Security Vulnerabilities in IEEE 802.22

Kaigui Bian and Jung-Min "Jerry" Park
Department of Electrical and Computer Engineering
Virginia Tech, Blacksburg, VA 24061
{kgbian,jungmin}@vt.edu

ABSTRACT

Cognitive Radio (CR) is seen as one of the enabling technologies for realizing a new spectrum access paradigm, viz. Opportunistic Spectrum Sharing (OSS). IEEE 802.22 is the world's first wireless standard based on CR technology. It defines the air interface for a wireless regional area network (WRAN) that uses fallow segments of the licensed (incumbent) TV broadcast bands. CR technology enables unlicensed (secondary) users in WRANs to utilize licensed spectrum bands on a non-interference basis to incumbent users. The coexistence between incumbent users and secondary users is referred to as incumbent coexistence. On the other hand, the coexistence between secondary users in different WRAN cells is referred to as self-coexistence. The 802.22 draft standard prescribes several mechanisms for addressing incumbent- and self-coexistence issues. In this paper, we describe how adversaries can exploit or undermine such mechanisms to degrade the performance of 802.22 WRANs and increase the likelihood of those networks interfering with incumbent networks. The standard includes a security sublayer to provide subscribers with privacy, authentication, and confidentiality. Our investigation, however, revealed that the security sublayer falls short of addressing all of the key security threats. We also discuss countermeasures that may be able to address those threats.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*.

General Terms

Design, Security, Standardization

Keywords

IEEE 802.22, security, incumbent coexistence, self-coexistence, cognitive MAC

WICON'08 November 17-19, 2008, Maui, Hawaii, USA.

1. INTRODUCTION

IEEE 802.22 is the first wireless access standard based on Cognitive Radio (CR) technology. It specifies the air interface for a fixed wireless regional area network (WRAN) that operates in fallow TV broadcast bands [13]. An 802.22 *cell* is a single-hop, point-to-multipoint wireless network composed of a Base Station (BS) and several Consumer Premise Equipments (CPEs). The BS manages the CPEs within its cell and controls medium access via the Cognitive MAC (CMAC). Throughout the paper, incumbent services refer to TV broadcasting services or services for Part 74 devices[1] (wireless microphones) operating in TV bands. On the other hand, secondary users of the TV bands (i.e., BS and CPEs) are referred to as 802.22 entities. In 802.22, secondary users access incumbent spectrum bands opportunistically on a non-interference basis to incumbent users.

To protect incumbent services and achieve coexistence between incumbent users and secondary users (a.k.a. *incumbent coexistence*), IEEE 802.22 employs various incumbent protection mechanisms. The IEEE 802.22 standard mandates that CPEs perform distributed spectrum sensing (DSS) under the control of the BS. In this cooperative spectrum sensing approach, each CPE executes spectrum sensing on its own and sends its "local" spectrum sensing report to the BS, which then makes a final spectrum sensing decision. The presence of Part 74 devices is much more difficult to detect, compared to TV broadcast transmitters, due to their low transmission power. To protect Part 74 communications, 802.22 prescribes two classes of solutions: class A and class B. In the class B solution, class B CPEs are deployed to inform collocated 802.22 systems about the presence of Part 74 devices. Information gathered from regular CPEs and class B CPEs is used by the BS to identify fallow spectrum bands that are free of incumbent signals.

In IEEE 802.22, ensuring the congruous coexistence among overlapping WRAN cells (a.k.a. *self-coexistence*) is of paramount importance. Unlike other IEEE 802 standards, where self-coexistence is considered only after the specifications are essentially finalized, 802.22 takes a proactive approach and mandates that the MAC include self-coexistence mechanisms as part of the initial standard definition. In 802.22, the self-coexistence problem is exacerbated by the fact that a BS's coverage range may be as large as 100 Km [4]. Multiple

[1]Part 74 devices are low-power wireless devices, such as wireless microphones, which are licensed to operate in the TV broadcast bands.

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976

BSs and a number of CPEs under their control may operate in large overlapping regions. Without proper mechanisms to handle self-coexistence in such a situation, the resulting self-interference may render the 802.22 systems useless. There are two main technical challenges in self-coexistence: (1) minimizing the self-interference between overlapping cells and (2) satisfying the QoS of the cells' admitted service workloads in a dynamic spectrum access environment. The CMAC of 802.22 addresses self-coexistence using the inter-BS dynamic resource sharing mechanisms.

In an effort to provide subscribers with confidentiality, authentication, and data integrity, IEEE 802.22 prescribes a *security sublayer* that applies cryptographic transformations to MAC data units. Most of the features of the security sublayer are inherited from the security sublayer of IEEE 802.16e [11]. IEEE 802.16e is an amendment to the base standard, IEEE 802.16, and it addresses some of the base standard's security flaws by incorporating new security mechanisms [17]. Specifically, 802.16e incorporates the privacy key management scheme, PKMv2 [16], as part of the standard. The PKMv2 and the encapsulation protocol form the foundation of IEEE 802.22's security sublayer.

The security mechanisms supported by IEEE 802.22's security sublayer are insufficient to ensure robust security. The standard is vulnerable against various security threats which we will describe in this paper. The security vulnerabilities of IEEE 802.22 are partly due to the fact that the designers of the standard attempted to reuse the security sublayer designed for IEEE 802.16 networks. IEEE 802.22 networks are composed of cognitive radio nodes, and thus face unique security threats not faced by conventional networks. In this paper, we delineate security threats to 802.22, some of which are not addressed by the security sublayer. In particular, we describe how adversaries can exploit or undermine self-coexistence or incumbent coexistence mechanisms to degrade the performance of 802.22 WRANs and increase the likelihood of those networks interfering with incumbent networks. Attacks against the coexistence mechanisms are security threats unique to 802.22 networks (or cognitive radio networks, to be more precise). We also discuss possible countermeasures for thwarting the threats.

