Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security

Jack L. Burbank
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723
jack.burbank@jhuapl.edu

Abstract - **This paper discusses the topic of wireless security in cognitive radio networks, delineating the key challenges in this area. With the ever-increasing scarcity of spectrum, cognitive radios are expected to become an increasingly important part of the overall wireless networking landscape. However, there is an important technical area that has received little attention to date in the cognitive radio paradigm: wireless security. The cognitive radio paradigm introduces entirely new classes of security threats and challenges, and providing strong security may prove to be the most difficult aspect of making cognitive radio a long-term commercially-viable concept. This paper delineates the key challenges in providing security in cognitive networks, discusses the current security posture of the emerging IEEE 802.22 cognitive radio standard, and identifies potential vulnerabilities along with potential mitigation approaches.**

I. Introduction

Communication as we know it is rapidly changing. A rapidly increasing subscriber base and the emergence of high data throughput applications continue to fuel the rapidly increasing demand for broadband wireless services. Both have led to the development of numerous wireless technologies that continuously evolve with ever-increasing capabilities. Cellular communications standards have evolved from tens of kbps types of services with 1G technology to hundreds of kbps types of services with 2G and 2.5 G technologies to multi-Mbps services provided by 3G technologies such as cdma2000. The demand for high-performance wireless local area network (WLAN) solutions have led to the rapid evolution of technologies such as IEEE 802.11 from tens to hundreds of Mbps types of capability with an ever-increasing amount of support for flexible operations, such as mobility and roaming support. Interest in broadband wireless access is also evident from the tremendous interest and increasing deployment of IEEE 802.16-based WiMAX technologies, which can provide tens of Mbps to nomadic users. In fact, this insatiable demand for broadband wireless services and the desire of corporations to capitalize on this demand has pushed the wireless industry to evolve into one of the most competitive industries in the world, often characterized by bitter politics and technology wars.

The one undeniable constraint in providing the types of wireless capability that is demanded by users commercial and military alike is spectrum. Spectrum is a precious resource, and there is simply not enough to meet the needs of today and tomorrow's user base. This problem is exacerbated by the outdated way in which we manage spectrum. Regulatory agencies, such as the Federal Communications Commission (FCC), allocate spectrum for particular types of services that are then licensed to bidders for a fee. Those allocations and licenses are static in nature, which means that this spectrum is unavailable for use, even if those who own the rights to that spectrum do not use it. This has led to considerable inefficiency in spectrum utilization, and has created an unnecessary shortage of spectrum. This issue has been temporarily alleviated by providing for the availability of spectrum for unlicensed usage, and has fueled the global deployment of 802.11-based technology. However, these unlicensed frequency bands are becoming over-populated and interference has grown to be a significant deployment constraint. All of these factors have led to the need to make dramatic changes in the spectrum regulatory process, as existing practices and policies are not capable of scaling with demand. This, in part, has led to the concept of Cognitive Radio (CR).

This paper provides a brief overview of cognitive radio and the draft IEEE 802.22 specification. This paper then goes on to discuss some of the key security functionality that is important to consider in the design of a strong security model for a cognitive radio network, identifying potential vulnerabilities along with a high-level security model that could lead to potential mitigation approaches.

II. An Overview of Cognitive Radio

CR is in itself an overloaded term with many potential meanings. The FCC defines CR as "A radio system whose parameters are based on information in the environment external to the radio system." (Reference 2) The National Telecommunications and Information Agency (NTIA) has proposed to define CR as "A radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operations, such as maximize throughput, mitigate interference, facilitate interoperability, and access

secondary markets." The term itself, 'Cognitive Radio', was coined by Mitola in [1]. Some of the key features that are typically associated with CR include [2]:

- ***Maintains awareness*** of surrounding environment and internal state
- ***Adapts*** to its environment to meet requirements and goals
- ***Reasons*** on observations to adjust adaptation goals
- ***Learns*** from previous experiences to recognize conditions and enable faster reaction times
- ***Anticipates*** events in support of future decisions
- ***Collaborates*** with other devices to make decisions based on collective observations and knowledge.

