Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks

Ruiliang Chen, Jung-Min Park, Y. Thomas Hou, and Jeffrey H. Reed, Virginia Polytechnic Institute and State University

ABSTRACT

Cognitive radio is a revolutionary technology that promises to alleviate the spectrum shortage problem and to bring about remarkable improvement in spectrum utilization. Spectrum sensing is one of the essential mechanisms of CR and is an active area of research. Although the operational aspects of spectrum sensing are being studied actively, its security aspects have attracted very little attention. In this paper, we discuss security issues that may pose a serious threat to spectrum sensing. Specifically, we focus on two security threats — *incumbent emulation* and *spectrum sensing data falsification* — that may wreak havoc in distributed spectrum sensing. We also discuss methods for countering these threats and the technical hurdles that must be overcome to implement such countermeasures.

INTRODUCTION

The success of wireless applications operating in unlicensed frequency bands has resulted in the overcrowding of these bands. Unfortunately, most of the usable electromagnetic spectrum already has been allocated for licensed use, resulting in a shortage of spectrum for new and emerging wireless applications. To alleviate this problem, regulators and policy makers are working on new spectrum management strategies. Specifically, the U.S. Federal Communications Commission (FCC) is tackling the problem in three ways: spectrum reallocation, spectrum leases, and spectrum sharing [1]. In spectrum reallocation, bandwidth from government and other long-standing users is reassigned to new wireless services such as mobile communications. In spectrum leases, the FCC relaxes the technical and commercial limitations on existing spectrum licenses by permitting existing licensees to use their spectrum flexibly for various services or even lease their spectrum to third parties. In spectrum sharing, the FCC allocates spectrum for unlicensed or shared services. Whereas spectrum reallocation and spectrum leases focus on improving the efficiency of spectrum usage from the perspective of licensed spectrum management, spectrum sharing aims to better regulate unlicensed spectrum usage. Spectrum sharing, in particular, has attracted great interest from regulators, manufacturers, and researchers. The FCC is considering a new spectrum sharing paradigm, where licensed bands are opened to unlicensed operations on a *non-interference* basis to licensed operations. Because some licensed bands (such as TV bands) are underutilized, spectrum sharing in fallow sections of these licensed bands can effectively alleviate the spectrum scarcity problem. In this spectrum sharing paradigm — which is often referred to as dynamic spectrum access (DSA) — licensed users are referred to as primary users or incumbents, whereas unlicensed users that access spectrum opportunistically are referred to as secondary users or secondaries.

The technology of cognitive radio (CR) plays an important role in realizing the DSA paradigm. To achieve the highly flexible operating characteristics required for DSA, software-defined radios (SDRs) will be employed in CR instead of hardware-based application-specific integrated-circuit (ASIC) devices as in conventional radios. In addition, a CR can learn from its environment and intelligently adjust its operating parameters based on what was learned. In DSA, CRs used by secondaries must be able to scan a certain spectrum range and intelligently decide which spectrum band to use for its transmission. This process is called *spectrum sensing*. During spectrum sensing, if a secondary detects that it is within an incumbent's protection region[1] of a particular band, it refrains from accessing that band and searches for a fallow band that is accessible. If no incumbents are detected, the secondary coordinates with other secondaries to share the spectrum not utilized by incumbents.

Depending on the deployment scenario, the secondaries can employ either a cellular network architecture or an ad hoc network architecture. A cellular CR network architecture is employed in the IEEE 802.22 standard that specifies the air interface (physical [PHY] and medium access control [MAC] layers) for a CR-based wireless regional area network (WRAN) [2, 3]. A WRAN

This article was presented in part in the First IEEE Workshop on Networking Technologies for Software Defined Radio (SDR) Networks, Sept. 2006, Reston, VA.

This work was supported in part by the National Science Foundation under grants CNS-0627436, CNS-0716208, and CNS071570.

[1] An incumbent's protection region is defined as the area in which secondaries cannot operate while the incumbent is in operation (i.e., transmitting) so that no interference to the incumbent is introduced.

