11

Security Issues in Cognitive Radio Networks

Chetan N. Mathur and K. P. Subbalakshmi
Stevens Institute of Technology, NJ, USA

1. Introduction

One of the primary requirements of cognitive radio networks is their ability to scan the entire spectral band for the presence/absence of primary users. This process is called spectrum sensing and is performed either locally by a secondary user or collectively by a group of secondary users. The available spectrum bands are then analyzed to determine their suitability for communication. Characteristics like signal-to-noise ratio (SNR), link error rate, delays, interference and holding time can be used to determine the most appropriate band. After the spectrum band is selected, secondary transmission in that band takes place. If a secondary user/network detects a primary user transmission, it vacates the corresponding spectrum band and looks for another vacant band. The process of handing off the licensed spectrum band to a primary user is called *spectrum handoff*. We later show that the delay associated with spectrum handoff causes many of the attacks proposed on cognitive networks.

There are two basic types of cognitive radio networks: centralized and distributed. The centralized network is an infrastructure-based network, where the secondary users are managed by secondary base stations which are in turn connected by a wired backbone. In a decentralized architecture, the secondary users communicate with each other in an ad-hoc manner. Spectrum sensing operation in decentralized architecture is usually performed collaboratively. This type of architecture also encompasses coexistence of two or more wireless networks operating in unlicensed bands. An example of this type of network is the coexistence of IEEE 802.11 with IEEE 802.16 [20].

To analyze the security of cognitive networks, we start by introducing some basic security concepts in the context of cognitive networks. Some of the fundamental building

Cognitive Networks: Towards Self-Aware Networks Qusay H. Mahmoud

blocks of communication security we consider are availability, integrity, identification, authentication, authorization, confidentiality and non- repudiation. We categorize the security issues in cognitive networks into inherent reliability issues and security attacks. Among reliability issues we specifically concentrate on those that are unique to cognitive radio networks like high sensitivity to weak primary signals, unknown primary receiver location, tight synchronization requirement in centralized cognitive networks, lack of common control channel, etc. We then show that each of these vulnerabilities can be utilized by a malicious entity to perform attacks at various layers of communication protocol. Attacks at physical, link, network, transport and application layers are considered.

In the next section, we will provide a brief background on cognitive networks, in Section 3 we will look at building blocks of security, specifically as applied to cognitive networks and in Section 4 we discuss reliability issues inherent in cognitive radio networks. In Section 5 we look at attacks that can occur in each of the layers of the protocol stack as well as cross-layer attacks. In Sections 5.1 and 5.2 we propose novel attacks on the PHY layer and the link layer, respectively. Network layer attacks are discussed in Section 5.3. Most of the network layer attacks are directed against the routing protocol. Transport layer attacks are discussed in Section 5.4. Attacks at this layer basically target the TCP protocol and security mechanisms. In addition to the layer-specific attacks, we also consider cross-layer attacks in Section 5.6. These are attacks performed in one layer to affect another layer. In Section 6, we briefly introduce some recent developments in cognitive network architectures like OCRA [3], Nautilus (http://www.cs.ucsb.edu/htzheng/cognitive/nautilus.html), IEEE 802.22 [10] and DIMSUMnet[6] and discuss their reliability and security issues. The concept behind cognitive networks is to have in-built cognitive (intelligence) capabilities through which the cognitive users detect and prevent intrusions and attacks on the network. In this chapter we show that the cognitive radio networks are still vulnerable to a variety of attacks across various layers of the protocol stack. This is largely because most of the protocols used for cognitive radio networks are borrowed from existing wireless networks. We further suggest that protocols developed for cognitive radio networks need to be improved to make them more intelligent to the surrounding environment, spectrum aware and resilient to intrusions and attacks. In Section 7 we propose some future directions to make cognitive radio networks secure and resilient to many of the proposed attacks. Finally, we conclude the chapter in Section 8.

2. Cognitive Radio Networks

2.1. Cognitive Radio Network Functions

2.1.1. Spectrum Sensing

One of the primary requirements of cognitive networks is their ability to scan the spectral band and identify vacant channels available for opportunistic transmission. As the primary user network is physically separate from the secondary user network, the secondary users do not get any direct feedback from primary users regarding their transmission. The secondary users have to depend on their own individual or cooperative sensing ability to detect primary user transmissions. Since the primary users can be spread across a huge geographical area, sensing the entire spectral band accurately is a challenging task [7] [11]. The secondary users have to rely on weak primary transmission signals to estimate their presence. Most of the research on spectrum-sensing techniques falls into three categories: transmitter detection, cooperative detection and interference-based

detection [2]. The main aim of all these techniques is to avoid interference to primary transmissions. The amount of interference caused by all the secondary users at a point in space is referred to as the interference temperature [39] at that point. When a primary user transmission is taking place, the interference temperature should be below a specified threshold near the primary receivers. However, this is not easy to achieve as the location of the primary receiver is not known to the secondary users. Additionally, when multiple secondary networks overlap, the secondary users scanning the spectrum should not confuse transmissions from secondary users in other secondary networks with primary transmissions.

2.1.2. Spectrum Analysis and Decision

Each spectrum band has some unique features owing to its frequency range and the number of users (both primary and secondary) using the band. Spectrum sensing determines a list of spectrum bands that are available; however, the secondary users decide on the most appropriate band from the list of available bands. In addition to the commonly used SNR parameter, some of the characteristics of spectrum bands that can be used to evaluate their effectiveness are interference, path loss, wireless link errors, link layer delay and holding time (expected duration that the secondary user can occupy the band).

2.1.3. Spectrum Mobility

Spectrum mobility refers to the agility of cognitive radio networks to dynamically switch between spectrum access. As secondary users are not guaranteed continuous spectrum access in any of the licensed bands and the availability of vacant spectrum bands frequently changes over time, spectrum mobility becomes an important factor when designing cognitive protocols. One of the primary factors affecting spectrum mobility is the delay incurred during spectrum handoff. This delay adversely affects protocols employed at various layers of the communication protocol stack. Another important factor to be considered in spectrum mobility is the time difference between the secondary network detecting a primary transmission and the secondary users vacating the spectral band. Transmissions from secondary users during this period will cause harmful interference to the primary users. The FCC [13] has set upper bounds on the spectrum handoff duration to avoid prolonged interference to primary users.

2.2. Cognitive Network Types

2.2.1. Centralized Cognitive Networks

In a centralized architecture, the secondary user network is infrastructure oriented. That is, the network is divided into cells; each cell is managed through a secondary base station. These base stations control the medium access and the secondary users as shown in Figure 11.1. The secondary users are synchronized with their base stations and may perform periodic spectrum-sensing operations. The secondary base stations can be interconnected through a wired backbone network.