However, the community remains quite divided on how many of these features a radio must possess before it is considered a CR. Furthermore, the community is divided on the scope of these features. Many believe that the scope is limited to the lower radio layers of the protocol stack. Others envision CR as a device that can exhibit these characteristics across the entire protocol stack, such as the vision put forth in [3]. It is also important to note that an adaptive radio is not a CR. Indeed, adaptation is a subset of CR characteristics, and an adaptive radio is not necessarily cognitive at all. There are many existing examples of adaptive radios and techniques that do not exhibit characteristics such as learning and reasoning [4]. Rather, these devices simply adapt based on some pre-defined algorithm or rule-set.

There are currently multiple development and standardization activities relevant to CR. One of which is the DARPA neXt Generation (XG) project, which aims to develop (likely proprietary) technology to utilize unused spectrum in an opportunistic fashion, primarily for the United States military. More information on the DARPA XG program can be found in [5] and [6]. The IEEE 802.11k project aims at developing extensions to existing 802.11 WLAN technology to enable radio resource measurements. These extensions will specify the types of radio resource information that will be made available to developers along with the interface mechanisms for accessing this information [7]. The first large-scale standardized CR technology will be IEEE 802.22, which is the primary commercial activity in this area. The IEEE 802.22 working group aims to develop technology to utilize unused television spectrum for broadband wireless services [8][9]. It should be mentioned that both XG [10] and IEEE 802.22 efforts are focused on the lower layers of the protocol stack, and that both of these efforts focus on frequency agility for interference mitigation purposes. As such, at least a portion of the community would consider neither of these efforts truly "cognitive" in nature. However, CR is often associated with frequency agility, whether this association is correct or not in the true academic sense.

IEEE 802.22 [9]will specify the air interface of fixed point-to-multipoint wireless regional area networks (WRANs) operating in the Very High Frequency (VHF) and Ultra High Frequency (UHF) television (TV) broadcast bands from 54 MHz to 862 MHz. These frequency bands are statically allocated by regulatory agencies, such as the Federal Communications Commission (FCC) for use by TV broadcast services. However, this spectrum is unused in many regions, leading to 'white space' in spectrum, and inefficiency in spectrum utilization. This is particularly the case in rural regions, where spectrum is assigned to a regional TV broadcast service, but whose transmissions do not reach that far beyond its urban transmission base. Furthermore, TV broadcasters often win allocation of spectrum across numerous market regions, but only actually broadcast in a portion of those regions, leaving unused spectrum even in urban regions. The primary goal of IEEE 802.22 is to take advantage of the untapped market for broadband wireless access in rural and other un-served/underserved areas where wired infrastructure cannot be economically deployed by taking advantage of this unused spectrum.

The fundamental tenant of IEEE 802.22 is *protection of incumbents*. That is, the primary charge of IEEE 802.22 is to make use of unlicensed TV spectrum on a *non-interference basis*. The primary incumbents within the scope of IEEE 802.22 are: 1) Broadcast TV and 2) FCC Rules Part 74 Sub-part H low power Auxiliary stations (i.e. wireless microphones). As such, a key requirement for IEEE 802.22 is to develop mechanisms to provide incumbent awareness and avoidance. This is provided by numerous mechanisms in the IEEE 802.22 specification: 1) distributed spectrum sensing, 2) quiet period and fast/fine sensing management, 3) measurements and clustering, 4) detection algorithms, and 5) spectrum management. For the case of TV incumbents, collective knowledge of channel sensing, CPE locations, and TV operation database information is used to determine the existence of an interference issue. This TV operation database is populated with, among other information, locations of TV transmitters and protected contour locations. For these incumbents, the known locations of these transmitters provide a significant advantage for 802.22. Low power devices operating in the TV band present a much greater challenge. The location of these devices (which includes wireless video assist systems and wireless microphones) are generally not known a priori as this is equipment associated with television field crews, and as such typically 'follow the news.' These incumbents can appear anywhere, potentially in large numbers, and the 802.22 WRAN must always accommodate these devices on a non-interference basis. The envisioned method is to employ a special class (class B) CPE that would be collocated with Class 74 emitters. This special CPE would emit a beacon that can be used by the 802.22 WRAN to detect the presence of the Class 74 device. If a beacon is not detected after some period of time, the channel is assumed to be unoccupied and available for use by the WRAN. If beacons are detected, that channel is avoided. If a Class 74 device is activated during WRAN usage, the WRAN will detect the beacon and begin a channel change operation. Additionally,

