Denial-of-Service Attacks on Dynamic Spectrum Access Networks

G. Jakimoski and K. P. Subbalakshmi

Abstract— **Cognitive radio technologies have emerged as a platform to solve the problem of spectrum scarcity for wireless applications since cognitive radios have the potential to utilize the idle licensed spectrum bands in an intelligent way without interfering with other licensed devices. However, most of the proposed protocols for opportunistic usage of the licensed spectrum bands assume that the participants involved in the protocols are honest and that there are no malicious adversaries that will attack the network. Using two examples, we demonstrate that in the presence of a malicious adversary the systems designed making these assumptions will fail to fulfill their goals of minimal disruption of the primary users and efficient utilization of the unused spectrum. We also briefly discuss some security design goals of the future cognitive DSA networks.**

Keywords— **cognitive radio, dynamic spectrum access, overlay networks, security, denial-of-service**

I. Introduction

Cognitive radio [12], [8], [1] includes a range of technologies for making wireless systems computationally intelligent. The original formulation defines the cognitive radio as an autonomous agent that perceives the user's situation to pro-actively assist the user in performing some tasks. The first significant application proposed for cognitive radios was opportunistic utilization of licensed spectrum bands. Traditionally, the spectrum has been regulated by governmental agencies and the spectrum bands are assigned to license holders or services on a long term basis for large geographical regions. These fixed spectrum assignment policies have led to under-utilization of the available spectrum. The inefficiency in the spectrum usage and the limited available spectrum for wireless applications gave rise to Dynamic Spectrum Access (DSA) as a new communication paradigm [7]. The DSA networks use the idle licensed spectrum bands for communication, and they vacate the licensed bands upon the return of the primary licensed users. Cognitive radio technologies have emerged as a natural platform for implementation of DSA networks since they provide tools for opportunistic spectrum usage in an intelligent way.

A plethora of protocols and techniques for DSA implementation have been proposed so far (e.g., [2–6,9–11,13–15]). There are two main common design goals of all these protocols and techniques: the disruption of the primary licensed users should be minimal, and the idle spectrum bands should be used by the secondary users in an efficient manner. We point out that most of the existing proposals achieve these goals without taking the security of the system into consideration. That is, it is assumed that there are no network attackers and the participants involved in the protocols are honest. If a malicious adversary is introduced into the model, then the existing proposals will fail to fulfill the main objectives of minimal disruption of the primary users and efficient utilization of the vacant spectrum bands. We demonstrate this by analyzing examples for two different topologies, an infrastructure-based secondary network and an ad-hoc secondary network. Although we have presented analysis of only two proposed solutions, the types of vulnerabilities we discuss are common to most of the existing proposals. To avoid such vulnerabilities, we suggest making security as one of the goals of the DSA network designs.

The paper is organized as follows. We discuss the denial-of-service vulnerabilities of the existing DSA solutions in Section II. In Section III, we study two proposed systems for opportunistic spectrum access. The paper ends with concluding remarks and a brief discussion of our future work.

II. Denial-Of-Service Attacks on Dynamic Spectrum Access Protocols

There are three main radio network functions in the DSA cognitive radio networks: spectrum sensing, spectrum analysis and decision, and spectrum mobility.

One of the primary requirements of cognitive networks is their ability to scan the spectral band and identify vacant channels available for opportunistic transmission. As the primary user network is physically separate from the secondary user network and the primary users are expected to be legacy systems, the secondary users do not get any direct feedback from primary users regarding their transmission. The secondary users have to depend on their own individual or cooperative sensing ability to detect primary user transmissions. Since the primary users can be spread across a huge geographical area, sensing the entire spectral band accurately is a challenging task. The secondary users have to rely on weak primary transmission signals to estimate their presence. Most of the research on spectrum sensing techniques fall into three categories: transmitter detection, cooperative detection and interference based detection. The main aim of all these techniques is to avoid interference to primary transmissions. The amount of interference caused by all the secondary users at a point in space is referred to as the interference temperature at that point. When a primary user transmission is taking place, the interference temperature should be below a specified

The authors are with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030, USA, e-mail: goce.jakimoski@stevens.edu, ksubbala@stevens.edu.

This work was funded in part by NSF CT grant number: 0627688 and US Army ARDEC/Picattiny Arsenal.

threshold near the primary receivers. However, this is not easy to achieve as the location of the primary receiver is not known to the secondary users. Additionally, when multiple secondary networks overlap, the secondary users scanning the spectrum should not confuse transmissions from secondary users in other secondary networks with primary transmissions.

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

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

The existing implementations of the previously described network functions are designed assuming that all participants involved in the protocols are honest and that there are no malicious adversaries that will try to attack the primary or the secondary network. In most cases, this will lead to DoS vulnerabilities that can be exploited by corrupt users or a malicious adversary. For instance, a corrupt node or a malicious adversary impersonating a network node might lie to its peers about the availability of certain frequency ranges. It might say that a certain band is vacant when it is not, and the secondary users will use that band resulting in a disruption of the primary transmissions. Furthermore, a malicious adversary can alter the sensing data exchanged among the nodes in the network so that they make a wrong conclusion about the availability of channels. The adversary might also modify the control data sent by a central authority to the mobile nodes in order to trick them into using a channel that is not idle (vacant) or evacuating an idle channel. By modifying the data exchanged during the spectrum analysis, the adversary can also trick the secondary network to often switch spectrum bands although there is no return of the primary users, and so on. We demonstrate these vulnerabilities in the next section using two examples, one involving an infrastructure-based cognitive network and one involving an ad-hoc cognitive network. Although we use only two examples, similar vulnerabilities apply to all protocols for cognitive DSA networks that we have studied.