The rest of the paper is organized as follows. In Section 2, we provide the technical background needed to understand the security problems discussed in this paper. We discuss the attacks that exploit the vulnerabilities of 802.22's security protocols in Section 3. In Section 4, we discuss possible countermeasures for thwarting the attacks. Related work is presented in Section 5, and we conclude the paper in Section 6.

2. THE 802.22 AIR INTERFACE

One of the most critical design requirements of the 802.22 air interface (i.e., PHY and CMAC layers) is adaptability, which is best embodied in its coexistence mechanisms. In this section, we give a brief overview of the various aspects of 802.22's air interface that are relevant to coexistence.

2.1 PHY-Layer Support for Incumbent Coexistence

Spectrum sensing is one of the most important functionalities carried out by 802.22's air interface. 802.22 entities perform spectrum sensing to identify fallow licensed bands free from incumbent signals. The standard describes a two-stage spectrum sensing approach: *fast sensing* and *fine sensing*. The fast sensing stage is executed before the fine sensing stage, and it typically uses a quick and simple detection technique such as *energy detection*. The measurements from the fast sensing stage are used to determine the need and the duration of the subsequent fine sensing stage. The accuracy of a sensing technique is dependent on various environmental factors, such as the signal-to-interference ratio (SIR).

The 802.22 standard employs a distributed spectrum sensing framework. A CPE is required to report its local spectrum sensing results to its BS (i.e., the BS that controls the CPE) via CMAC-layer measurement messages. Using the local spectrum sensing results, the BS determines and adjusts various PHY-layer parameters such as channel bandwidth, modulation/encoding rate (e.g., QPSK with encoding rate $\frac{1}{2}$), etc.

2.2 The Cognitive MAC Layer

The MAC Protocol Data Unit (MPDU) is the smallest unit of transmission/reception in the CMAC. It is comprised of the MAC header, the MAC payload and the CRC (cyclic redundancy checking) field. There are two types of MPDUs. The two types are distinguished by their respective MAC headers, described below:

- General MAC header: This header is used for intra-cell general MPDUs. It is used in general MPDUs that contain either higher-layer data traffic or management messages in their payload.
- Beacon MAC header: This header is used for inter-cell beacons. An inter-cell beacon only carries beacon Information Elements (IEs) in its payload.

In IEEE 802.22, BSs and CPEs exchange inter-cell control messages using *inter-cell beacons*. Inter-cell beacons play a vital role in incumbent coexistence and self-coexistence mechanisms. Two types of inter-cell beacons are defined in the standard:

- BS beacons: These beacons are used to provide information about the BS's traffic schedule, the current operation channel of the cell, etc.
- CPE beacons: These beacons are used to provide information about a CPE's current cell of attachment as well as information on the traffic flows between the CPE and its BS.

2.2.1 Inter-Cell Synchronization

To facilitate incumbent signal detection, a BS periodically schedules a quiet period (QP). IEEE 802.22 recommends that neighboring BSs, if possible, synchronize their QPs to improve the reliability of incumbent signal detection. During these QPs, all network traffic is suspended, and 802.22 entities sense the channel for incumbent signals.

Suppose two overlapping cells, with two base stations BS_1 and BS_2, need to synchronize their transmissions. For every inter-cell beacon received from BS_1, BS_2 records the frame offset that indicates when it was received. Accuracy of this reception offset[2] is critical for successful synchroniza-

[2]The reception offset indicates the offset (in units of slot duration) relative to the start of the first slot of the frame where the beacon was received.

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976

tion. The transmission offset[3] is indicated in the beacon sent by BS_1. Figure 1 depicts the relationship between the transmission offset and the reception offset.

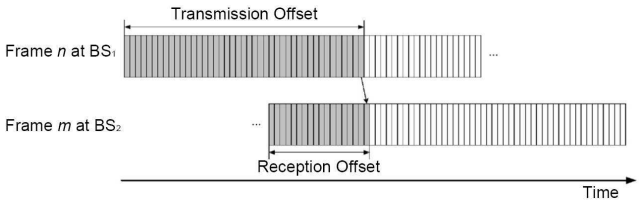

Figure 1: Synchronization of overlapping BSs.

After receiving BS_1's beacon, BS_2 attempts to synchronize with BS_1 by sliding its frames using the following *convergence rule*:

- If $\left(FDC - O_{Tx} + O_{Rv} \leq \lceil \frac{FDC}{2} \rceil\right)$, slide frames right by $(FDC - O_{Tx} + O_{Rv})$;
- Otherwise, slide frames left by $(O_{Tx} - O_{Rv})$,

where O_{Tx} is the transmission offset, O_{Rv} is the reception offset, and FDC is Frame Duration Code (i.e., time duration of a frame).

2.2.2 Inter-BS Dynamic Resource Sharing

Every cell requires a certain number of channels to satisfy the QoS of its admitted service workload. When the current channel condition is not sufficient to support the required QoS of its workload, a BS in need of spectrum initiates an inter-BS dynamic resource sharing process so that better channels or more channels can be acquired from neighboring cells. 802.22 prescribes two types of inter-BS dynamic resource sharing mechanisms: *non-exclusive* spectrum sharing and *exclusive* spectrum sharing.

After selecting a *target channel*, the BS in need of spectrum has to determine whether non-exclusive sharing of the selected channel is feasible using the following criterion: non-exclusive spectrum sharing is feasible as long as the maximum achievable SIR on the selected channel is higher than the required SIR threshold of the network's supported services. If non-exclusive sharing is feasible, the BS schedules data transmissions on the selected channel with appropriate transmission power control settings. Transmission power control is needed to minimize interference to co-channel neighboring 802.22 systems.