the presence of this incumbent can be signaled to the rest of the WRAN through the Urgent Coexistence Situation (UCS) field in the MAC header.

III. Cognitive Radio – The Required Evolution of Wireless Security

In general, the area of security in cognitive radio networks has received far less attention than other areas of cognitive radio (e.g. spectrum sensing methods), with very little existing literature on this topic. In general, it is expected that 802.22 will leverage the 802.16e security model and mechanisms. In fact, the current working draft 802.22 specification states "The security sublayer is in many respects inspired by the IEEE 802.16e/D12 draft." [8] This makes sense in many respects, since the 802.16 security model has evolved significantly since its original inception, and is generally considered to provide reasonably strong security. With that said, 802.16e access technologies do not consider the unique aspects of a cognitive radio network. These concepts require security mechanisms whose scope extends beyond what is provided in 802.16e. In the case of 802.22, this traditional approach might make sense, since 802.22 may or may not eventually embrace or reflect the entirety of what it means to be cognitive (as defined in [2]). Furthermore, it is not envisioned that XG will fully embrace all these cognitive radio tenets. However, these traditional approaches are insufficient for the generalized cognitive radio network. Following a conventional (e.g. 802.16e or 802.11i/802.11w) approach to wireless network security will ultimately provide reasonably good security to the network against numerous types of attack. However, the CR nature of the system introduces an entire new suite of threats and tactics that are not easily mitigated. Denial of Service (DoS) attacks will be very challenging to prevent in the cognitive radio network. There are also new unique opportunities presented to the malicious attacker, leading to potentially devastatingly effective spoofing and integrity attacks that can influence both spatial (i.e. an attack causing effects in an increasingly large geographic area) and temporal (i.e. an attack causing effects that are long-lasting over time) behavior of the network. At this point in the still immature point of cognitive radio networks, and understanding how to provide security services in a cognitive radio network, it is important to step back and first understand the key fundamental issues:

1) What are the potential threats to a cognitive radio network?
2) What are the potential attacks against a cognitive radio network?
3) What is the likelihood of these threats and attacks?
4) What is the potential consequence of these attacks?

There is the obvious desire to provide basic network security services in a cognitive radio network, such as confidentiality, privacy, and authentication, as there is in any wireless network. However, this is where the commonality ends between the cognitive and non-cognitive network.

Certainly, threats to non-cognitive wireless networks in general are still of interest in the cognitive network. The following threats are of specific interest:

- The outside threat (i.e. unauthorized user) attempting to inject energy into the victim network to achieve a desired goal
- The Byzantine threat.(i.e. insider threat) attempting to use its privilege to achieve a desired goal

The outside threat could consist of an attacker attempting to inject energy into the cognitive radio network to induce some type of behavior. A jammer is a traditional type of this outside threat. Furthermore, the outside threat could be attempting to inject otherwise valid messages into the network for a desired effect (i.e. spoofing). The Byzantine threat is another serious threat, particular in wireless networks, due to the distributed and often unseen peers of the network.

However, in order to understand the true impact of the CR paradigm on wireless network security, let us revisit the key features of the CR with us now also considering these features from the perspective of a malicious attacker, and the implications of these features on the types of attacks that might be conducted, as summarized in Table I.

There are two fundamental differences between a traditional wireless network and the CR network:

1) The potential far reach and long-lasting nature of an attack
2) The ability to have a profound effect on network performance and behavior through simple spectral manipulation (i.e. generation of signals).