0163-6804/08/$25.00 © 2008 IEEE

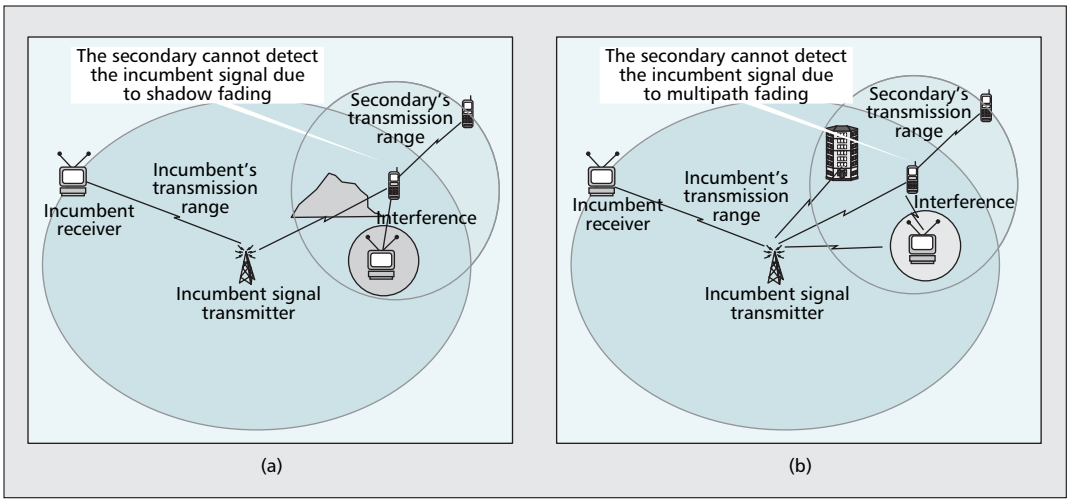

Figure 1. *The hidden node problem caused by a) shadow fading; b) multipath fading.*

cell is composed of a base station (BS) and a number of consumer premise equipments (CPEs), and the coverage of a WRAN cell can range from tens of kilometers to a hundred kilometers. In contrast, an ad hoc CR network is comprised of low-energy mobile computing devices equipped with CRs, and they interact with each other via multihop wireless links. The establishment of each wireless link is via DSA. Although these two types of CR networks have different network architectures, spectrum sensing is an essential component of both, and it represents one of the key technological hurdles that must be overcome before the widespread deployment of CR networks is possible.

Distributed Spectrum Sensing

Performing reliable spectrum sensing is a challenging task for a CR. In a wireless channel, signal fading can cause the received signal strength to be significantly lower than what is predicted by path loss models. There are two types of fading: shadow fading and multipath fading. Shadow fading (also known as slow fading) is frequency independent, and it does not cause significant fluctuations in signal strength over small changes in receiver location, whereas multipath fading (also known as fast fading) is frequency dependent and can vary significantly with small changes in location. The effect of fading — shadow fading, in particular — can result in the *hidden node problem*. The hidden node problem in the context of CR networks can be described as an instance in which a secondary in a CR network is within the protection region of an operating incumbent but fails to detect the existence of the incumbent.[2] Figure 1 shows two scenarios in which the hidden node problem may occur.

Recent research results [4] indicate that the hidden node problem can be alleviated by requiring multiple secondaries to cooperate with each other in spectrum sensing, that is, in distributed spectrum sensing (DSS). An illustration of DSS is shown in the upper half of Fig. 2. In DSS, each secondary acts as a sensing terminal that conducts local spectrum sensing. The local results are gathered at a data collector (or *fusion center*) that executes data fusion and determines the final spectrum sensing result. In an 802.22 WRAN, DSS can be implemented in a straightforward manner: the BS acts as the data collector, and the CPEs serve as sensing terminals. In an ad hoc CR network, where each node is a secondary equipped with a CR, each node acts as both a sensing terminal and a fusion center. A node sends its local sensing measurements to its neighbors and executes data fusion using the measurements received from its neighbors. One advantage of DSS over non-cooperative spectrum sensing by an individual terminal is its ability to reduce the variance of the spectrum sensing process. Furthermore, to overcome the hidden node problem with a single CR, the CR must have sufficiently high sensitivity to detect even extremely weak incumbent signals. The high cost of such highly sensitive CR terminals may limit the wide deployment of CR networks. With DSS, reliable incumbent signal detection with low-cost, low sensitivity CR terminals is possible. However, DSS has its share of drawbacks: DSS incurs communication overhead when exchanging spectrum sensing data, and requires reliable communications links between the sensing terminals and the data collector.