If the maximum achievable SIR on the selected channel is lower than the required SIR threshold, then the BS needs to acquire the spectrum resources through exclusive spectrum sharing. 802.22 prescribes exclusive spectrum sharing via the *On-Demand Spectrum Contention (ODSC)* protocol [7]. The BS that initiates the ODSC is called the *contention source*. The contention source randomly selects a *channel contention number* (CCN) that is uniformly distributed in the range $[0, W]$, where W is the contention window size. The CCN is used for determining the "winner" of each pair-wise contention. After selecting the target channel, the contention source includes its CCN in a spectrum contention request that it broadcasts to its co-channel, neighboring BSs (i.e., *contention destinations*). After receiving a spectrum contention request, a contention destination selects a CCN in the same manner as the contention source. Then the contention destination uses the following contention resolution rule to determine which BS wins this pair-wise contention: the BS with a greater CCN value wins the pair-wise contention. According to this contention resolution rule, the contention source's probability of winning a pair-wise contention is 1/2. The contention source wins the contended channel only if it wins *all* of the pair-wise contentions. If the contention source wins the contended channel, all contention destinations perform channel switching to vacate the target channel.

[3]The transmission offset indicates the offset (in units of slots) relative to the start of the first slot of the frame where the the beacon is transmitted.

2.2.3 Protection of Part 74 Devices

Part 74 devices are much harder to detect compared to TV broadcast transmitters due to their significantly lower transmission power. The current 802.22.1 Task Group is considering options for the protection of Part 74 devices. Two classes of solutions—class A and class B—have been identified. In class A, a separate beacon device is deployed to transmit short wireless microphone beacon (WMB) messages to notify collocated 802.22 systems about the presence of co-channel wireless microphone operations. In class B, the 802.22 system supports a special type of CPE that has specific capabilities to inform collocated 802.22 systems about wireless microphone operations. The 802.22 draft standard states that a single approach is not the best solution.

In the class B solution, a class B CPE shall transmit WMBs to notify neighboring BSs about the scheduled wireless microphone operation during the QPs of the BSs. Upon receiving a WMB, the BS shall acknowledge the reception of the WMB by including a Part 74 acknowledgement in the BS beacons.

2.3 An Overview of the IEEE 802.22 Security Sublayer

The security sublayer defined in 802.22 provides confidentiality, authentication, and data integrity services by applying cryptographic transformations to MAC data units carried across connections between CPEs and the BS. The security sublayer has two components: an encapsulation protocol and a Privacy Key Management (PKM) protocol. The encapsulation protocol defines a set of supported cryptographic suites (i.e., pairings of data encryption and authentication algorithms) and the rules for applying those algorithms to a MPDU payload. The PKM protocol ensures the secure distribution of keying material from the BS to the CPEs.

The security sublayer protects network control information by attaching message authentication codes to CMAC management messages. However, the security sublayer only protects *intra-cell* CMAC management messages and does not protect *inter-cell* beacons. Therefore, inter-cell beacons are vulnerable to unauthorized modification or forgery. In the next section, we describe how adversaries can exploit this weakness to launch attacks against 802.22's coexistence mechanisms. Figure 2 illustrates 802.22 air interface's functionalities and the ones protected by the security sublayer.

3. SECURITY VULNERABILITIES IN 802.22

IEEE 802.22 networks are vulnerable to several security threats. As noted in [20], the current draft standard does not specify any security mechanisms to protect sensing and

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976

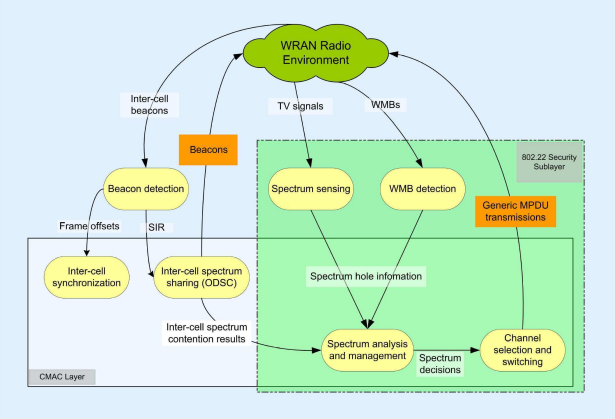

Figure 2: The 802.22 air interface's functionalities and the ones protected by the security sublayer.

geolocation information as well as information coming from the incumbent database. In this section, we review the security threats against 802.22. Note that the security sublayer has provisions to address some, but not all, of these threats. In Subsections 3.2 and 3.3, we focus our discussions on security threats unique to cognitive radio networks—i.e., threats against 802.22's self-coexistence and incumbent coexistence mechanisms.

3.1 The Security Threats

3.1.1 Denial of Service (DoS)

In an opportunistic spectrum sharing environment, it is necessary to ensure the availability of spectrum for the incumbent users as well as the secondary (WRAN) users. In the context of opportunistic spectrum sharing, a DoS attack (an incumbent DoS or WRAN DoS attack [20]) involves the insertion of forged management messages by rogue terminals to create havoc for the spectrum sensing or spectrum allocation processes. The 802.22 security sublayer provides protection against this type of attack in two ways: (1) PKMv2 is used to provide mutual authentication between a BS and a CPE, thus preventing a rogue terminal from masquerading as a legitimate terminal and (2) message authentication codes are used to protect the authenticity and integrity of critical management messages exchanged within an 802.22 cell.