2.2.2. Decentralized Cognitive Networks

In a decentralized architecture, the secondary users are not interconnected by an infrastructure-oriented network. Figure 11.2 represents a decentralized network, where

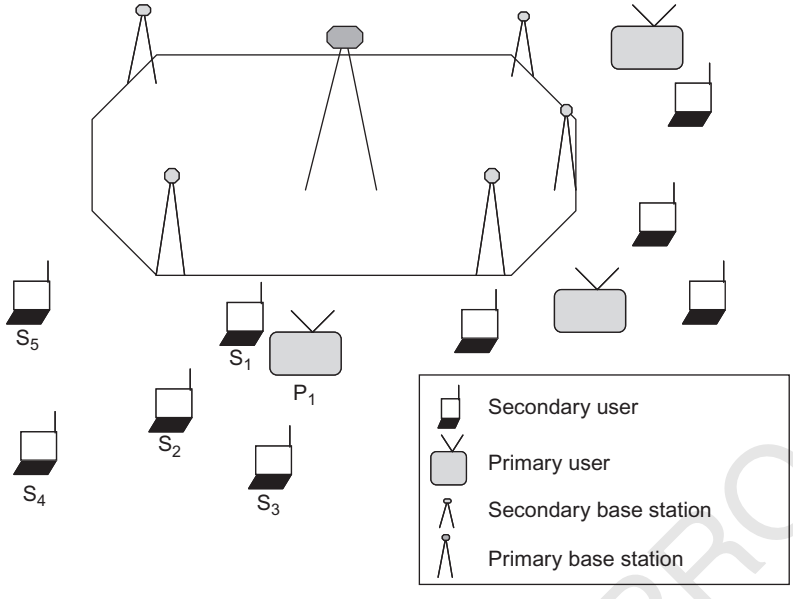

Figure 11.1 Centralized cognitive radio network

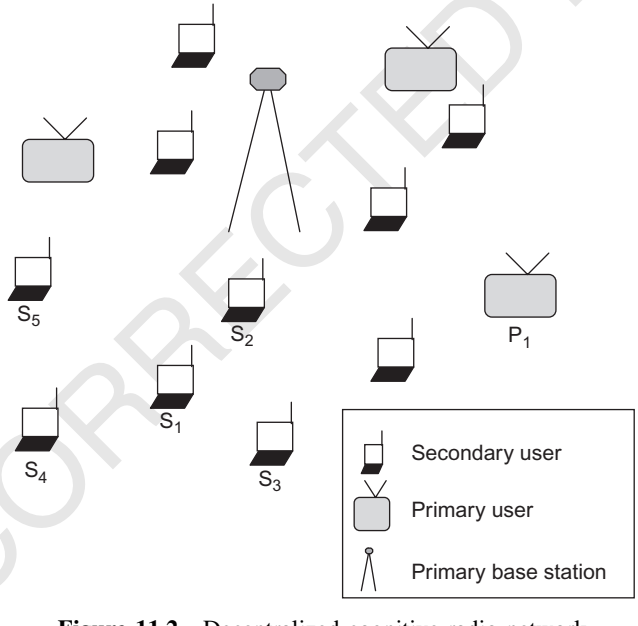

Figure 11.2 Decentralized cognitive radio network

the secondary users communicate with each other in an ad-hoc manner. Two secondary users who are within communication range can exchange information directly, while the secondary users who are not within direct communication range can exchange information over multiple hops.

In distributed cognitive networks, secondary users make decisions on spectrum bands, transmit power, etc. based on either local observations or cooperatively through some utility functions to get near optimum performance for all the secondary users. To illustrate the basics of a collaborative approach, consider the following example (see Figure 11.2), where two secondary users (S_1 and S_2) are operating in a band licensed to a primary base station. S_1 is in the boundary of the transmission range of the primary base station whereas S_2 is closer to the primary base station. Hence S_2 will detect the presence of primary users quickly and easily compared to S_1. Collaborative sensing techniques highlight the fact that if the secondary users share their relative sensing information, then the overall primary user detection for the cognitive network can be improved. However, these protocols do not consider malicious users in the network. Later in this chapter we show that collaborative protocols can be used by malicious users to cause security violations in cognitive networks.

A subclass of decentralized cognitive networks are the spectrum sharing networks, where two wireless networks coexist in an unlicensed band [12]. An example of such a network is the coexistence of IEEE 802.11 and 802.16 [20]. In such networks, a common spectrum coordination channel is established to exchange control information on transmitter and receiver parameters. Primary user identification, spectrum mobility and management functions are not necessary in these class of networks.

3. Building Blocks of Communication Security

In this section, we briefly introduce the basic building blocks of communication security. We describe how these building blocks are applied in existing wireless networks like IEEE 802.11 wireless LAN and discuss their importance in cognitive networks.

3.1. Availability

One of the fundamental requirements for any type of a network is availability. If the network is down and not usable, the purpose of its existence is defeated. Most of the attacks that we hear about these days like the denial of service (DoS) attacks, jamming attacks, buffer overflow attacks on network queues are all targeted towards rendering the network unavailable either temporarily or permanently [14]. An issue that is closely related to network availability is data availability. This is the availability of data (user information, routing tables, etc.) to the users in the network.

In wireless networks, availability usually refers to the availability of the wireless transmission medium. Several techniques are used to ensure that the wireless communication medium is available for transmission. For example, random back-off mechanism [29] is used to prevent collision (jamming) between multiple users at the medium access control (MAC) sublayer of the IEEE 802.11 link layer.

In the context of cognitive networks, availability refers to the ability of primary and secondary users to access the spectrum. For primary (licensed) users, availability refers to being able to transmit in the licensed band without harmful interference from the secondary users. From the definition of dynamic spectrum access policies [13], spectrum availability for the primary users is guaranteed. For the secondary (unlicensed) users, availability refers to the existence of chunks of spectrum, where the secondary user can transmit without causing harmful interference to the primary users. Although studies have shown that large chunks of licensed spectrum are available for opportunistic use [14], availability

of spectrum to the secondary users is not guaranteed. In centralized cognitive networks, availability also refers to the availability of secondary base stations. Security mechanisms should ensure that DoS attacks against secondary base stations are appropriately countered.

3.2. Integrity

Data that is in transit in the network needs to be protected from malicious modification, insertion, deletion or replay. Integrity is an assurance that the data received is exactly as sent by an authorized entity. However, some parts of the data are mutable [41], that is, they need to be legitimately modified as they move from one node to the other. For example, the next hop information, timestamp, hop count are all mutable fields. For this reason, most of the techniques used to ensure integrity perform selective field integrity [41] (provide integrity only for the selected non-mutable fields).