In the CR network, locally-collected and exchanged information is used to construct a perceived environment that will impact both current and future behaviors, as well as the behavior of those around them. At this point, spoofing the radio is more analogous to manipulating a group of people, a feat which history has unfortunately proved to be all too easy a task. The induction of an incorrectly perceived environment will cause the CR to adapt incorrectly, which affects short-term behavior. Unfortunately, the CR uses these experiences to reason fundamentally new behaviors, learning from these experiences to anticipate future actions. Thus, if the maliciousattack perpetrator is clever enough to disguise their actions from detection, they have the opportunity for long-term impact on behavior. Furthermore, the CR collaborates with its fellow radios to determine behavior. Consequently, this provides an opportunity to propagate a behavior through the network in much the same way that a malicious worm propagates through a network. It is also important to note that this is achieved through relatively simple spectral

TABLE I THE FEATURES OF A CR FROM THE PERSPECTIVE OF AN ATTACKER

CR Feature	What this Means to the CR	What this Means to the Attacker	Potential Attack / Malicious Tactic	Potential Goal / Desired Effect	Implication for Attacker and Attacker Capability
Maintains awareness	CR is performing functions such as spectrum sensing (what spectrum is being used, who/what is using it)	Opportunity for spoofing	Create a signal environment to cause erroneously perceived environment by cognitive network member(s)	Cause CR to sense an environment defined and controlled by malicious attacker	Must know what victim is sensing, and have the capability to create the desired signal environment (occupy spectrum and pretend to be certain device/signal types
Adapts	CR adapts its behavior based on perceived environment	Opportunity to force desired changes in behavior in victim	N/A – Attack influences this through awareness spoofing	Cause radio to adapt in a way controllable by malicious attacker	Must have insight into methods/algorithms and objectives/goals that govern CR adaptation
Reasons	CR adapts its adaptation methods based on awareness to accommodate changing goals	Opportunity to influence fundamental behavior of CR	N/A – Attack influences this through awareness spoofing	Introduce biases into CR decision-making process by shaping goals in a way advantageous to attacker	Need to fine-tune attack strategy for desired behaviors. Need insight into reasoning algorithms. Need insight into changing goals.
Learns	CR adapts its adaptation methods based on awareness to improve adaptation methods	Opportunity to affect long-lasting impact on CR behavior	N/A – Attack influences this through awareness spoofing	Introduce biases into CR decision-making process by introducing biases into CR adaptation rules/algorithms	Need to observe long-term effect to adapt attack as necessary. Need insight into learning algorithms. Need ability for long-term awareness spoofing
Anticipates	CR uses awareness to predict future environment to proactively adapt/reason/learn	Opportunity for long-lasting impact	N/A – Attack influences this through awareness spoofing	Control/influence future actions of CR by sustained awareness spoofing	Need to observe long-term effect to adapt attack as necessary. Need ability for long-term awareness spoofing
Collaborates	CRs share information and use that information in adaptation/reasoning/learning/anticipation process	Opportunity to propagate attack through network	N/A – Attack influences this through awareness spoofing. Collaborative attack could influence from multiple network points	Control/influence actions and future actions of CR(s) outside the physical reach of attacker	Can observe neighboring nodes to assess effectiveness

manipulation. That is, the malicious attacker can generate signals to influence the perceived environment by the CR(s). This spectral manipulation could be aimed at influencing the behavior of a set of local CRs (i.e. those physically reachable), or may be targeted at influencing distant CR(s). This spectral manipulation may be aimed at influencing near-term behavior, or may be aimed at causing a desired behavior in the far-term, conditioning the CR network for a future malicious action.

