Spread Spectrum (DSSS) transmission. This is vulnerable to an attack in which a specially crafted RF signal will cause the algorithm to conclude that the channel is busy, so that no device in range of the signal will transmit data. The attacker must be actively transmitting a signal and within range to affect wireless devices. The last wireless attack category is the Denial of Service attacks such as SSID mask, probe request, association, and data flood attacks; attackers can flood the network with useless traffic and slow or even block legitimate users from accessing the wireless network resources.

Other types of attacks include Incumbent Emulation, Spectrum Sensing Data Falsification [2], and false spectrum sensing due to multi-path fading.

3. INITIAL CONDITIONS

The spectrum of use must be well defined for any cognitive radio in order to start communication on the licensed spectrum. We can do pairing of frequency which a CR can access including its normal frequency of operation. The classes can be made in CR operation where the number of bands a CR can switch is defined. This will restrict user from accessing other bands which will prevent unnecessary access of white space and eavesdropping. The CR classes can also be divided in "Buck Frequency Shift" or "Boost Frequency Shift". In buck frequency shift, the device will scan down in spectrum to search for license spectrum from its normal operating frequency. In boost frequency shift, the device will scan in up in spectrum to search for license spectrum from its normal operating frequency.

4. PREVENTIVE METHODS

Following section explains various preventive methods can be used to secure cognitive radio operation.

4.1 Installing guard AP (802.22 WRAN Topology)

IEEE 802.22 is a new working group of IEEE 802 LAN/MAN standards committee which aims at constructing Wireless Regional Area Network (WRAN) utilizing white spaces in the allocated TV frequency spectrum. The spectrum will be used in an opportunistic way in order not to interfere with any signal transmitting TV channel. IEEE 802.22 will be the first worldwide CR based standard to support the unlicensed operation in TV bands (54-862 MHz), which is to coexist with incumbent users and provide wideband internet access to rural and suburban areas [9].

The 802.22 system specifies a fixed point-to-multipoint wireless air interface whereby a base station (BS) manages its own cells and all associated Consumer Premise Equipments (CPEs), as depicted in Figure 1. The BS (a professionally installed entity) controls the medium access in its cell and transmits in the downstream direction to the various CPEs (which can be user-installable), which respond back to the BS in the upstream direction. In order to ensure the protection of incumbent services, the 802.22 system follows a strict masters/slave relationship, wherein the BS performs the role of the master and the CPEs are the slaves. No CPE is allowed to transmit before receiving proper authorization from a BS, which also controls all the RF characteristics (e.g., modulation, coding, and frequencies of operation) used by the CPEs. In addition to the traditional role of a BS, which is to regulate data transmission in a cell, an 802.22 BS manages a unique feature of *distributed sensing*. This is needed to ensure proper incumbent protection and is managed by the BS, which instructs the various CPEs to perform distributed measurement activities.

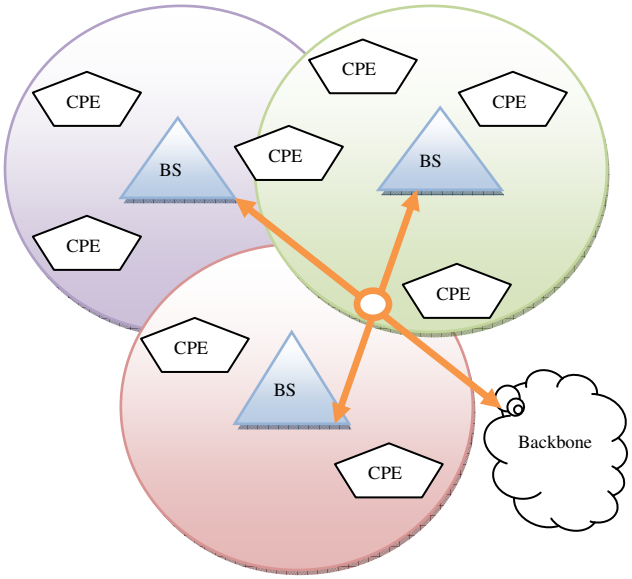

Fig. 1 802.22 WRAN Topology

4.2 RF cognitive Access chip

The use of RF transceiver is a basic need of any wireless device. This RF transceiver is a small chip which contains important blocks for transmitter and receiver which typically include low noise amplifier (LNA), Power Amplifier (PA), Mixer, Low pass filter (LPF) etc. The RF front end is

Proceedings of the SDR '08 Technical Conference and product Exposition, Copyright © 2008 SDR Forum, Inc. All Rights Reserved

actually responsible for spectrum sensing and wireless transmission. The RF cognitive access chip will decide the spectrum of access for any cognitive radio [8].