3.1.2 Replay Attacks

The replay of captured messages is common attack tactic used by adversaries. In an incumbent replay attack [20], an adversary captures and replays the local sensing reports (which is one of many types of intra-cell management messages defined in 802.22) sent by CPEs to their BS. This may cause the BS to make incorrect spectrum sensing decisions. The security sublayer provides protection against the replay of intra-cell management messages by employing nonces in challenge/response protocols.

IEEE 802.22 thwarts the replay of data packets by using AES (Advanced Encryption Standard) in CCM mode (counter encryption mode with cipher-block-chaining message authentication code). CCM combines counter mode encryption (for data confidentiality) and cipher block chaining message authentication code (for data authenticity). IEEE 802.22 requires that a packet number is inserted into each MPDU. If AES in CCM mode is chosen to encrypt MPDUs, a window has to be used for packet number values in order to validate the freshness and uniqueness of the packet. A receiver validates the received data packets by verifying that the packets correctly decrypt under AES-CCM and have monotonically increasing packet numbers. The replay countermeasures of the 802.22 security sublayer are inherited from the 802.16e security sublayer.

3.1.3 Spurious Transmissions in QPs

In [20], Mody et al. discuss another type of attack that pose a threat to 802.22—spurious transmissions (or jamming) in quiet periods (QPs). By transmitting spurious messages in QPs, an adversary can interfere with the various coexistence-related control mechanisms carried out during QPs. Non-adversarial devices may also cause spurious transmissions as a result of hardware and/or software defects.

3.1.4 Incumbent Signal Emulation

In primary (incumbent) user emulation (PUE) attacks, an adversary's CR transmits signals whose characteristics emulate those of incumbent signals. This type of attack is also known as "incumbent ghosting" [20]. The highly flexible, software-based air interface of CRs makes such an attack possible. A PUE attack interferes with the spectrum sensing process and significantly reduces the channel resources available to legitimate secondary users. In [3], Chen et al. propose a transmitter verification scheme, called *LocDef* (localization-based defense) that uses both signal characteristics and location of the signal transmitter to verify incumbent users' signals.

3.1.5 Security Threats against WMBs

IEEE 802.22 prescribes two solutions (class A and class B) to detect the presence of Part 74 devices. In the class B solution, the standard prescribes the use of class B CPEs to detect Part 74 signals. If Part 74 signals are detected, a class B CPE sends a WMB to collocated BSs in its vicinity. The 802.22 standard specifies that each class B CPE needs to possess pre-programmed security keys that enable the use of an authentication mechanism to prevent the forgery and modification of WMBs. The security sublayer protects WMBs from replay attacks in the same manner as it protects intra-cell management messages.

3.1.6 Security Vulnerabilities in Coexistence Mechanisms

One of the most significant security oversights in IEEE 802.22 is the lack of protection provided to inter-cell beacons. All inter-cell control messages are vulnerable to unauthorized modification, forgery, or replay. As noted previously, most of the security features of the 802.22 security sublayer is inherited from the 802.16e's security sublayer. Therefore, the 802.22's security sublayer does not take into account the important difference between 802.16e and 802.22, viz. the incumbent and self-coexistence mechanisms. Specifically, 802.22's security sublayer fails to protect the inter-cell beacons used to carry out coexistence mechanisms.

In Subsection 3.2, we describe an attack that disrupts the

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976

inter-cell spectrum contention process, and in Subsection 3.3, we describe an attack that impedes inter-cell synchronization. In both attacks, the adversary forges or manipulates inter-cell beacons to achieve its attack objective. We coin the term *beacon falsification* (BF) attack to refer to such an attack. To carry out a BF attack, an adversary needs to be able to install manipulated software or modify software already installed on a CR to manipulate the CR's behavior—this is a plausible scenario given that the CR's software is just as vulnerable as PC software.

3.2 Disrupting Inter-Cell Spectrum Contention

3.2.1 Description of the Attack

A terminal under the control of an adversary first selects the operation channel of a WRAN cell (i.e., "victim cell") as the target channel by eavesdropping on the BS beacons transmitted by the victim cell's BS. Then the attacker's terminal sends spurious contention requests via forged inter-cell beacons to the victim cell. This will trigger the victim cell to participate in an inter-cell spectrum contention process via the ODSC protocol. To increase the probability of winning the target channel, the malicious terminal may arbitrarily select a very large CCN value. If the victim cell loses the contention, then it vacates the current operation channel (i.e., target channel) and switches to another channel.

If the attacker initiates spectrum contention processes with high frequency and wins most of those contentions, then the victim cell is forced to waste a significant proportion of its network resources in switching channels. This would ultimately lead to significant degradation in network performance. Note that the capture and subsequent replay of contention requests with large CCN values by the adversary would have a similar effect.

Since all traffic activity is suspended during a cell's QP, the attacker's spurious inter-cell beacons have the best chance of being received by a victim cell during its QPs. This means that the attacker can increase the effectiveness of the attack by synchronizing its transmissions with the victim cell's QPs.