Integrity is extremely important in wireless networks because, unlike their wired counterparts, the wireless medium is easily accessible to intruders. It is for this reason that in wireless LANs an additional layer of security is added at the link layer, to make the wireless links as secure as the wired links. The security protocol used in this layer is called the CCMP [9] (counter-mode encryption with CBC-MAC authentication protocol). The CCMP protocol uses the state-of-the-art advanced encryption standard (AES) [15] in cipher block chaining mode [33] to produce a message integrity check (MIC), which is used to verify the integrity of the message by the recipient. These techniques can also be employed in cognitive radio networks.

3.3. Identification

Identification is one of the basic security requirements for any communication device. It is a method to associate a user/device with their name or identity. For example, in cellular networks, the mobile devices are provided with an equipment identification called international mobile equipment identifier (IMEI). This identifier is used to uniquely identify the mobile devices in the cellular networks. Similarly, a tamper-proof identification mechanism should be built into the secondary user devices in cognitive networks.

3.4. Authentication

Authentication is an assurance that the communicating entity is the one that it claims to be. The primary objective of an authentication scheme is to prevent unauthorized users from gaining access to protected systems. It is a necessary procedure for verifying both an entity's identity and authority. From the service provider's perspective, authentication protects the service provider from unauthorized intrusions into the system. Most of the mechanisms that ensure authentication rely on a centralized certificate authority (CA) that is trusted by all the users in the network. A typical authentication protocol would require the peer entities to get their identities signed (using public key encryption) by the CA and the digitally signed certificates are exchanged and verified by the peers to ensure authenticity. Once the authenticity of peers is established, regular communication is initiated.

In cognitive radio networks, there is an inherent requirement to distinguish between primary and secondary users. Therefore, authentication can be considered as one of the

basic requirements for cognitive networks. In centralized cognitive networks, where the primary and secondary base stations are connected to a wired backbone network, it may be easier to have the CA connected to the wired backbone. However, in distributed cognitive networks with a number of secondary users dispersed over a large geographical area, providing the functionalities of a CA can be quite a challenge [42].

3.5. Authorization

Different entities in the network have varying levels of authorization. For example, the wireless access point has the authorization to remove a possibly malicious user from access to the network. Other users in the network do not have this privilege. The network access control policy describes the level of authorization for each of the entities. In the context of cognitive networks, we have a unique authorization requirement which we call conditional authorization. It is conditional because the secondary users are authorized to transmit in licensed bands only as long as they do not interfere with primary users' communications in that band. As it is difficult to pinpoint exactly which of the secondary users is responsible for harmful interference to the primaries' transmission, this type of authorization is hard to enforce and even more so in a distributed setting. Hence conditional authorization poses a unique challenge in dynamic spectrum access.

3.6. Confidentiality

Confidentiality is closely linked with integrity. While integrity assures that data is not maliciously modified in transit, confidentiality assures that the data is transformed in such a way that it is unintelligible to an unauthorized (possibly malicious) entity. This is achieved by employing ciphers and encrypting the data to be transmitted with a secret key which is shared only with the recipients. The encrypted data is then transmitted and only the recipients with a valid key can decrypt and read the data.

Since the wireless medium is open to intruders, the IEEE 802.11 LAN employs the AES encryption in counter mode in its CCMP protocol [9] to encrypt the data at the link layer as an additional layer of security. The error-prone and noisy nature of wireless medium poses a unique challenge to both data confidentiality and integrity mechanisms. This is because almost all confidentiality and integrity techniques rely on ciphers which are sensitive to channel errors and erasures. This sensitivity property under noisy conditions triggers excessive retransmissions consuming a lot of network bandwidth [28], [31]. This issue is even more pronounced in cognitive networks, where the secondary user access to the network is opportunistic and spectrum availability is not guaranteed.

3.7. Non-repudiation

Non repudiation techniques [34] prevent either the sender or receiver from denying a transmitted message. Therefore, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can in fact prove that the data received was by the alleged receiver. In cognitive radio network setting, if malicious secondary users violating the protocol are identified, non-repudiation techniques can be used to prove the misbehavior and disassociate/ban the malicious users from the secondary network.

4. Inherent Reliability Issues

In this section we point out some of the inherent reliability issues in cognitive radio networks.

4.1. High Sensitivity to Primary User Signals

To prevent interference to licensed primary users, secondary users should detect the primary transmissions in the first place. To ensure high probability (e.g. 99%) of non-interference to the primary users, stringent sensitivity requirements are placed on the detectors at the unlicensed secondary devices. There are two prominent ways to detect the primary user's transmissions: (a) energy-based and (b) waveform-based sensing. Energy-based sensing does not require any knowledge of the primary user's transmission signal, it is based on the simple fact that any information-baring signal has finite signal strength (power). However, energy-based sensing techniques are prone to false detections and usually take a longer time when the signal is low power. Waveform-based sensing is applied when information about the waveform and signal patterns of the primary users transmission signal is known. This makes the waveform-based sensing techniques perform better than energy-based sensing in terms of speed and reliability. However, in many instances, primary user transmission signal patterns may not be known to the secondary users. Moreover, the FCC mandates [13], as one of the requirements for cognitive networks, to predict the temperature interference (measured by energy) on nearby primary user's receivers and keep it below a threshold. To ensure compliance with this requirement the sensitivity towards primary user signals in cognitive networks is usually set to be high. This high sensitivity magnifies false detections due to energy-based sensing resulting in inefficient use of spectrum.

4.2. Unknown Primary Receiver Location

One issue that has received very little attention so far is the lack of knowledge of the primary receivers' location. In order to minimize the interference to the primary user network, the secondary transmitters need to know the locations of the primary receivers. Most of the interference models that have been studied in the literature [16], propose to minimize interference temperature, but the primary receivers' location is unknown. This may lead to hidden terminal [35] problems in cognitive networks. Some recent works (like [38]) have studied this issue and proposed techniques that can be used to detect primary receivers by detecting the receiver power leakage. However, significant work remains to be done to protect the primary receivers from accidental interference caused by secondary users.

4.3. Synchronization Requirement

The secondary users in centralized cognitive radio networks perform fast sensing operations between periods of transmissions (e.g., IEEE 802.22 [10]). These measurements are relayed to the base station which aggregates and determines the presence of primary user transmissions. Therefore, synchronization of secondary users in time is an important requirement to detect the presence of primary users. Even if one secondary user is out of sync with the rest of the secondary users, all other secondary users would in turn detect the energy from the out of sync secondary user and transmit that information to

the base station. The base station would then assume that a primary user transmission is going on and may shut down all the secondary user transmissions in that frequency band. This would result in what is known as a missed opportunity [36]; the band is available yet unused by the secondary users. However, synchronization between secondary users is harder to achieve in some spectrum bands like the TV bands that span over a large geographical area.

4.4. Lack of Common Control Channel

Unlike other infrastructure oriented wireless networks, cognitive networks lack a predetermined control channel. Therefore, as soon as a secondary user boots up, it needs to search for control signals across the entire spectral band. Additionally, this operation needs to be performed during connection reestablishment and whenever mobile secondary users move out of the coverage area of an existing base station to the coverage area of another base station.