To illustrate the complications that are introduced by the CR paradigm, consider the classical DoS jamming attack. Virtually any wireless system is vulnerable to brute force DoS approaches, such as jamming. However, without protective mechanisms in place, CR technologies such as 802.22 could be trivially easy to jam with only limited sophistication. In the 802.22 paradigm, the network is acting in a frequency-agile manner based on spectrum observations and the determination of the presence of incumbent interferers. The system must yield to incumbent interferers, and must find a new operating spectrum in the presence of those interferers. In the case of Class 74 devices, this case is somewhat easier because the system relies on specialized 802.22 equipment to signal the presence of Class 74 devices to the WRAN; authentication mechanisms can be employed to ensure the authenticity of these beacons. This places the emphasis on physical security of these Class 74 device beacons in the overall security architecture. The problem is worse for TV broadcasts. There is currently no mechanism described to determine the authenticity of incumbent TV broadcast signals. Here, 802.22 will likely relying (at least in part) on the pre-known nature of television transmitter locations so that interference determining thresholds can be set according to valid signals. However, there is no mechanism to know that the signal that is observed is an authentic TV signal. As such, a jammer could generate a signal that resembles a TV signal and then broadcast that into the 802.22 WRAN. The jammer can then adjust its signal level until it observes an adaptation by the WRAN. This immediately gives the jammer knowledge of the required signal power to induce an adaptation, and it can then begin 'chasing' the signal targets across spectrum, causing

continual adaptation and outage of service. This could present an opportunity for a jammer to disrupt service at power levels far less than otherwise required, increasing the ease of operation and/or reach of the jammer. This is illustrated in Fig. 1.

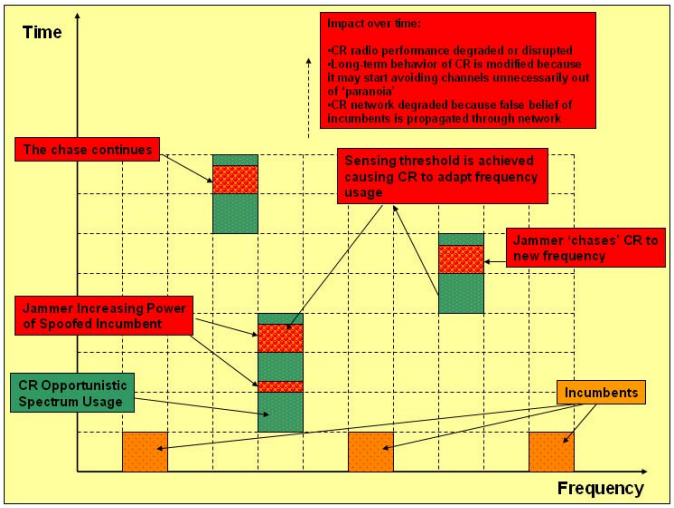

Figure 1. An Illustration of the 'Incumbent-Spoofing Chaser Jammer' Threat to a Cognitive Radio Network

IV. Envisioned Security Features of a Secure Cognitive Radio Network

To mitigate malicious manipulation of CRs and CR networks into forced behaviors, a CR must possess four key characteristics:

1) The ability to authenticate the local observations that are used to form perceived environments
2) The ability to strongly secure collaboration exchanges between CR elements
3) The ability to authenticate the validity of observations exchanged between CR elements
4) The ability to perform self analysis of behavior

All of these security features relate to the need for the CR to ***exhibit good judgment***. At this point, it is important to recognize that the CR paradigm imposes human characteristics onto the radio device. As such, it may be beneficial for the designers of CR network security models to examine (at least in part) social and science and human behavior, and consider the characteristics that protect humans from manipulation, primarily relationships, judgment, and wisdom. This is a daunting task, as humanity has not yet mastered these capabilities themselves. However, it is valuable to consider the human behavioral model in order to isolate protection characteristics that may perhaps be leveraged when beginning to develop a CR security model.