Although spectrum sensing is an active area of research, relevant security issues have yet to be studied. The security aspects of spectrum sensing must be addressed before the benefits of CR technology can be fully reaped. In the rest of this article, we describe two security threats to DSS in CR networks: *incumbent emulation* and *spectrum sensing data falsification*. After analyzing the attacks, we also discuss potential countermeasures.

Incumbent Emulation Attacks

When an incumbent is detected in a given band, all secondaries avoid accessing that band. However, when a secondary is detected, other secondaries may choose to share that same band. In other words, incumbents have higher priority than secondaries in accessing spectrum resources. In an incumbent emulation (IE) attack, a malicious secondary tries to gain priority over other secondaries by transmitting signals

[2] Note that the hidden node problem discussed here is different from the "hidden incumbent problem" in 802.22 networks. The hidden incumbent problem refers to a situation in which a CPE is within the protection region of an operating incumbent but fails to report the existence of the incumbent to its BS. Suppose that the BS started service in a certain band unaware of the fact that an incumbent is using the same band. In such a scenario, some CPEs within the incumbent's transmission range may not be able to decode the BS signal because of the strong interference from the incumbent signal. Therefore, these CPEs are unable to report the existence of the incumbent to the BS, and hence the BS fails to detect the presence of the incumbent.

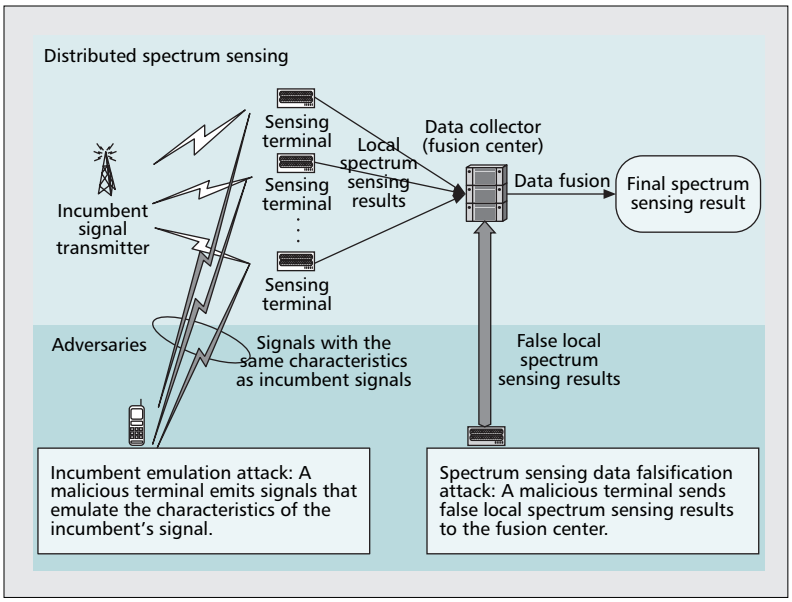

Figure 2. *Security threats in distributed spectrum sensing.*

that emulate the characteristics of an incumbent. An illustration of an IE attack is shown in the lower left corner of Fig. 2. Due to the programmability of CRs, it is possible for an adversary to modify the radio software of a CR to change its emission characteristics (e.g., modulation, frequency, power, etc.) so that the emission characteristics resemble those of an incumbent. The potential impact of an IE attack depends on the legitimate secondaries' abilities to distinguish the attacker's signal from actual incumbent signals while conducting spectrum sensing. Here we examine two existing spectrum sensing techniques and explain why they may be vulnerable to IE attacks.

Energy detection is one of the simplest methods for spectrum sensing. An energy detector infers the existence of an incumbent based on the measured signal energy level. Obviously, energy detection cannot distinguish incumbent signals and secondary signals. An improved scheme proposed in [2] suggests the use of periodic *quiet periods*. To facilitate spectrum sensing during a quiet period, all secondaries refrain from transmitting. When quiet periods are observed by all secondaries, detecting incumbents becomes straightforward — that is, any terminal whose received signal energy level is beyond a given threshold can be considered an incumbent transmitter. However, such a detection strategy breaks down completely when malicious secondaries deliberately transmit during quiet periods.