4.5. Protocols and Utilities Based on Homo Egualis Model

The utility functions in many coordinated spectrum access protocols are usually based on *Homo egualis* [17] like model. This model is based on an *Homo egualis* society where individuals have an inequality aversion. Such models assume no centralized structure of governance, so the enforcement of norms depends on the voluntary participation of peers. However, in reality this situation rarely exists. Malicious entities tend to violate the *Homo egualis* model for selfish purposes like gaining more bandwidth and resources or to intentionally block others from getting specific resources. More robust models that account for malicious behavior must be employed (more in Section 7) to design coordinated access protocols in cognitive networks.

5. Attacks on Cognitive Networks

We define an attack on cognitive networks as any activity that results in (a) unacceptable interference to the licensed primary users or (b) missed opportunities for secondary users. An attack is considered strong if it involves a minimal number of adversaries performing minimal operations but causing maximum damage/loss to the primary and or secondary users in the network. In this section we describe attacks on various layers of cognitive networks. Most of the attacks we describe make use of one or more reliability issues we pointed out in the previous section. We consider five layers in the protocol stack, namely, the physical layer, link layer, network layer, transport layer and application layer. In addition to the attacks that are specific to a given layer, we also discuss some cross-layer attacks that can be applied at one layer to affect at another layer.

5.1. Physical Layer Attacks

The physical layer is the most basic layer in the protocol stack. It provides the means of transmitting raw signals over the transmission medium. The physical layer determines the bit rate, channel capacity, bandwidth and maximum throughput of the connection. In cognitive networks, the physical layer has the capability to transmit at various frequencies across most of the spectrum band. This makes the physical layer in cognitive networks more complex compared to conventional wireless networks [8]. Therefore, when transmission from one frequency band is switched to another frequency band, the switching process

incurs considerable delay in the physical layer of cognitive networks. In this section, we propose some attacks on cognitive networks that specifically target the physical layer.

5.1.1. Intentional Jamming Attack

This is one of the most basic types of attack that can be performed by secondary users in cognitive radio networks. The malicious secondary user jams primary and other secondary users by intentionally and continuously transmitting in a licensed band. The attack can be further amplified by using high transmit power, transmitted in several spectral bands. Although simple energy-based detection and triangulation techniques can be used to detect this attack, the time it takes to pinpoint and ban the malicious user impacts severely on the network performance. The attack can be made more dangerous by a mobile malicious secondary user performing the attack in one geographical area and moving to another area before being caught.

5.1.2. Primary Receiver Jamming Attack

The lack of knowledge about the location of primary receivers can be used by a malicious entity to intentionally cause harmful interference to a victim primary receiver. The attack is caused when a malicious entity closer to the victim primary receiver participates in a collaborative protocol and requests transmissions from other secondary users to be directed towards the malicious user. Although the interference temperature is kept below a specified threshold at some other point in space, this would still cause continued interference to the primary receiver eventually blocking it out from listening to primary transmissions. Moreover, the naive secondary users causing the interference are oblivious about it.

5.1.3. Sensitivity Amplifying Attack

In order to prevent interference to the primary network, some primary user detection techniques have higher sensitivity towards primary transmissions (see Section 4). This leads to frequent false detections and missed opportunities for the secondary users. A malicious entity can amplify the sensitivity and hence the number of missed opportunities by replaying the primary transmissions. What makes this attack more lethal is that even an adversary with low transmit power can transmit in spectrum band boundaries and still cause multiple secondary users operating in multiple spectrum bands to incur missed opportunities and render spectrum usage inefficient.

5.1.4. Overlapping Secondary User Attack

In both centralized and distributed cognitive networks, multiple secondary networks may coexist over the same geographical region. In such cases, transmissions from malicious entities in one network can cause harm to the primary and secondary users of the other network. This type of attack is hard to prevent because the malicious entities may not be under the direct control of the secondary base station/users of the victim network.

5.2. Link Layer Attacks

This is the second layer in the network protocol stack. The main purpose of the link layer is to transfer data from one node to the next node in one hop. The link layer provides

the functional means to allow fragmentation of data, error correction and modulation. The medium access control (MAC) layer is one of the important sublayers of the link layer, which controls channel assignment. Fairness is one of the primary requirements for channel assignment protocols. In traditional wireless environments, SNR is considered as one of the main parameters to judge the fairness of a channel allocation scheme. However, in cognitive network environments other parameters such as holding time, interference, path loss, wireless link error rate and delay are just as important as the SNR. For this reason, channel assignment is a more complex operation in cognitive networks. In this section, we propose three novel attacks that can be performed at the link layer in cognitive networks.

5.2.1. Biased Utility Attack

A malicious secondary user may selfishly tweak parameters of the utility function to increase its bandwidth. If the secondary users and/or base stations are unable to detect such anomalous behavior, this may result in deprivation of transmission medium for other secondary users. For example, in [39] the authors propose a utility function that is used by the secondary users to determine their bandwidth (in terms of transmission power) with the constraint that the interference temperature due to the secondary transmissions on the primary receivers is below a given threshold. The problem is formulated as a public good game and Nash equilibrium solutions for a global optimum determines the transmit powers of the secondary users. If a malicious user tweaks its utility function to transmit at higher power, it will result in other users getting less bandwidth. Some secondary users may not even get to transmit.

5.2.2. Asynchronous Sensing Attack

Instead of synchronizing the sensing activity with other secondary users in the network, a malicious secondary user may transmit asynchronously when other secondary users are performing sensing operations. If the base station or other secondary users consider this as a transmission from a primary user, then this could result in missed opportunities. This attack can be made more efficient by transmitting only during sensing periods [23].

5.2.3. False Feedback Attack

For protocols that rely on secondary users exchanging information, false feedback from one or a group of malicious users could make other secondary users take inappropriate actions and violate the goals of the protocol. For example, consider a scenario represented in Figure 11.2. In this decentralized cognitive network, five secondary users, $S_1, \ldots, S_5$, are associated with a secondary base station. Secondary user S_2 is closer to the primary base station. Suppose S_2 was a malicious user. When the primary base station starts using its licensed spectrum band, S_2 senses it but does not reveal that information to other secondary users. Secondary user S_1 on the other hand is just outside the boundary region of the primary base station's transmission range and hence does not sense the presence of the primary user. Similarly, secondary users S_3, S_4 and S_5 also fail to sense the presence of the primary user. Now any transmission from S_1, S_3, S_4 and S_5 may cause harmful interference to the primary receivers within the primary base station's transmission range. A similar attack is possible in centralized cognitive radio network.