As the first line of defense of the network, the CR needs to be capable of judging whether what it is locally sensing is real or falsified. This goes far beyond protecting the network from injection of false messages, as is the focus of traditional network authentication mechanisms. Rather, this means that not only network messages are authenticated, but also that observations of physical phenomena are also authenticated. These physical phenomena can take the form of physical attributes of the environment that do not lend themselves to traditional authentication mechanisms. Humans are provided this first line of defense in three primary forms: 1) sensory input (what is seen, heard, etc.), 2) cross-referencing sensory input with context of situation (does what I sense make sense within the context of my situation?) 3) the intangible 'gut instinct' (what I sense is consistent with the context of my situation, but something doesn't feel right). Basic human senses (sight, smell, etc.) are analogous to algorithms processing data from input devices, and are certainly implementable within a CR. Furthermore, a CR can be made aware of the context of its usage (i.e. where am I located and what would I expect to sense given this location?). However, the intangible 'gut instinct,' which is often critical to effective human decision-making, will prove much more difficult to integrate in a manner that lends itself to stable behavior.

Since a CR is utilizing not only its own observations as a basis for decision making but also the observations of others, there is the obvious need to authenticate the shared observations. This is particularly true given the distributed and unseen nature of its peer CRs. The CR needs assurances that messages are indeed from who they claim they are from. This is similar in nature to authentication of traffic in any wireless network, and as such is not necessarily unique to the CR paradigm. It is here that lessons can be drawn from the field of secure exchanges of routing information in ad-hoc wireless networks, an area that continues to receive significant research activity (e.g. [11]).

Once the authenticity of the source of collaborative CR network messages has been established, the CR needs to be the judge of whether the observations that other CR elements within the CR network are reporting are real or falsified. This combined with the ability to establish the authenticity of the source is critical to preventing the propagation of attacker effects within the CR network. This is critical for two reasons: 1) to prevent degradation of the network because of a spoofed CR element within the network and 2) to protect against the Byzantine attack. Human behavior provides protection mechanisms against this type of deceit in two forms: 1) a trust model, and 2) a respect model. How much do we trust the person that is communicating information with us? This trust is typically built over time through experience. There is no 'best' equation as to what this trust vs. time model looks like, and often effective human decision making can span a wide variety of these models. But what is consistent in effective collaborative human decision making is the model of 1) friends 2) acquaintances, and 3) adversaries. This is consistent with human concepts of society and community, and it is likely beneficial to think of a CR network as a virtual community.

Friends are elements for which a strong positive trust relationship has been built over time through a deeper level of understanding and familiarity. As such, that understanding can be used to put the conveyed information into a context that can be judged against. The tendency is to trust a friend. Acquaintances are known, but not as well as friends. Here, the tendency tends to remain neutral and not form any type of preconceived notion of trust. Adversaries are the converse of a friend. Here, a deeper level of understanding has been built from which the tendency is to distrust what is being communicated. Humans achieve this type of understanding over time through gained information, where this information is gained through both direct and indirect communications (i.e. gossip). All of these relationships and the tendency to trust or distrust information are related (at least loosely) to the societal structure and the stated/perceived goals of individuals and individual actions (e.g. custom-based, emotion-based, value-based, etc.). In the CR paradigm, this type of communication represents overhead which is undesirable. So, the goal then is to establish a trust relationship while minimizing the required knowledge to establish the type of peer relationship to be formed with other elements of the CR network. From a security perspective, it is desirable for a malicious attacker to have as little information as possible to the social values, customs, and motivations of the members of the CR virtual society. In practical terms, this traces to the need of a malicious attacker to have insight into the goals, methods, and techniques to achieve many of the desired goals (Table I).

The Byzantine attack represents the case where a friend or acquaintance has, unbeknownst to the CR, become an adversary and represents the most difficult subset of this problem space. There are indeed lessons that can be drawn from existing work in the area of Byzantine routing (e.g. [12]). However, we must be careful not to create an overly-paranoid network where nodes are quickly distrusted if behavior of friends or acquaintances becomes inconsistent with expectations. This is because this paranoia itself could be used against the CR by an attacker to cause a forced effect. In the case of a CR employing a friend-acquaintance-adversary model, a friend node is likely easier to identify as a Byzantine threat than an acquaintance.