Signal feature detection is an alternative technique that uses either cyclostationary feature detection or matched filter detection [4] to capture special characteristics of an incumbent signal. However, relying solely on signal feature detection may not be sufficient to reliably distinguish an incumbent's signal from those of an attacker. For example, in a CR network where incumbents are TV systems, an attacker may emit signals that emulate TV signals. Alternatively, the attacker can replay TV signals that were previously recorded. In either case, signal feature detection will falsely identify the attacker's signal as that of an incumbent.

An adversary may have two different motives for launching IE attacks. One motivation is to gain an unfair advantage in accessing spectrum in the spectrum sharing paradigm of DSA. Because secondaries will avoid accessing a band if an incumbent signal is detected in the band, an attacker can preempt and monopolize a fallow band if it manages to fool others into believing that it is an incumbent. We refer to such an attack as a *selfish* IE attack. The second motivation is to suppress legitimate secondaries from accessing spectrum, thereby causing denial of service. We refer to this attack as a malicious IE attack. We carried out simulation experiments to evaluate the disruptive effects of both types of IE attacks. Figure 3 shows the simulation result. We simulated a 2000m × 2000m ad hoc CR network containing 300 secondaries, among which the number of IE attackers varied from 0 to 30. There are 20 incumbent TV channels, each with a bandwidth of 6 MHz and a duty cycle of 0.2. Whereas a selfish IE attacker aimed to preempt at most one TV band for its own use, a malicious attacker launched IE attacks in all spectrum bands that were not used by incumbents to maximize the disruptive effect of the attacks. Our simulation results demonstrate the effectiveness of IE attacks. The figure shows that both types of IE attacks can drastically decrease the available bandwidth opportunities that each legitimate secondary can detect. According to our results, malicious IE attacks are more disruptive in decreasing the amount of available bandwidth.

Defending against IE Attacks

The key to defending against IE attacks is to devise a robust technique for verifying the authenticity of an incumbent signal. One naive approach for verifying incumbent transmitters is simply to embed a signature in an incumbent signal. Another method is to employ an authentication protocol between an incumbent transmitter and a verifier. These approaches, however, are inappropriate because no modification to an incumbent system should be required to accommodate opportunistic spectrum use by secondaries.

A potential solution exists when incumbents are TV systems. In a TV system, TV broadcast towers are incumbent transmitters, where two properties can be used to distinguish incumbent signals from secondary signals. One distinguishing property is the location of the transmitter. Because the location of a TV tower is fixed, if the transmitter can be localized based on its signal, then the location information can be used for verification. However, a secondary located sufficiently close to a TV tower also would pass this location-based verification. Then another distinguishing property, signal power level, should be considered. The coverage range of a TV tower typically varies from several miles to tens of miles, and its transmitter output power is typically hundreds of thousands of watts. In contrast, secondaries are hand-held CR devices that have a maximum transmission output power in a range from a few hundred milliwatts to a few

watts — this corresponds to a transmission range of a few hundred meters. If an attacker is in the vicinity of a TV tower, its signal power level would be significantly lower than that of the TV signal. Therefore, an incumbent signal transmitter can be verified using a combination of the location of the TV transmitter information and the received signal power level. Here the most challenging task is estimating or verifying the location of the origin of a signal. Because the DSA paradigm prescribes that no modification to the incumbent system should be required, the location estimation/verification scheme must be *non-interactive* — that is, the location estimators/verifiers cannot interact with the signal transmitter to estimate or verify its location.