In this attack, the objective of the adversary is to maximize its chance of winning the target channel in a spectrum contention process while not arousing the suspicion of the contention destinations. One way of achieving this objective is for the adversary to employ the following strategy. The adversary selects a CCN that is uniformly distributed in the range $[W/z, W]$, where $z \geq 1$ is an adjustable parameter, and inserts this value in an inter-cell beacon. Then the adversary emits this forged beacon to neighboring BSs during their QPs. Let α_a denote the attacker's CCN, and α_d denote a contention destination BS's CCN that is uniformly distributed in the range $[0, W]$. Then we calculate the probability that the adversary will successfully win the target channel. The probability that the adversary wins a pair-wise contention from one contention destination is

$$p_p = \int_0^{W/z} Pr\{\alpha_a > \alpha_d | \alpha_d = x\} \cdot \frac{1}{W} dx + \int_{W/z}^{W} Pr\{\alpha_a > \alpha_d | \alpha_d = x\} \cdot \frac{1}{W} dx = \frac{1}{z} + \frac{z-1}{2z} = \frac{z+1}{2z}.$$

Therefore, the probability that the adversary will win the target channel from k contention destinations is

$$p_w = (p_p)^k = \left(\frac{z+1}{2z}\right)^k.$$

3.2.2 Attack's Effect on Channel Capacity

To discuss the attack's impact on channel capacity, we adopt the modeling approach used in [10] and assume that the presence or absence of incumbent users' signals on a channel, say channel i, can be modeled as a continuous-time "ON/OFF" Poisson process, where inter-arrival times of consecutive incumbent signals are exponentially-distributed with a rate parameter. Let the random variable V_i denote the length of an incumbent's idle interval (*incumbent idle time period*) on channel i. Similarly, let the random variable U_i denote the length of an incumbent's busy interval (*incumbent busy time period*) on channel i. Suppose that $E[V_i] = v_i$ and $E[U_i] = u_i$. The probability that channel i is free of incumbent users' signals is

$$\alpha_i = \frac{v_i}{v_i + u_i}.$$

Let T denote the duration of a *channel contention period*. At the end of every contention period, a *contention phase* is scheduled during a QP for contending the selected channel, and the length of one QP is S. The channel contention period also contains a *data transmission phase* of length $(T - S)$. 802.22 entities of a given cell cannot immediately start to access a channel until the BS determines that the channel is fallow based on spectrum sensing measurements. A QP is needed for performing spectrum sensing and channel setup before an 802.22 entity can access the channel. As shown in Figure 3, the incumbent idle time period is composed of a quiet period, a number of contention periods and a residual time interval R, where $0 \leq R < T$. Contention phases incur control overhead, thus reducing network performance. One way of quantifying this control overhead is to consider the length of a contention phase, S. S must be long enough to perform contention-related operations, such as determining the target channel(s), performing pair-wise contentions (via the exchange of inter-BS control messages), and preparation for resuming transmissions on a new channel (if a new channel has been acquired or if a channel switching event has occurred).

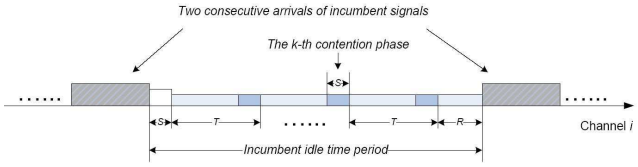

Figure 3: The model used for analyzing the attack's effect on channel capacity.

Suppose an attacker sends spurious contention requests to contend for the target channel, channel i, in every scheduled contention phase and wins the channel in the k^{th} contention phase. Under this assumption, the average transmission time for a cell on channel i during an incumbent

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976

idle time period is

$$\mathcal{T}(i) = \int_S^{\infty} \sum_{k=1}^{\lfloor \frac{t-S}{T} \rfloor} (1-p_w)^{(k-1)} \cdot p_w \cdot k \cdot (T-S) \cdot p_t(i) dt,$$

where $p_t(i)$ is the probability that there is no incumbent signal arrival in channel i during a time interval of t; this value can be calculated using the following equation:

$$p_t(i) = \int_t^{\infty} \frac{1}{v_i} \cdot e^{-\frac{u}{v_i}} du = e^{-\frac{t}{v_i}}.$$

The resulting channel capacity is

$$\mathcal{C}(i) = \alpha_i \cdot \frac{\mathcal{T}(i)}{v_i}.$$

In the absence of any channel contention requests (both legitimate and spurious), the average transmission time of a cell on channel i during an incumbent idle time period is

$$\mathcal{T}^*(i) = \int_S^{\infty} \left[\lfloor \frac{t-S}{T} \rfloor \cdot (T-S) + \min(R, T-S) \right] \cdot p_t(i) dt,$$

In this case, the resulting channel capacity is

$$\mathcal{C}^*(i) = \alpha_i \cdot \frac{\mathcal{T}^*(i)}{v_i}.$$

Since $\mathcal{T}(i) < \mathcal{T}^*(i)$, we can conclude that $\mathcal{C}(i) < \mathcal{C}^*(i)$.

3.2.3 Simulation Results

The 802.22 WG has suggested that a variation of the *Hata model* is the most appropriate propagation model for studying 802.22 WRANs [14]. Hata modeled the urban area propagation loss as a standard formula and used correction equations to modify this formula so that the model is applicable to suburban and open rural areas [24]. Using the Hata model and the ODSC protocol, we performed simulations to evaluate the impact of BF attacks (i.e., attacks that interfere with inter-cell spectrum contention) on 802.22 WRAN performance. Figure 4 illustrates the simulation layout. The victim WRAN cell includes a BS and ten CPEs. The BS schedules the superframes by periodically transmitting BS beacons and divides each superframe into 16 frames (see [13] for how a BS schedules superframes). We use a Cartesian coordinate system to represent the location of the 802.22 entities. The BS is located at position (0,0), and CPE_1, which is the CPE nearest to the attacker, is located at (20 Km, 0). The attacker's radio device, CPE_A, is initially positioned at (40 Km, 0). We define d as the distance between CPE_A and CPE_1. The initial value of d is 20 km. We assume that the victim cell's coverage area is defined by a circular region whose radius is equal to CPE_1's x-coordinate value.