The CR needs to be the judge as to whether it is acting erratically or logically. This self-check is critical to the long-term health of the CR network. If the long-term behavior of the CR has been affected by an attacker, the CR must be capable of identifying itself as an injected node and take self-corrective measures. Humans are typically quite poor at this type of self-diagnostic in an isolated manner. Rather, humans rely on communications from friends ('Is everything OK?') for initial identification of an issue. And even following initial identification, humans often struggle to correct undesired behavior without intervention from friends or paid professionals (e.g. therapists). As such, the friend-acquaintance-adversary model could work well in the CR paradigm, with every node charged to help care for not only itself but for other nodes within the CR network. Additionally, the CR could follow the human model even further and have a subset of CR nodes identified as network diagnostic nodes (i.e. therapists) that are charged with analyzing behavior of CR network nodes and assessing the presence of erratic behavior and then assist in the resolution of these issues.

Revisiting the 802.22 context, for the cognitive system to be effective against an adaptive threat such as the 'chaser jammer' depicted in Figure 1, a method is required that can authenticate valid TV transmitters based solely on RF characteristics. Tomko et al. has shown in [13] that physical layer features extracted from the RF waveform can be used to finger each packet source in the network, providing a mechanism for identifying rogue node activity. While this previous work was performed for an IEEE 802.11b network, it is interesting to consider the possibility of the extension of such work to broadcast TV signals as a possible way forward in mitigating these types of DoS attacks.

V. A Multi-Dicipline Problem

An important observation to make is that cognitive radio network security crosses many technical disciplines, all which must be brought to bear on the problem space to fully understand the issues surrounding security in a cognitive radio network, much less develop effective solutions. The issues of positive peer identification and insider attack can at least in part be approached, or at least partially understood, through traditional approaches [11] and existing research areas [12]. The issues of determining the authenticity of the locally-observed environment can perhaps leverage the work in the area of physical emitter classification and identification (e.g. [13]).

Once the CR has locally-collected observations and observations reported from peers within the CR network, the responsibility is placed on the CR to make a determination on its action (adapt) and how it is going to use this information to maintain its current goals (reason) and optimize its adaptation algorithms (learn). This fundamental problem of attempting to form an optimal decision regarding present and future behaviors has a rich research base that can be drawn upon. There are several fundamental approaches to this optimization problem, all of which stemming from the artificial intelligence research, including machine learning, biologically-inspired (genetic) algorithms, and game theoretical approaches. Barreno et al. [14] provides a very good treatment of the current state of security issues surrounding machine learning algorithms. From these research communities there is significant work that can be leveraged to begin developing security solutions for CR networks. For example, researchers have considered the issue of optimally combining advice from a set of experts (e.g. [15]), analogous to CRs sharing their expert advice regarding their environment, and several solutions have been proposed that attempts to optimally combine those expert opinions in a way that is most beneficial (e.g. [15]). Contributions can also be found in the data mining

research community, where work has also been done in the area of attempting to make an optimal decision when an adversary is attempting to corrupt the process with false information (e.g. [16]). Here, the adversary is attempting to influence the learning-adaptation cycle, and [8] shows that if the adversary and learner has complete information about each other, than the learner can find a strategy to defeat the adversary's attempted adaptations. This gets back to the point made in Table 1 that an adversary must have information regarding the CR's goals, methods, and techniques for adaptation, learning, and reasoning to be effective. Furthermore, this suggests that it is highly beneficial to precisely understand the threat and the types of tactics that would be employed by the threat.

Lastly, this paper contends that since the CR paradigm is imposing human-like characteristics into the radio network, it may be beneficial to consider and look into the fields of social science and human behavior and psychology, to examine the the mechanisms employed in the human network security model and determine if these can be applied to CR networks. However, this notion of human behavior-based security and trust models appears to be receiving little attention in open literature. This is understandable, given the enormous task at hand in making learning algorithms robust to deception. However, CR security models must eventually move beyond 'securing the individual' (i.e. secure decision-making), and begin to consider 'securing the society.' (i.e. secure collaborative decision-making).