The configuration of radio transceiver can be made for single, dual, triple, quadruple bands operation and it depends on how many tuning circuits presents inside the transceiver. As the number of tuning blocks increases, cost, power consumption and complexity of transceiver increases.

Figure 2 shows the RF cognitive transceiver with access block present on it. Here we are assuming that the transceiver is a dual band device working on 2.4 GHz as primary and on 3 GHz as secondary band.

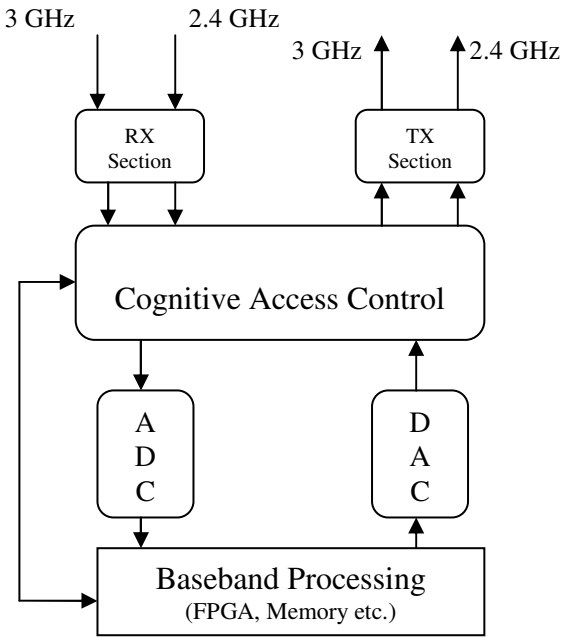

Fig. 2 RF Cognitive Access Method

The normal operation of transceiver is on 2.4 GHz where it works in ISM band for communication. The 3 GHz band is used for radio astronomy and radio navigation. The cognitive access control blocks senses the 3 GHz band on periodic interval and notifies baseband processing block about the availability of the channel. If it senses high power on the particular channel, it simply shifts to sense another white space in neighboring region until it finds sufficiently low power to start cognitive communication. Once the decision is made on channel availability based on bandwidth available, the baseband processing station applies these parameters to an adaptive filter which tunes itself for that particular channel. Now, the baseband processing station requests cognitive access control to shift transmission from 2.4 GHz to 3 GHz band. Transmit and receive operation goes on for least amount of time and cognitive access control senses the medium again for presence of primary transmitter. As soon as it senses presence of primary incumbent it stops the transmission on 3 GHz band and switches back to original 2.4 GHz band notifying baseband processing to restore previous filter settings. The loop goes on till the communication is completed. Here, the processing of baseband signal with different filter design has to be accurate else the loss of actual data is possible. The sensing of 3 GHz band is a crucial stage as it is going to decide whether a new communication band is available or not. The cognitive access control block is more of a Hybrid block which is sensing analog data on a digitally controlled algorithm. For spectrum sensing following three schemes are generally used: Matched filter detection, Energy Detection and feature detection [2]. The combination of three would give the best result but the complexity and processing time of the algorithm may delay the decision.

4.3 CR classification based on type of frequency shift (boost or buck)

This method can be efficiently used in defining classes for cognitive radio. It is certain that CR will shift its operation to a licensed band when it finds primary channel capacity is full. If the CR already knows that it is going to look for frequency range below or above its current operating frequency then we can eliminate excessive white space sensing which will reduce eavesdropping on licensed band. Figure 3 shows an example of a frequency spectrum from 500MHz-960MHz which covers GSM and TV broadcasting channels where as 902MHz to 928MHz (center frequency 915 MHz) is ISM band for region 2.