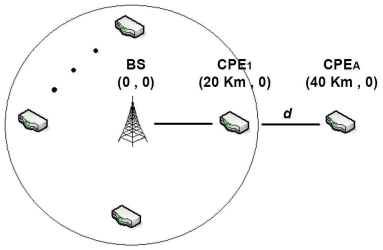

Figure 4: Simulation layout.

The values of the simulation parameters were chosen to be consistent with those used in the simulation experiments of [12, 21]. We assume that the frame size, the length of a QP, and channel switching delay are 40 ms, 5 ms, and 20 ms, respectively. We assume that a channel bonding mechanism is employed to utilize three 8 Mbps TV channels together. We also assume that all entities use QPSK modulation. The attacker's transmission power is set to 36 dBm (about 4 Watts), which is the suggested maximum CPE transmission power [12].

We fixed the network load at 24 Mbps and varied three parameters that are under the control of the attacker. These parameters are: r (attack rate: the number of contention requests sent during a QP), z (parameter for changing the attacker's contention window size), and d (distance between CPE_A and CPE_1). The victim cell's throughput vs. d is plotted in Figures 5 and 6.

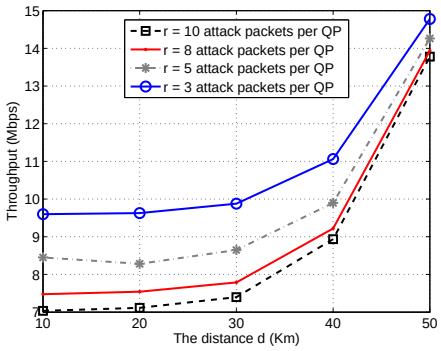

Figure 5: Throughput vs. d (z is fixed to 2).

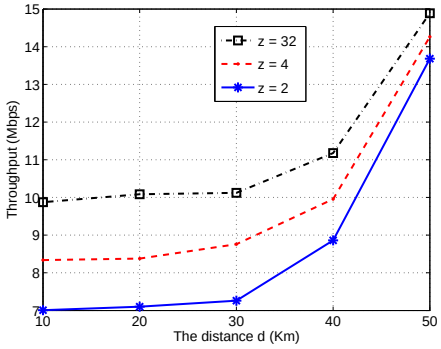

Figure 6: Throughput vs. d (r is fixed to 10).

3.3 Interfering with Inter-Cell Synchronization

The 802.22 standard states that overlapping cells should synchronize their QPs, when possible, to improve the accuracy of spectrum sensing. As noted previously, there is no security mechanism prescribed by 802.22 that protects the inter-cell beacons against forgery or unauthorized modification. Since neighboring cells coordinate synchronization by exchanging inter-cell beacons, the inter-cell synchronization process is just as vulnerable to BF attacks as the inter-cell

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976

spectrum contention process. It is possible for an adversary to insert false frame offsets in inter-cell beacons. Suppose an adversary inserts spurious transmission offset values in inter-cell beacons and transmits those beacons to two cells that are adjacent to each other. The false information contained in the spurious beacons may cause the two cells to calculate incorrect frame sliding lengths, thus leading to imprecise synchronization of the two cells. In turn, the impreciseness of synchronization leads to increased inaccuracy in spectrum sensing. If the QPs of the two cells are not synchronized, secondary users of those cells need to detect incumbent signals in the midst of secondary signals, which makes spectrum sensing more difficult and may require the use of costly detection techniques such as cyclostationary feature detection.

3.3.1 Impact of the Attack in Energy Detection

The *fast sensing* stage described in 802.22 adopts a quick and simple detection algorithm such as energy (power) detection. We describe how BF attacks can affect the accuracy of spectrum sensing when energy detection is used. We adopt the energy detector model described in [26].

An energy detector detects a given signal by estimating the signal's received power and comparing the estimate with a threshold [27]. The energy detector's detection algorithm takes the form of a hypothesis test with two hypotheses:

$$H_0 : y(n) = w(n),$$
$$H_1 : y(n) = x(n) + w(n),$$

where $y(n)$ is the signal observed by the detector, $x(n)$ is the signal component due to an incumbent signal and $w(n)$ is complex additive white Gaussian noise. The test statistic, Y, for the energy detector is an estimate of the received signal power. Under certain assumptions, we can derive the value of the detector threshold, γ, for test statistic Y:

$$\gamma = N \cdot B \left(1 + \frac{Q^{-1}(P_{FP})}{\sqrt{M}}\right), \quad (1)$$

where P_{FP} is the maximum allowable false positive probability (typically set to 0.1), M is the number of samples, N is the noise spectral density, and B is the sampling bandwidth. See [26] for details on the derivation. The energy detector selects hypothesis H_1 if $Y > \gamma$ and selects H_0 if otherwise.

A BF attack may result in asynchronous QPs. In turn, this causes a scenario in which a cell performs spectrum sensing while neighboring cells transmit their signals. In such a scenario, transmissions by 802.22 entities of neighboring cells contribute to the noise power (i.e., $N \cdot B$) in (1), thus causing the detector threshold to increase to a larger value, say γ^*. In this case, the probability of misdetection (i.e., failure to detect an incumbent signal) increases by

$$Pr(\gamma < Y < \gamma^*) = \int_{\gamma}^{\gamma^*} f_Y(x)dx,$$

where $f_Y(x)$ is the probability density function of the test statistic Y under hypothesis H_1.

4. COUNTERMEASURES TO THE SECURITY THREATS

Most of 802.22's serious security vulnerabilities are due to the lack of protection provided to the inter-cell beacons. Security mechanisms are needed to thwart the forgery and unauthorized modification of the beacons. Specifically, security mechanisms are needed to ensure the authenticity and integrity of the beacons. To provide such security services, an inter-cell key management scheme is needed. In the following subsections, we discuss the technical challenges in the implementation and deployment of an inter-cell key management scheme.