VI. Conclusions

The cognitive radio paradigm introduces entirely new types of security threats to wireless networks and makes the development of effective security models and mechanisms very challenging. However, wireless security in cognitive radio networks is a technical area that has received relatively little attention to date, even though security will likely play a key role in the long-term commercial viability of the technology. This paper has delineated some of the key challenges in providing security in cognitive networks, loosely tying this to the current security posture of the emerging IEEE 802.22 cognitive radio standard, and identifying potential threats and vulnerabilities to a CR network along with concepts that could potentially lead to mitigation approaches.

This paper has attempted to illustrate the multi-discipline nature of developing cognitive radio security models, and has attempted to draw analogies and comparisons to applicable research communities. This paper has attempted to show that the traits of a CR (awareness, adaptation, etc.) are human traits that we as designers are attempting to impose on machines. As a result, we also have to impose good judgment in order for the CR network to behave responsibly and predictably. History has shown good judgment is still a trait that humans have only arguably achieved (and only intermittently). So, certainly imparting this ability into a radio is a formidable task. There exists promising preliminary approaches and active research to securing the decision-making process that will be fundamental to a CR. There exists promising research in the area of authenticating spectral observations. There exists promising research in the area of secure collaboration exchanges within the network. One potential method to improve the security posture of a CR network is to protect and secure the goals, methods, and algorithms used by the CR in its decision-making process. Another method to improve the security posture of a CR network is to understand the threat and the threat's potential tactics as well as possible. Regardless of the actual approaches and techniques employed, it is important to realize the key differences in developing secure CR networks, and that it requires a change in mindset and an evolution in how the problem of wireless network security is approached.

References

[1] J. Mitola, III. and G.Q. MaGuire, Jr., "Cognitive Radio: Making Software Radios more Personal," IEEE Personal Communications, Vol. 6, Issue 4, pp. 13-18, August 1999.

[2] "IEEE 802 Tutorial: Cognitive Radio", Scott Seidel, Raytheon, Presented at the IEEE 802 Plenary, 18 July 2005.

[3] J.L. Burbank, Ross E. Conklin, Jr., William T. Kasch, and Robert A. Nichols, "Cross-Layer Interactions: A Framework for Adaptable Communications," Proceedings of the 14th Virginia Tech/MPRG Wireless Personal Communications Symposium, 9-11 June 2004.

[4] Andrea J. Goldsmith and Stephen B. Wicker, "Design Challenges for Energy-Constrained Ad Hoc Wireless Networks," IEEE Wireless Communications Magazine, August 2002.

[5] The XG Vision, Request for Comments, Version 2.0, XG Working Group, http://www.darpa.mil/ato/programs/XG/rfcs.htm

[6] The XG Architectural Framework, Request for Comments, Version 2.0, XG Working Group, http://www.darpa.mil/ato/programs/XG/rfcs.htm

[7] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment: Radio Resource Measurement, " IEEE P802.11k/D7.0, January 2007.

[8] current working draft of 802.22 ???

[9] Carlos Cordeiro, et al., "IEEE 802.22: The First Worldwide Wireless Standard based on Cognitive Radios," 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 8-11 November 2005, pp. 328-337.

[10] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks : A survey," Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 50, Issue 13, September 2006, pp. 2127-2159.

[11] Manel Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," ACM Workshop on Wireless Security (WiSe), September 28, 2002.

[12] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, and Herbert Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," ACM Workshop on Wireless Security (WiSe), September 28, 2002.

[13] A.A. Tomko, C.J. Rieser, and L.H. Buell, "Physical-Layer Intrusion Detection in Wireless Networks," Proceedings of the 2006 IEEE Military Communications (MILCOM) Conference, October 2006, pp. 1-7.

[14] Marco Barreno, et al., "Can Machine Learning Be Secure?" Proceedings of the ACM Symposium on Information, Computer, and Communication Security, March 2006.

[15] N. Cesa-Bianchi, et al., "How to use Expert Advice,". Journal of the ACM," May 1997.

[16] V. Vovk. "Aggregating strategies," Proceedings of the 7th Annual Workshop on Computational Learning Theory, San Mateo, CA, 1990, pp. 371–383.

[17] N. Dalvi, et al., "Adversarial classification," Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2004, pp. 99–108.