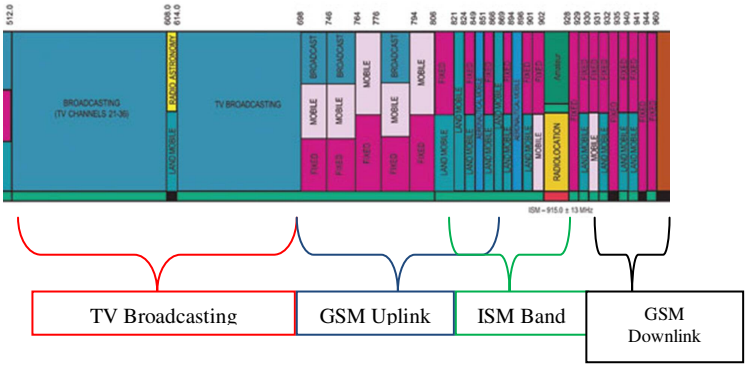

Fig. 3 “Buck Frequency” Spectrum for GSM/ISM band

The buck frequency shift in GSM and ISM band will allow its transceiver to scan frequency range from 512 MHz to 698 MHz which is TV broadcasting band which is lower in value of their current operation. Similarly, GSM band in 1800 MHz and ISM band in 2450 MHz can access higher frequency band for their cognitive communication. This separation will avoid excessive spectrum sensing,

Proceedings of the SDR ’08 Technical Conference and product Exposition, Copyright © 2008 SDR Forum, Inc. All Rights Reserved

eavesdropping. This method defines the region for spectrum sensing and has definite answer. This will have definite RF tuner which will limit the cost of hardware. On the birds view, this method is like extending the bandwidth of operation with certain limit. This method is useful for small radio devices which has limited hardware, power and size requirement.

4.4 Defending against Incumbent emulation

Incumbent Emulation is an attack in which a malicious device emits signal that emulates same properties that of incumbent's signal. This attack is powerful in small signal communication. Energy detection is the simplest method to find out which device is transmitting the signal. With high power TV antenna, the amount of power transmitted is in kilo watts and malicious attacker is comparatively small power device which cannot override power level of incumbent.

4.5 Spectrum Sensing Data Falsification

This attack is tied-up with installation of guard AP in which a wireless devices sends false information to access point about its identity. This data falsification leads AP to give network access to the device and then it overrides the primary operation. This attack can be defended by collecting all local spectrums sensing result and authenticating all the present access point. If a new device tries to join the network, it will not be given access as the guard AP will not found any reference in its database about the node.

5. COMPARISON OF METHODS

The above mentioned methods can be compared on numerous factors which will evaluate its function for different conditions. Following points shows description for comparison metrics. A table of comparison shows prevention of wireless attacks by three different methods.

5.1 Implementation

Guard AP method is simple as it takes installation and configuration of another network device. RF chip can be implemented in transceiver RF front end which will force dual radio operation to follow certain protocol while switching frequency bands. This act will require design of a mini-spectrum analyzer on RF block. The frequency buck-boost operation will limit the band of operation hence user will be blocked on limited white space. This method can be implemented with devices with multiple radios.

5.2 Complexity

The RF chip implementation is the complex procedure over others as it will require special design of hardware and algorithm to carry out required operation.

5.3 Network Structure

Network can be classified on power requirement and frequency of operation. High powered network such as TV broadcasting, Mobile communication tower etc. has additional advantage with power which eliminates attack from a small transmitter. Guard Access point method would work best here as it will monitor activities with high power of operation.

5.4 Cost

The Guard AP method and RF cognitive chip are costly methods as it involves actual device to be installed. On other hand, Frequency shift method has existing hardware tuned to specific frequency which does not involve additional cost.

Following Table shows comparison of three methods at a glance with metrics as Implementation, Complexity, cost etc. and their level of prevention with general wireless attacks.

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

Table 1. Comparison chart showing prevention of wireless attacks by three methods

Proceedings of the SDR '08 Technical Conference and product Exposition, Copyright © 2008 SDR Forum, Inc. All Rights Reserved

6. CONCLUSION

In this paper, we have identified common wireless network attacks at the physical layer which can be a threat for cognitive radio communication. These attacks can disrupt operation in CR network, and moreover may compromise security of the communication. For instance, simple beacon jamming attack may be very effective in interfering with the spectrum sensing process. If this important sensing process fails, then entire network is affected and starts malfunctioning. We have discussed three major security procedures in order to control and regulate the spectrum access. These can be applied to CR networks. We also discussed comparison methods for different networks. The comparison shows that Guard AP method is useful for high power communication where the other two would be suitable for low power operation. Comparison also shows that RF access chip method is more efficient over the other two methods. Combination of RF access chip and any other method provides more efficient and secure network operation, and details of how this can be implemented is being researched as part of our ongoing research.

6. 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.

Proceedings of the SDR '08 Technical Conference and product Exposition, Copyright © 2008 SDR Forum, Inc. All Rights Reserved