5.3. Network Layer Attacks

While the data link layer is responsible for node to node (one-hop) packet delivery, the network layer is responsible for end-to-end (source-to-destination) packet delivery. The network layer provides functional means for performing routing, flow control and ensuring quality of service (QoS). Routing refers to selecting paths along the network through which data is transmitted from source to destination. Every node in the network is responsible for maintaining routing information (usually in the form of a table) about its neighboring nodes. When a connection needs to be established, every node determines which of its neighbors should be the next link in the path towards the destination. Some of the routing protocols used in wireless environment are for example dynamic source routing (DSR) and ad-hoc on demand distance vector (AODV) routing [32]. A malicious node in the path can disrupt routing by either broadcasting incorrect routing information to its neighbors or by redirecting the packets in the wrong direction. Several routing attacks have been discovered in wireless ad-hoc networks, most of the attacks can be classified into two categories: routing disruption attacks and resource consumption attacks. Some of the examples of routing attacks are the black hole attack [19] where the malicious node attracts packets from every other node and drops all the packets, the gray hole attack [1] where the malicious node selectively drops the packets, the worm hole attack where the malicious user uses two pairs of nodes with a private connection between the two pairs. The worm hole attack is a dangerous attack since it can prevent route discovery where the source and the destination are more than two hops away. Most of these attacks are prevented by using secure on-demand routing protocols like Ariadne [18] or secure AODV [4], which use cryptographic mechanisms to guarantee integrity of routing information and authenticity of nodes. Although most of the network layer security issues in wireless LANs and wireless ad-hoc networks have been well studied, a similar analysis of network layer security issues in cognitive networks is yet to be performed. In this section we point out some of the unique network layer attacks applied on cognitive networks.

5.3.1. Network Endo-Parasite Attack (NEPA)

NEPA [30] assumes at least one compromised or malicious node in the network. The malicious node attempts to increase the interference at heavily loaded high priority channels. Most of the time, the affected links are along the routing path through the malicious nodes towards the wired gateway; hence the attack takes the name of a parasite attack. Under normal channel assignment operation, a node assigns the least loaded channels to its interfaces and transmits the latest information to its domain neighbors. A compromised node launches NEPA by assigning its interfaces the high priority channels. However, it does not inform its neighbors about this change. Since the transmitted information is not verified by neighbors, the network remains unaware of change. It results in hidden usage of heavily loaded channels; hence the attack takes the name endo-parasite, which refers to internal/hidden parasites. The links using these channels experience interference, decrease in available bandwidth and continuous degraded performance.

5.3.2. Channel Ecto-Parasite Attack (CEPA)

CEPA [30] is a special case of NEPA with slight modification in the attack strategy. A compromised node launches CEPA by switching all its interfaces to the channel that is

being used by the highest priority link. However, the severe nature of this attack makes the detection easy.

5.3.3. Low cOst Ripple effect Attack (LORA)

In LORA [30], misleading information about spectrum assignments is transmitted to all the neighbors to push the network into a quasi-stable state. Since the channel assignment of the compromised node is not actually changed, this attack is significantly different from NEPA and CEPA and it is a low-cost (stronger) attack. The attack is relatively more severe then NEPA and CEPA because the effect is propagated to a large portion of the network beyond the neighbors of the compromised node, disrupting the traffic forwarding capability of various nodes for considerable time duration. The attack is launched when the compromised node transmits misleading channel assignment information, forcing the other nodes to adjust their channel assignments. This may generate a series of changes even in the channel assignment of non-neighboring nodes. Note that normally loaded channels are selected instead of heavily loaded ones and an illusion of heavy load on these channels is created, which results in propagation of change upwards in the routing tree. Heavily loaded channels are not selected because such selection will affect the links closer to gateways resulting in quick adjustment to the change and hence no ripple effect will be created.

5.4. Transport Layer Attacks

The transport layer provides functional requirements to transfer data between two end hosts. It is primarily responsible for flow control, end-to-end error recovery and congestion control. There are two main protocols that operate in the transport layer, the User Datagram Protocol (UDP) and the Transport Control Protocol (TCP). UDP is connectionless while TCP is connection oriented and guarantees ordered packet delivery. TCP performance is usually measured by a parameter called round trip time (RTT). Errors in the wireless environment cause packet loss which in turn triggers retransmissions. Moreover, frequent spectrum band changes by secondary users due to spectrum handoff at the link layer increases RTT. This phenomenon is utilized in our proposed variant (see Section 5.6, of jellyfish attack [1]) to degrade the performance of TCP. Further, different secondary nodes operate in different frequency bands and these bands constantly change. Hence the RTT for a TCP connection in cognitive networks has a high variance.

5.4.1. Key Depletion Attack

Unusually high round trip times and frequently occurring retransmissions imply that transport layer sessions in cognitive networks last only for a short duration. This results in large number of sessions being initiated for any given application. Most of the transport layer security protocols like SSL and TLS establish cryptographic keys at the beginning of every transport layer session. A higher number of sessions in cognitive networks and hence the number of key establishments will increase the probability of using the same key twice. Key repetitions can be exploited to break the underlying cipher system [37]. For example, the WEP and TKIP protocols used in IEEE 802.11 link layer are vulnerable to key repetition attacks. The newer and stronger CCMP protocol [9] is designed to exponentially delay key repetitions. However, most of the security protocols used below the

network layer are designed taking into consideration the total number of sessions typically occurring in wireless LANs. These protocols need to be reinvestigated in the context of the number of sessions that occur in cognitive networks.

5.5. Application Layer Attacks

The application layer is the final layer of the communication protocol stack. It provides applications for users of the communication devices. Some of the basic application layer services include file transfer protocol (FTP), Telnet, email and lately multimedia streaming [27]. Protocols that run at the application layer rest on the services provided by the layers below it. Therefore, any attack on physical, link, network or transport layers impact adversely on the application layer. One of the most important parameters in the application layer is the quality of service (QoS). This is especially important for multimedia streaming applications. Physical and link layer delays due to spectrum handoffs, unnecessary rerouting and stale routing due to network layer attacks and delays due to frequent key exchanges cause degradation of the QoS in the application layer protocols.

5.6. Cross-layer Attacks

By cross-layer attacks we mean malicious operations performed at one layer to cause security violations at another layer. In cognitive networks, there is an inherent need for greater interaction between the different layers of the protocol stack. It is for this reason that cross-layer attacks need to be given special attention in cognitive networks. In this section, we discuss the well-known jellyfish attack [1] performed in the network layer to attack the transport layer, and also present a novel routing information jamming attack which is performed in the link layer to attack the network layer.