4.1 Key Management Infrastructure

There are plenty of existing cryptographic solutions that can be utilized to thwart the forgery, modification, or replay of inter-cell beacons. The more difficult challenge is securely handling the generation, distribution, and revocation of keys needed in those cryptographic solutions. The security sublayer does not address the problem of inter-cell key management. Although the security sublayer includes the PKM protocol, PKM is only capable of managing *intra-cell* keys and does not have any provisions to support the management of *inter-cell* keys.

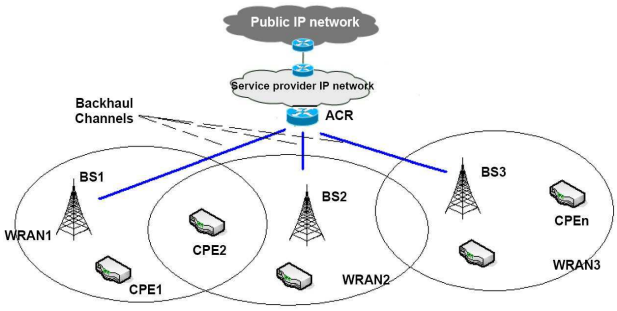

Figure 7: A backhaul infrastructure for 802.22 WRANs.

One possible approach for designing an inter-cell key management scheme is to utilize the backhaul infrastructure that connects multiple WRANs, if such an infrastructure exists. Use of a backhaul infrastructure would provide a secure way of distributing inter-cell keys. In a typical backhaul infrastructure, multiple WRANs are connected to an access control router (ACR) via backhaul channels (see Figure 7). The ACR is connected to the service provider IP network which, in turn, is connected to the public IP network. However, this approach may not be feasible due to the fact that different cells are often managed by different wireless operators. 802.22 WRANs are networks based on license-exempt operation, and hence the existence of a common backhaul infrastructure amongst competing operators serving a given location may be unlikely, and cannot be assumed.

4.2 Distributed Key Management

If a common backhaul infrastructure amongst cells (managed by competing wireless service operators) is not available, a distributed key management scheme is needed. In such a scheme, 802.22 BSs cooperatively utilize a distributed algorithm to manage inter-cell keys. A comprehensive survey on key management schemes is given in [9], which classifies key management schemes into two categories: contributory and distributive. The contributory category is defined to encompass schemes where the key is a result of a collaborative effort of multiple nodes. The distributive category

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976

includes schemes where each key originates from a single node.

In contributory schemes, there is no trusted third party that is responsible for the generation and distribution of the cryptographic keys. Instead, all communicating parties cooperate to establish (i.e., "agree" upon) a secret symmetric key. The Diffie-Hellman algorithm [5], which enables two parties to establish a pair-wise shared key, is a simple example of a contributory scheme. The contributory approach seems to be appropriate for the decentralized nature of the inter-cell key management problem. The drawback of most contributory schemes is that they are vulnerable to the Man-In-the-Middle (MIM) attack [9].

In distributive schemes, each node generates a key and distributes it to others. In [28], Zhou and Haas propose a distributed public-key management scheme for ad hoc networks. In their scheme, the functionality of the central certificate authority (CA) is distributed over a subset of nodes through a threshold cryptographic scheme that can tolerate at most K intruders. A more recent proposal by Luo et al. [19] describes a similar approach that allows any node to carry a share of the private key of the system CA. However, this scheme is vulnerable to the impersonation attack and the Sybil attack [6]. In a Sybil attack, an attacker uses as many identities as necessary (more than K) so that it can collect enough shares of the system CA's private key to reconstruct the private key.

5. RELATED WORK

MAC-layer misbehaviors have been studied previously in the context of 802.11 Distributed Coordination Function (DCF) [15]. We discuss existing work on misbehaviors in 802.11 DCF, since such security issues have some traits in common with the security threats discussed in this paper. In [8], the authors study simple DoS attacks at the MAC layer and show the impact of the attacks using simulation results. The authors used multiple different attack traffic patterns in the simulations. In [1], Bellardo et al. describe vulnerabilities in the 802.11 MAC protocol and explain how to exploit them by tampering with 802.11 MAC firmware. In [25], Raya et al. discuss MAC-layer misbehaviors in wireless hotspots. The authors describe a particular type of misbehavior in which an adversary sends spurious RTS/CTS frames to reserve a channel without any intention of actually using the channel for transmissions. The paper also discussed detection techniques for detecting such attacks. It is widely known that a selfish node can exploit the 802.11 DCF to get priority access to a channel. Specifically, a selfish node can unilaterally modify the parameters in the back-off mechanism to get priority access to the channel. As a result, the selfish node achieves better throughput. There are existing works that propose schemes for detecting the aforementioned selfish behavior. Kyasanur and Vaidya [18] proposed a detection scheme that enables the receiver to assign and send back-off values to the sender in CTS and ACK frames so that those values can be used later to detect misbehavior. A detection framework based on sequential analysis was introduced in [23]. This scheme does not require any modification to the current 802.11 DCF.

To a large extent, security in cognitive radio (CR) networks is an uncharted research area that needs to be further explored. There are only a handful of works on this topic. In [22], the authors note that primary (or incumbent) user emulation attacks pose a serious threat to CR networks. Chen et al. [3] explain the impact of such attacks on CR network performance and propose a scheme for detecting them. A comprehensive discussion of potential DoS threats to CR networks and countermeasures can be found in [2].