Two techniques are presented in [5] to address the problem. The first technique is called a distance ratio test (DRT), which uses received signal strength (RSS) measurements obtained from a pair of location verifiers (LVs) to verify the location of the transmitter. An LV can be a dedicated network device or a secondary user with enhanced functions to perform location verification. Individual LV nodes form a network and communicate with each other. We assume that their data exchange is secured by a security protocol [5]. Because there is a strong correlation between the length of a wireless link and RSS, the RSS measurements at two LVs correlate with their respective distances to the location of the transmitter. The RSS value also depends on parameters under the control of the transmitter, such as the transmitted power value and the antenna gain. However, when two LVs use identical radio receivers and make synchronized measurements, it can be shown that under a realistic radio propagation model, the ratio between their RSS measurements only depends on the ratio between their respective distances to the location of the transmitter. One can calculate the expected ratio of the respective distances between each LV and the transmitter by using the location information of the two LVs and the assumed position of the incumbent transmitter. This ratio is compared with the ratio derived from RSS measurements taken from each LV. If the expected value and the measured value are sufficiently close (to a predefined degree), the transmitter is considered an incumbent and passes the location verification; otherwise it fails the verification. A major drawback of the DRT technique is that its efficacy is influenced by the radio propagation model, which in turn is affected by various environmental variables. Different propagation environments may require the use of different parameters, and may even require the use of totally different propagation models. To address such issues, significant changes to the aforementioned DRT technique is required.

The second technique is called a distance difference test (DDT). This technique uses the fact that when a signal is transmitted from a single source to two LVs, a relative phase difference can be observed when the signal reaches the two LVs due to their differing distances from the transmitter. For example, when the incumbent network is a TV broadcast network, because TV signals have embedded within them periodic synchronous pulses or symbols, two LVs can readily measure the relative phase difference using the pulses or symbols. The phase difference can be translated into a time difference that in turn can be translated into a distance difference. One can calculate the expected difference of the respective distances between each LV and the transmitter by using the location information of the two LVs and the assumed position of the incumbent transmitter. This expected difference is compared with the measured difference to determine the authenticity of the incumbent signal. If the two values are sufficiently close, the transmitter is considered an incumbent and passes the location verification; otherwise it fails the verification. Although a DDT does not suffer from the drawbacks of a DRT, a DDT requires tight synchronization among the LVs (on the order of hundreds of nanoseconds [5]) that may be expensive to implement.

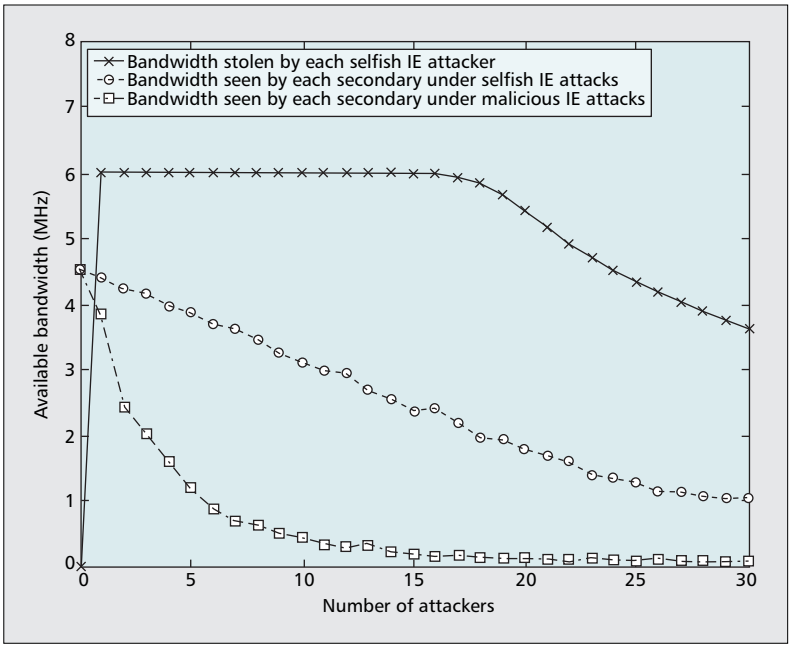

Figure 3. *The disruptive effect of IE attacks.*

The previous discussion has been limited to a scenario where TV systems are incumbents. However, another type of incumbent, Part 74 devices, also are licensed in the TV band. Furthermore, future DSA applications may be extended into other licensed bands such as those used by cellular networks. These incumbents are mobile and have low transmission power. Formulating an effective defense against IE attacks that consider these types of incumbents is a more difficult problem. One possible solution to this problem would be to utilize the concept of radio environment map (REM) [6]. REM is an integrated database that consists of comprehensive multi-domain information for a CR network, including the locations and activities of radio devices. Given that such information is reliable and accessible to LVs (e.g., a REM is installed in an LV), it is possible to verify an incumbent transmitter by comparing its observed location and activities with those stored in the REM. More research is required to make such a solution practical.