5.6.1. Jellyfish Attack

This attack is performed at the network layer but it affects the performance of the transport layer, specifically the TCP protocol. The goal of this attack is to reduce the throughput of the TCP protocol. There are three variants [1] of this attack: misordering, dropping and delay variance. In the misordering attack, the packets are intentionally and periodically reordered as they pass through the malicious node. This attack takes advantage of TCP's vulnerability to misordered packets [5], which triggers retransmissions and degrades throughput. The second variant is the packet dropping attack, where the malicious node periodically drops a fraction of packets that pass through it. This is similar to gray hole attack (see Section 5.3), however, the packets are dropped intelligently by the adversary to coincide with the TCP transmission window. When carefully executed it can cause near zero throughput in the TCP protocol. The third variant of the attack is called delay variance attack, here the packets are randomly delayed as they pass through a malicious node. This causes the TCP timers to be invalid which results in congestion inferences. Although these attacks are primarily proposed for ad-hoc wireless networks, they can be applied to decentralized cognitive networks as well. We propose a fourth variant of the jellyfish attack, where the attacker performs operations in the link layer to attack the transport layer. To perform this attack, the attacker causes the victim cognitive node to switch from one frequency band to another frequency band (using any of the link layer attacks), this causes considerable delay in the network and transport layers. When

performed actively observing the TCP traffic timing, the delay caused due to spectrum handoffs can push RTT to round trip timeout (RTO). RTOs result in retransmissions and hence drastic degradation of TCP throughput. Note that all of the attacks above are hard to detect at the network layer but cause DoS attack at the transport layer.

5.6.2. Routing Information Jamming Attack

This is a novel cross-layer attack that makes use of the lack of a common control channel in cognitive networks and the spectrum handoff delay to jam the exchange of routing information among neighboring nodes. This results in the network using stale routes and incorrect routing of packets from source to destination. The attack is initiated when a malicious node causes spectrum handoff in the victim node just before routing information is exchanged. When this happens, the victim node stops all ongoing communication, vacates the spectral band, opportunistically selects a new spectrum for transmission, scans the entire spectrum band to identify the neighboring nodes and informs the neighboring nodes of the new frequency. Only after these operations are performed can the victim node receive/transmit the updated routing information from/to its neighbors. Until this period any path that goes through the victim node and its neighbors uses stale routing information. This attack can be extended by performing spectrum handoff attacks on the victim node successively just before routing information exchange. The attack can be made more severe if it is performed along the min-cut between the source and destination nodes.

6. Cognitive Network Architectures

In this section, we briefly introduce some recent developments in cognitive network architectures and discuss the attacks presented in Section 5 in the context of these architectures.

6.1. Nautilus

Nautilus (http://www.cs.ucsb.edu/htzheng/cognitive/nautilus.html) is a distributed, scalable and efficient coordination framework for open spectrum ad-hoc networks. The Nautilus framework addresses the lack of a common control channel faced in distributed cognitive network architectures. Some collaborative spectrum access schemes that do not rely on a centralized entity or a common control channel are proposed. One of the proposed collaborative schemes is based on graph coloring, where a topology-optimized allocation algorithm is used for a fixed topology. For mobile cognitive networks, a distributed spectrum allocation based on local bargaining is proposed, where mobile users negotiate spectrum assignment within local self-organized groups. For resource-constrained cognitive devices, a rule-based spectrum management is proposed, where unlicensed users access spectrum according to some predetermined rules and local spectrum observations. Although these novel techniques make spectrum access in cognitive networks more robust and independent of a centralized authority, other security attacks like spectrum handoff attacks, routing attacks, jellyfish attacks pose significant threat to the Nautilus architecture.

6.2. Dimsumnet

DIMSUMnet architecture [6] relies on a spectrum broker who permanently owns and manages the licensed bands (referred to as coordinated access bands (CABs)). The secondary

base stations register with radio access network managers (RANMANs). The RANMANs negotiate with spectrum brokers to lease the appropriate portion of the spectrum requested by the secondary base stations. The spectrum broker, who maintains a database of currently available frequency bands, responds to RANMANs with allotted spectrum frequencies and timeslots. After spectrum bands are assigned to the secondary base stations, the secondary users connected to those base stations are informed to switch to the corresponding frequency bands. Since DIMSUMnet is a truly centralized architecture, with spectrum sensing performed by a centralized entity, security mechanisms are easier to implement and adhere to. The sensing attacks [23] that are possible in IEEE 802.22 are harder to implement in DIMSUMnet. However, as the spectrum monitoring function is performed by just one entity the information about spectrum availability may not be as accurate as in the case of distributed sensing performed by IEEE 802.22. Inaccurate spectrum information can be a primary reliability issue in the case of DIMSUMnet.

6.3. IEEE 802.22

IEEE 802.22 is a standard for wireless regional area networks (WRAN) [10] that utilize ultra high frequency (UHF) and very high frequency (VHF) television bands between 54 and 862 MHz. The standard mandates a centralized cognitive network architecture, where the secondary IEEE 802.22 base stations manage a unique feature of distributed sensing. To perform distributed sensing, the base station instructs the secondary cognitive user devices (referred to as consumer premise equipments (CPEs) in the standard) to synchronously sense various spectral bands for the presence of primary user activity. These sensing results are periodically collected by the base station, which then performs aggregation on the results to determine the presence/absence of primary users in each of the licensed spectrum bands. Hence, the IEEE 802.22 relies on synchronous sensing. This requirement can be a source of vulnerability as pointed out in [23]. Here, the malicious entity transmits during the sensing period causing all other secondary users to report primary user activity to the base station. This results in inefficient use of spectrum resources. In [23] we provide a digital signature-based solution, which helps the base stations identify the original primary signals from those that are sent by malicious entities.

6.4. OCRA (OFDM-based Cognitive Radio Architecture)

The OCRA network [3] is based on orthogonal frequency division multiplexing (OFDM) technology. Here both centralized and distributed cognitive network architectures are considered. To perform spectrum sensing and handoff decisions, OCRA employs a novel OFDM-based spectrum management technique which is based on a physical layer that enables dual mode spectrum sharing [3]. This type of spectrum sharing enables access to existing networks as well as coordination between cognitive users. OCRA proposes to use a novel cross-layer routing technique that jointly considers rerouting and spectrum handoff. To increase the reliability and QOS, multiple transport layer connections over non-contiguous spectrum bands are established.

7. Future Directions

In this section we provide some future directions that need to be taken to make secure cognitive radio networks against both accidental and intentional attacks. Most of our

proposed solutions are easy to implement (for example, using existing security protocols). However, we also propose solutions (for example, developing analog crypto primitives) that require more work.