6. CONCLUSIONS

In this paper, we have discussed a broad range of security threats to IEEE 802.22. Some of those threats are addressed by 802.22's security sublayer while others are not. Some of the security threats not addressed by the security sublayer exploit the fact that the current 802.22 draft standard prescribes no security mechanisms to thwart the forgery and unauthorized modification of inter-cell beacons. Inter-cell beacons play an important role in carrying out many crucial network functions—especially functions needed for addressing incumbent coexistence and self-coexistence issues. In this paper, we described an attack, called the *beacon falsification* attack, in which adversaries transmit spurious inter-cell beacons to disrupt vital network functions, such as inter-cell spectrum contention and inter-cell synchronization.

7. REFERENCES

[1] J. Bellardo, S. Savage and D. Medina, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," in *Proc. of the USENIX Security Symposium*, August 2003, pp. 15–27.

[2] T. X. Brown, and A. Sethi, "Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: a Multi-dimensional Analysis and Assessment," *Journal of Mobile Networks and Applications Special Issue on Cognitive Radio Oriented Wireless Networks and Communications*, Vol. 13(5), October 2008, pp. 516–532.

[3] R. Chen, J.-M. Park, and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communcations Special Issue on Cognitive Radio Theory and Applications*, Vol. 26 (1), January 2008, pp. 25–37.

[4] C. M. Cordeiro, K. Challapali, and D. Birru, "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios," *Journal of communications*, Vol. 1(1), April 2006, pp. 38–47.

[5] W. Diffie, and M. E. Hellman, "New Directions in Cryptography," *IEEE Transsactions on Infomation Theory*, Vol IT-22(6), Nov. 1976, pp. 644–654.

[6] J. R. Douceur, "The Sybil Attack," in *Proc. of the First International Workshop on Peer-to-Peer Systems (IPTPSą́02)*, 2002, pp. 251–260.

[7] D. Grandblaise and W. Hu, "Inter Base Stations Adaptive On Demand Channel Contention for IEEE 802.22 WRAN Self Coexistence," IEEE docs: IEEE 802.22-07/0024r0, Januarary 2007.

[8] V. Gupta, S. Krishnamurthy and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," in *Proc. of IEEE Military Communications Conference (MILCOM '02)*, 2002, pp. 1118-1123.

[9] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," *IEEE*

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976

Communications Surveys & Tutorials, the 3rd Qtr. 2006, Vol. 8(3), pp. 48–66.

[10] S. Huang, X. Liu, and Z. Ding, "Opportunistic Spectrum Access in Cognitive Radio Networks," in *Proc. of IEEE INFOCOM 2008*, April 2008.

[11] IEEE 802.16 Task Group E, "Amendment to IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems—Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," IEEE Standard 802.16e-2005, IEEE Press, 2005.

[12] IEEE 802.22 WG, "ETRI FT Philips Samsung Proposal," IEEE docs: 22-06-0005-01-0000, January 2006.

[13] IEEE 802.22 WG, "IEEE P802.22/D0.1 Draft Standard for Wireless Regional Area Networks Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands," IEEE docs: 22-06-0067-00-0000_P802-22_D0.1, May 2006.

[14] IEEE 802.22 WG, "Reviews of Channel Model," IEEE docs: 22-05-0070-00-0000, August 2005.

[15] IEEE Standard for Wireless LAN-Medium Access Control and Physical Layer Specification, 802.11, 1999.

[16] D. Johnston and J. Walker, "Mutual Authorization for PKMv2", IEEE C802.16e-04/229, 2004.

[17] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," *IEEE Security & Privacy*, Vol. 2(3), May 2004, pp. 40–48.

[18] P. Kyasanur and N. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," *IEEE Transaction on Mobile Computing*, Vol. 4(5), September-October 2005, pp. 502–516.

[19] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," *IEEE/ACM Transaction on Networking*, Vol.12(6), pp.1049–1063, December 2004.

[20] A. N. Mody, R. Reddy, M. J. Sherman, T. Kiernan, and DJ Shyy, "Security and the Protocol Reference Model Enhancements in IEEE 802.22," IEEE doc: 802.22-08/0083r04, June 2008.

[21] J. Notor, "The Evolution of Spectrum Sharing in the IEEE 802.22 WRAN Standards Process," February 2006. Available at: `http://www.eecs.berkeley.edu/~dtse/3r_otherpapers.html`

[22] P. Pawelczak, "Protocol Requirements for Cognitive Radio Networks," Technical Report, July 2005. Available at: `https://doc.freeband.nl/dscgi/ds.py/Get/File-60831`

[23] S. Radosavac, J. S. Baras and I. Koutsopoulos, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks," in *Proc. of the 4th ACM workshop on Wireless security (Wise '05)*, 2005, pp. 33–42.

[24] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Upper Saddle River, NJ: Prentice Hall, 2001.

[25] M. Raya, J.P. Hubaux and I. Aad, "DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots," in *Proc. of the International Conference on Mobile Systems, Applications, and Services (MobiSys '04)*, June 2004, pp. 84–97.

[26] S. J. Shellhammer, S. Shankar N, R. Tandra, and J. Tomcik, "Performance of Power Detector Sensors of DTV Signals in IEEE 802.22 WRANs," in *Proc. of the first international workshop on Technology and policy for accessing spectrum (TAPAS'06)*, 2006.

[27] H. Urkowitz, "Energy Detection of Unknown Deterministic Signals", in *Proc. of IEEE*, April 1967, pp. 523–531.

[28] L. Zhou and Z. Haas, "Securing Ad Hoc Networks", *IEEE Network*, Vol. 13(6), 1999, pp. 24–30.

Digital Object Identifier: 10.4108/ICST.WICON2008.4976
http://dx.doi.org/10.4108/ICST.WICON2008.4976