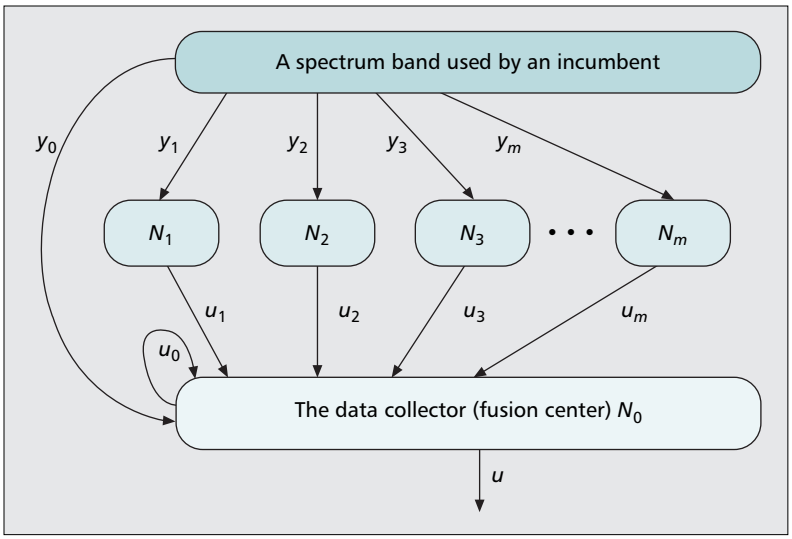

Figure 4. *Modeling DSS as a parallel fusion network.*

Spectrum Sensing Data Falsification Attacks

The second security threat to DSS is the transmission of false spectrum sensing data by malicious secondaries. An attacker may send false local spectrum sensing results to a data collector, causing the data collector to make a wrong spectrum-sensing decision. We use the term spectrum sensing data falsification (SSDF) attack to refer to such an attack. The attack is illustrated in the lower right corner of Fig. 2. To maintain an adequate level of accuracy in the midst of SSDF attacks, the data fusion technique used in DSS must be robust against fraudulent local spectrum-sensing results reported by malicious secondaries. Although a few data fusion techniques for DSS have been proposed recently, none address this problem.

In the following, we describe three data fusion techniques that were proposed recently for DSS. We describe each technique briefly and discuss its vulnerability to SSDF attacks. To facilitate our discussion, we model the DSS process as a parallel fusion network, as shown in Fig. 4. In this figure, N_i ($i = 0, 1, 2, ..., m$, where m is the number of sensing terminals) denotes a sensing terminal associated with N_0, which is both a data collector and a sensing terminal, y represents the incumbent signal received at N_i, and u_i is the local spectrum sensing result that N_i sends to N_0. The output u is the final sensing result, which is a binary variable — a one denotes the presence of an incumbent signal, and a zero denotes its absence. To simplify the discussion, the following description assumes that spectrum sensing is performed in a single band, and each u_i is also binary.

Decision fusion [3] sums all of the collected local spectrum-sensing results. A threshold value that is no less than one and no greater than ($m + 1$) must be specified. If the sum of the u_i's is greater than or equal to the threshold, then the final sensing result is "busy," that is, $u = 1$; otherwise the band is determined to be "free," that is, $u = 0$. Because interference to incumbents should be minimized, usually a conservative strategy is favored, which takes a threshold value of one. In this case, even if a band is free, as long as there is one N_i that erroneously reports $u_i = 1$, the final result will be busy, causing a false alarm. If an SSDF attacker exploits this and always reports one as its local spectrum sensing result, then the final result always will be busy. To prevent such a scenario, one can increase the threshold value. However, increasing the threshold value has the downside of increasing the miss detection probability.[a] Moreover, increasing the threshold is ineffective in decreasing the false alarm probability when there are multiple attackers.