7.1. Using Existing Security Protocols

Security services provided in cellular, WLAN and wireless ad-hoc networks can be applied to cognitive networks as well. In a centralized wireless network architecture, the backbone network is usually a wired medium. Hence, strong security mechanisms exist that protect this network. It is the last hop between the wireless base stations and the wireless terminals that needs to be protected over the air. As cellular networks are centralized, security solutions in existing cellular networks (3G in particular) could be used as a model to provide security in cognitive networks. In cellular networks, user identity is obtained by using a temporary identity called international mobile user identity. Authentication is achieved by a challenge/response mechanism using a secret key. A challenge/response mechanism is where one entity in the network proves to another entity that it knows a particular secret without revealing it. The UMTS authentication and key agreement (UMTS AKA) is used to achieve authentication. Confidentiality is provided by using the confidentiality algorithm known as f8 and the secret cipher key (CK) that is exchanged as a part of the AKA process. Integrity is provided by using the integrity algorithm, f9 and the integrity key (IK). A block cipher known as KASUMI [21] is the building block of both f8 and f9 algorithms. KASUMI operates on 64 bit blocks and uses a 128-bit secret key. A similar setup could be used in centralized cognitive networks to establish the basic security requirements between the secondary users and the secondary base station.

In decentralized networks, secondary users communicate with each other over one or more hops. Due to the lack of infrastructure, these networks are also referred to as ad-hoc networks. These types of networks usually employ a two-level security mechanism. One level of security is provided at the link layer to protect every hop of communication and the other level of security is employed at the network/transport or application layer to protect the end-to-end communication path. Two most complicated operations in ad-hoc wireless networks are key management and secure routing. Fortunately, there has been a lot of research in this area and several security architectures for IEEE 802.11 multihop wireless ad-hoc networks and mobile ad-hoc networks (MANETs) have been proposed [42]. Decentralized cognitive networks could use security mechanisms employed in ad-hoc wireless networks. Some of the indigenous issues such as lack of a common control channel and use of diverse frequency bands by different secondary users may impose additional constraints on the existing security protocols.

7.2. Using Cryptographic Primitives

Most of the attacks performed at the link layer involve a malicious entity masquerading as a primary user. Therefore primary user identification is very important for both centralized and decentralized cognitive networks. We recently proposed a digital signature based primary user identification mechanism [23] that can be used by secondary users to distinguish malicious transmissions from primaries. Further research in the use of cryptographic primitives to solve inherent security issues in cognitive network needs to be performed.

7.3. Reactive Security Mechanisms

Reactive security mechanisms that detect malicious activity in cognitive networks need to be developed (see Chapter 12). For example, mechanisms that can detect unusually high spectrum handoffs is useful to prevent jamming and spectrum handoff attacks. Detection mechanisms combined with non-repudiation mechanisms enable secondary users to identify and block malicious users from the network.

7.4. Spectrum Aware Approach

There are two ways to handle spectrum mobility and associated delays. One is to make spectrum sensing, analyzing and handoff process fast and transparent to the higher layer protocols. However, spectrum sensing and handoff processes are in their infant stages and it will take a long time for such approaches to materialize. Another approach is a cross-layer methodology to incorporate spectrum mobility as state information in protocols operating in upper layers. Although this approach increases cross-layer dependencies, it will make the entire communication protocol spectrum aware and hence better defend some of the attacks on the upper layer protocols in cognitive networks. For example, routing should consider the operational spectrum band and its frequency characteristics and the transport layer should consider the effect of spectrum handoff on the round trip time and correspondingly adjust the retransmission window.

7.5. Robust Security Models

Reliable and robust models need to be developed for collaborative protocols. Instead of assuming a *Homo egualis* (see Section 4) type of model, a more secure Byzantine model could be used. The Byzantine model originates from the Byzantine generals' problem [22], which assumes the following scenario. A group of generals of the Byzantine army are camped with their troops around an enemy city. Communicating only by a messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. Such models have been used to provide fault tolerance in distributed computing and reliability in ad-hoc wireless networks [4]. These models could be used to provide increased security against malicious users in cognitive networks as well.

7.6. Develop Analog Crypto Primitives

One of the challenges in incorporating security mechanisms into cognitive networks is that in some frequency bands like the TV band, the primary base stations transmit analog signals (with the exception of HDTVs). Since most of the cryptographic primitives operate in the digital domain, it may not even be possible to incorporate them into analog TV signals. Hence, crypto primitives that work in analog domains need to be developed.

7.7. Use Light-weight Security Protocols and Primitives

If secondary users in cognitive networks have mobile equipments with limited processing power and resources, it would be a challenge to provide both cognitive radio capability

and security in real time. Light-weight security protocols [24] need to be developed for power/resource constrained environments.

8. Conclusions

The main motivation behind cognitive radios [26] has been to increase spectrum utilization by allowing the unlicensed (secondary) users to opportunistically access the frequency band actually owned by the licensed (primary) user. In contrast to other network security architectures, in cognitive radios networks, the users are categorized into two distinct classes: primary users and secondary users. In this chapter, we showed that this categorization gives rise to several security issues that are unique to cognitive radio communications. We also discussed various security aspects such as authentication and authorization of users, confidentiality and integrity of communication as well as identification and non-repudiation of cognitive user devices. Some reliability issues that are inherent in cognitive networks were examined. We then proposed several novel security attacks on different layers of the protocol stack in cognitive networks that make use of one or more of the inherent vulnerabilities. Through these attacks we showed that the fundamental idea behind cognitive networks (to have self-aware networks that offer resilient services and keep the intruders out of it simply by cognition) is not yet fulfilled. We then briefly examined several existing cognitive radio network architectures such as OCRA, Nautilus, IEEE 802.22 and DIMSUMnet with comments on their security. Finally, we suggested some future directions that need to be taken to make the protocols that are employed in cognitive radio networks 'spectrum aware' and hence more resilient to the attacks that we discussed.

Acknowledgments

This work is partially supported by grants from the U.S. Army and the NSF Cyber Trust grant 0627688.

References

[1] Aad, I., Hubaux, J.-P. and Knightly, E.W. (2004) Denial of service resilience in ad hoc networks. *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom '04)*, pp. 202–15, New York, USA.

[2] Akyildiz, I., Lee, W.-Y., Vuran, M.C. and Mohanty, S. (2006) Next generation/dynamic spectrum access/ cognitive radio wireless networks: a survey. *Computer Networks*, **50**(13), 2127–59.

[3] Akyildiz, I. and Li, Y. (2006) *OCRA: OFDM-based cognitive radio networks*. Broadband and Wireless Networking Laboratory Technical Report, March 2006.

[4] Awerbuch, B., Holmer, D., Nita-Rotaru, C. and Rubens, H. (2002) *An on-demand secure routing protocol resilient to byzantine failures*. ACM Workshop on Wireless Security (WiSe), September, Atlanta, Georgia. citeseer.ist.psu.edu/article/awerbuch02demand.html.

[5] Blanton, E. and Allman, M. (2002) On making TCP more robust to packet re-ordering. *ACM Computer Communication Review*, **-**(1).

[6] Buddhikot, M.M., Kolodzy, P., Miller, S., Ryan, K., and Evans, J. (2005) Dim-sumnet: new directions in wireless networking using coordinated dynamic spectrum access. *Proceedings of the 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05),* pp. 78–85, Washington, DC, USA.