Bayesian detection [2] requires the knowledge of a priori conditional probabilities of u_i's when u is zero or one. It also requires the knowledge of a priori probabilities of u. Four cases must be considered — $u = 0$ when a given band is free; $u = 0$ when the band is busy; $u = 1$ when the band is free; and $u = 1$ when the band is busy. Among the four cases, two decisions are correct, whereas the other two are wrong. The two correct ones are allocated with small costs, and the wrong ones are associated with large costs. The miss detection case is the least desired scenario and therefore is assigned the largest cost. The overall cost is the sum of the four costs weighted by the probabilities of the corresponding cases. Bayesian detection outputs a final spectrum sensing result that minimizes the overall cost. When a network is under SSDF attacks, the values of the a priori conditional probabilities of the u_i's are not trustworthy. As a result, Bayesian detection is no longer optimal in terms of minimizing the overall cost.

The Neyman-Pearson test [7] does not rely on the knowledge of a priori probabilities of u or any cost associated with each decision case. It requires that either a maximum acceptable probability of false alarm or a maximum acceptable probability of miss detection be defined. The Neyman-Pearson test guarantees that the other probability is minimized, whereas the defined probability is acceptable. As with Bayesian detection, the Neyman-Pearson test also requires the knowledge of the a priori conditional probabilities of the u_i's when u is zero or one. For the same reason discussed previously, SSDF attacks would undermine the optimality of the test and potentially cause miss detection or false alarm instances.

The previously mentioned data fusion techniques share two properties in common that contribute to their vulnerability to SSDF attacks. First, these techniques treat all sensing terminals indiscriminatingly, regardless of whether a sensing terminal is reporting true or false sensing data. When an SSDF attacker constantly injects false data, the ideal solution would be to filter the data and only accept inputs from reliable sensing terminals. Second, both techniques cannot guarantee both a bounded false alarm probability and a bounded miss detection probability.

Defending Against SSDF Attacks

To counter SSDF attacks effectively, a two-level defense is required. At the first level, all local spectrum sensing results must be authenticated

[3] *Miss detection refers to the failure of detecting the presence of an incumbent signal.*

by the data collector. The purpose of this security measure is to prevent replay attacks or false data injection committed by entities outside the CR network. The second level of defense is the deployment of a data fusion scheme that is robust against SSDF attacks. As discussed previously, existing data fusion schemes are vulnerable against SSDF attacks. They can be improved in two ways. One way is to employ a sequential probability ratio test (SPRT), which is a data fusion scheme that supports a variable number of local spectrum sensing results [8]. SPRT has the desirable property of guaranteeing both a bounded false alarm probability and a bounded miss detection probability in a non-adversarial environment. Even if each sensing terminal has low spectrum sensing accuracy, SPRT can provide a guarantee by collecting more local spectrum sensing results. This is an advantage over the techniques discussed previously. The other way to increase robustness of the data fusion process is to introduce a reputation-based scheme into the DSS process. The design of such a reputation-based scheme can borrow ideas from the existing body of research on reputation-based secure routing schemes for ad hoc networks. For example, a well-known secure routing scheme proposed in [9] uses a two-module framework — a "watchdog" module for reputation maintenance and a "pathrater" module for applying reputation information to routing. A similar two-module framework can be used for DSS — one for reputation maintenance and the other for applying reputation information to data fusion. In the first module, a reputation rating is allocated to each sensing terminal based on the accuracy of the local sensing report of the sensing terminal relative to the final sensing decision of the data collector. In the second module, the data collector applies the reputation rating to differentiate the "trustworthiness" of the local spectrum sensing report received from each sensing terminal. There are many ways to integrate reputation ratings into an SPRT. For example, one method is to use the reputation rating as an exponent that is added to the probability ratio of a sensing terminal. Such a scheme ensures that a sensing terminal with a reputation rating that is higher than that of other terminals plays a greater role in making the final sensing decision. As a result, the accuracy of the final sensing decision improves.