[7] Cabric, D., Mishra, S. and Brodersen, R. (2004) Implementation issues in spectrum sensing for cognitive radios. *Signals, Systems and Computers*.

[8] Cabric, R.B.D. (2005) Physical layer design issues unique to cognitive radio systems. *Proceedings of the IEEE Personal Indoor and Mobile Radio Communications (PIMRC)*, vol. 2, pp. 759–63, September.
[9] Cam-Winget, N., Housley, R., Wagner, D. and Walker, J. (2003) Security flaws in 802.11 data link protocols. *ACM Communications*, **46**(5), 35–9.
[10] Cordeiro, D.B.C., Challapali, K. and Shankar, S. (2005) IEEE 802.22: the first worldwide wireless standard based on cognitive radios. *Proceedings of the IEEE DyS- PAN*, pp. 328–37, November.
[11] Digham, M.A.F. and Simon, M. (2003) On the energy detection of unknown signals over fading channels. *Proceedings of the IEEE ICC*, vol. 5, pp. 3575–9.
[12] Etkin, R., Parekh, A. and Tse, D. (2005) Spectrum sharing for unlicensed bands. *Proceedings of the IEEE DySPAN*, pp. 251–8, November.
[13] FCC (2003), *Notice of proposed rule making and order*, ET docket no 03-222, December.
[14] Ferguson, N. and Schneier, B. (2003) *Practical Cryptography*, John Wiley & Sons, Inc., New York, USA.
[15] FIPS (2001) *Specification for the advanced encryption standard (AES)*. Federal Information Processing Standards Publication 197. http://csrc.nist.gov/publications/_ps/_ps197/_ps-197.pdf.
[16] Ganesan, G. and Li, Y. (2005) Cooperative spectrum sensing in cognitive radio networks. *Proceedings of the IEEE DySPAN*, pp. 137–43, November.
[17] Gintis, H. (2000) *Game Theory Evolving: A Problem-Centered Introduction to Modeling Strategic Behavior*, Princeton University Press.
[18] Hu, Y.-C., Perrig, A. and Johnson, D.B. (2002) Ariadne: a secure on-demand routing protocol for ad hoc networks. *MOBICOM*, pp. 12–23.
[19] Jakobsson, M., Wetzel, S. and Yener, B. (2003) Stealth attacks on ad hoc wireless networks. *Proceedings of the VTC*.
[20] Jing, X. and Raychaudhuri, D. (2005) Spectrum co-existence of IEEE 802.22b and 802.16a networks using CSCC etiquette protocol. *Proceedings of the IEEE DySPAN*, pp. 243–50, November.
[21] Johansson, T (ed.) (2003) A concrete security analysis for 3GPP-MAC. *Fast Software Encryption*, LNCS 2887, Springer, Berlin.
[22] Lamport, L., Shostak, R.E. and Pease, M.C. (1982) The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, **4**(3), 382–401.
[23] Mathur, C. and Subbalakshmi, K. (2007a) Digital signatures for centralized dsa networks. *Proceedings of the Consumer Communications and Networking Conference (CCNC)*.
[24] Mathur, C. and Subbalakshmi, K. (2007b) Light weight enhancement to RC4 based security for resource constrained wireless devices. *International Journal of Network Security*, **5**(2).
[25] McHenry, M. (2003) *Spectrum white space measurements*. New America Foundation Broadband Forum, June.
[26] Mitola, J. (1995) The software radio architecture. *IEEE Communications Magazine*, May, 26–38.
[27] Mitola, J. (1999) Cognitive radio for flexible mobile multimedia communication. *Proceedings of the IEEE International Workshop on Mobile Multimedia Communications (MoMuC)*, pp. 3–10, November.
[28] Nanjunda, C., Haleem, M. and Chandramouli, R. (2005) Robust encryption for secure image transmission over wireless channels. *Proceedings of the IEEE International Conference on Communications*, vol. 2, May.
[29] Natkaniec, M. and Pach, A.R. (2000) An analysis of the back-o® mechanism used in IEEE 802.11 networks. *Proceedings of the Fifth IEEE Symposium on Computers and Communications*, p. 444, Washington, DC, USA.
[30] Naveed, A. and Kanhere, S.S. (2006) Security vulnerabilities in channel assignment of multi-radio multi-channel wireless mesh networks. *IEEE Globecom*, November.
[31] Reason, J.M. and Messerschmitt, D.G. (2001) The impact of confidentiality on quality of service in heterogeneous voice over IP. *Lecture Notes in Computer Science*, **2216**, 175.
[32] Santivanez, C.A., McDonald, A.B., Stavrakakis, I. and Ramanathan, R. (2002) On the scalability of ad hoc routing protocols. *Proceedings of INFOCOM*.
[33] Schneier, B. (1995) *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., New York, USA.
[34] Stallings, W. (1999) *Cryptography and Network Security: Principles and Practice*, Prentice-Hall, Upper Saddle River, NJ, USA.
[35] Tobagi, F. and Kleinrock, L. (1975) Packet switching in radio channels: Part II – the hidden terminal problem in carrier sense multiple-access and the busy-tone solution. *IEEE Transactions on Communications*, **23**, 1417–33.

[36] Visotsky, E., Kurner, S. and Peterson, R. (2005) On collaborative detection of tv transmissions in support of dynamic spectrum sharing. *Proceedings of the IEEE DySPAN*, pp. 338–45, November.

[37] Walker, J. (2000) *IEEE 802.11 wireless LANs unsafe at any key size: an analysis of the WEP encapsulation*. Technical report, Platform Networking Group, Intel Corporation, October. Available: citeseer.ist.psu.edu/558358.html.

[38] Wild, B. and Ramchandran, K. (2005) Detecting primary receivers for cognitive radio applications. *Proceedings of the IEEE DySPAN*, pp. 124–30, November.

[39] Xing, Y., Mathur, C., Haleem, M., Chandramouli, R., and Subbalakshmi, K. (2006a) Priority based dynamic spectrum access with QoS and interference temperature constraints. *Proceedings of the IEEE International Conference on Communications*, vol. 10, pp. 4420–5.

[40] Xing, Y., Mathur, C., Haleem, M., Chandramouli, R. and Subbalakshmi, K. (2006b) Dynamic spectrum access with QoS and interference temperature constraints. *IEEE Transactions on Mobile Computing*, **1**(8).

[41] Zapata, M.G. and Asokan, N. (2002) Securing ad hoc routing protocols. *Proceedings of the 3rd ACM Workshop on Wireless Security*, pp. 1–10, New York, USA.

[42] Zhou, D. (2003), *Security Issues in Ad Hoc Networks*, CRC Press, Inc., Boca Raton, FL, USA.