Summary

In this article, we have identified and discussed two security threats to CR networks: IE attacks and SSDF attacks. Both attacks potentially pose a great threat to CR networks. There are other types of attacks that can disrupt operations in a CR network. For instance, simple jamming attacks may be very effective in interfering with the spectrum sensing process. However, in this article, we have limited our discussion to security issues that are unique to CR networks, with particular focus on security threats to DSS. We also have discussed possible countermeasures against the two previously mentioned attacks.

References

[1] G. Staple and K. Werbach, "The End of Spectrum Scarcity," *IEEE Spectrum*, vol. 41, no. 3, Mar. 2004, pp. 48–52.

[2] L. Lu et al., "Technology Proposal Clarifications for IEEE 802.22 WRAN Systems," IEEE 802.22 WG on WRANs, Mar. 2006.

[3] A. Pandharipande *et al.*, "IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22," IEEE 802.22 WG on WRANs, Nov. 2005.

[4] I. F. Akyildiz *et al.*, "NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey," *Elsevier Comp. Networks J.*, vol. 50, Sept. 2006, pp. 2127–59.

[5] R. Chen and J.-M. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," *Proc. IEEE Wksp. Networking Technologies for Software Defined Radio Networks*, Sept. 2006, pp. 110–19.

[6] Y. Zhao *et al.*, "Overhead Analysis for Radio Environment Map-Enabled Cognitive Radio Networks," *Proc. IEEE Wksp. Networking Technologies for Software Defined Radio Networks*, Sept. 2006, pp. 18–25.

[7] J. Hillenbrand, T. A. Weiss, and F. K. Jondral, "Calculation of Detection and False Alarm Probabilities in Spectrum Pooling Systems," *IEEE Commun. Lett.*, vol. 9, no. 4, Apr. 2005, pp. 349–51.

[8] P. K. Varshney, *Distributed Detection and Data Fusion*, Springer-Verlag, 1997.

[9] S. Marti *et al.*, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. MobiCom*, Aug. 2000, pp. 255–65.

Biographies

RUILIANG CHEN (rlchen@vt.edu) received his Bachelor's degree in communications engineering in 2000 and his Master's degree in communications and information systems in 2003, both from Fudan University, China. He is currently a Ph.D. student in the Bradley Department of Electrical and Computer Engineering at Virginia Tech, Blacksburg. His research interests include traceback and mitigation mechanisms for thwarting denial-of-service attacks, attack-resilient routing protocols for wireless ad hoc networks, and security issues in cognitive radio networks.

JUNG-MIN PARK (jungmin@vt.edu) received a Ph.D. degree in electrical and computer engineering from Purdue University in 2003. He is currently an assistant professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. He conducts research in network attack countermeasures, applied cryptography, and security in cognitive radio networks. He has published numerous papers in leading journals and conference proceedings in the area of network/computer security. He was a recipient of a 1998 AT&T Leadership Award. Current research sponsors include the National Science Foundation, SANS Institute, and Samsung Electronics. More details about his research interests and publications can be found at http://www.arias.ece.vt.edu/index.html.

Y. THOMAS HOU (thou@vt.edu) is an associate professor of electrical and computer engineering at Virginia Tech. His current research interests are radio resource management and networking for cognitive radio wireless networks, optimization and algorithm design for wireless ad hoc and sensor networks, and video communications over dynamic ad hoc networks. From 1997 to 2002 he was a researcher at Fujitsu Laboratories of America, Sunnyvale, California. He is a recipient of an Office of Naval Research (ONR) Young Investigator Award (2003) and a National Science Foundation (NSF) CAREER Award (2004).

JEFFREY H. REED [F'05] (reedjh @vt.edu) is the Willis G. Worcester Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. His area of expertise is in software/cognitive radios, smart antennas, wireless networks, and communications signal processing. From June 2000 to June 2002 he served as director of the Mobile and Portable Radio Research Group (MPRG). He currently serves as director of the newly formed umbrella wireless organization Wireless@Virginia Tech. He is a cofounder of Cognitive Radio Technologies, Lynchburg, Virginia.

To counter SSDF attacks effectively, a two-level defense is required. At the first level, all local spectrum sensing results must be authenticated by the data collector. The second level of defense is the deployment of a data fusion scheme that is robust against SSDF attacks.