III. Case studies

In this section, we demonstrate the vulnerabilities of the existing proposals for dynamic spectrum access by analyzing the security of two solutions where a network of secondary users utilizes the spectrum in an opportunistic fashion. The first example that we study is an example of a centralized secondary network. The second example is a channel evacuation protocol in an ad-hoc secondary network.

A. Spectrum pooling systems

Weiss et al [13], [14] consider a new strategy called Spectrum Pooling that enables public spectrum access without sacrificing the transmission quality of the actual license owners (i.e., primary users). They suggest to use a modified wireless LAN as rental system. The spectrum sensing in their solutions is performed by the participating mobile terminals. That is, the mobile terminals detect idle frequency subbands, and send the information about the availability of the channels to an access point. The access point uses the received data to construct and broadcast back an allocation vector to the mobile terminals. The allocation vector specifies which channels are occupied by the primary users. The volume of spectrum sensing data can become very high, and signaling this data in ordinary data frames would leave only few resources left for useful data and would be very error-prone. So, the authors suggest the signaling of spectral resources to be performed in the physical layer using a so called boosting protocol. The basic idea of the boosting protocol is superposition of emitted radio power for signaling instead of creating new higher layer frames for the measured data. We demonstrate that a malicious adversary can easily mount a DoS attacks on both the primary and the secondary network by manipulation the data exchanged between the mobile terminals and the access point.

DoS attacks on the secondary network. The boosting protocol runs in two phases. In the first phase, the mobile terminals signal the access point that a primary user is transmitting in a subband that was previously considered idle. In the second phase, the mobile terminals signal the access point that a previously occupied subband has become idle. By manipulating the signaling in either of the two phases of the boosting protocol one can easily trick the secondary network into thinking that certain subbands are occupied even though they are idle. We now give more details.

As mentioned above, the goal of the first phase is to notify the access point that certain channels are no longer available. Having performed their measurements, the mo-

bile terminals compare their spectrum sensing results with the mandatory allocation vector that was broadcast by the access point after the previous detection cycle. If a mobile terminal encounters a spectral access by a primary user to certain channels that are not marked as occupied in the mandatory allocation vector, then it transmits complex symbols at maximum power level on these OFDM carriers where the new licensed user accesses were detected. As a result, we have a power amplification of the licensed user signal. The remaining channels (OFDM carriers) are spared from energy by transmitting complex zeros (0 + j0). The access point continues to detect the incoming signal which is a superposition of the transmitting primary users and all the boosting signals of the mobile terminals. Since the power level in the channels used by new primary users are boosted, the access point will be able to detect such channels with greater probability and make more reliable decisions about channel availability. Clearly, the first phase of the boosting period should be long enough in order to obtain higher level of detection reliability. On the other hand, it should be kept as short as possible as the signaling of the mobile terminals interferes with the signals transmitted by the primary users.

The main advantage of the proposed approach is that the detection results of all mobile terminals are gathered simultaneously. Normally, each mobile terminal would have to transmit an individual data frame containing the detection results. Then, the access point will have to apply a logical OR operation to the data frames received from different mobile terminals in order to decide which channels are not available anymore. In the boosting protocol, the logical OR operation of the individual detection results is replaced by the additive superposition of the boosting signals.

The access point will conclude that a certain channel has been occupied since the last detection cycle if at least one mobile terminal has detected a primary user transmission in the given channel. Since there is no authentication of the mobile terminals involved in the boosting protocol, a malicious adversary can easily trick the access point into thinking that certain subbands are no longer available by transmitting boosting signals on those carriers. Similar problem will arise if some of the mobile terminals are compromised or faulty.

In the second phase of the boosting protocol, the mobile terminals signal the deallocated channels of the primary system. The additive superposition of spectral power that was used on the first phase can only be used to perform a logical OR operation. However, a certain channel can be considered deallocated only if every mobile terminal says that it is deallocated. The boosting protocol solves this problem by signaling the channels that remain allocated, which is a logical negation of signaling the deallocated channels. To avoid disturbance of the primaries, the signaling is conducted on the idle channels detected in the previous detection cycle. Each channel which was marked as allocated in the last detection cycle is associated with a channel that was marked as idle in the last detection cycle. The first allocated channel is associated with the first idle channel. The second allocated channel is associated with the second idle channel, and so on. To signal that a given channel is still allocated, each mobile terminal transmits a boosting signal in the idle channel corresponding to the allocated channel. If the number of allocated channels is greater than the number of idle channels, then the mapping of allocated channels to idle channels is done in a cyclic fashion, and the signaling is extended in time by transmitting multiple boosting frames on the idle channels. If there are more idle channels than allocated channels, then the mapping is cyclically continued until there are no more idle channels left. This results in a redundant, but more reliable detection at the access point.

One can mount a denial of service attack in the second phase of the boosting protocol as follows. Suppose that a certain channel has been deallocated since the last detection cycle. That is, the given channel is no longer used by the primary users. The mobile terminals notify the access point about the deallocation of this channel by not sending a boosting signal in the idle channel corresponding to the (now) deallocated channel. Hence, by sending boosting signals in the idle channels corresponding to the deallocated channels, a malicious adversary can convince the access point that these channels are still in use and deprive the secondary network of a spectrum that is not used by the primary users.

DoS attacks on the primary network. After the execution of the boosting protocol, the access point knows which channels are newly allocated and which channels have been deallocated since the last detection cycle. By combining this knowledge with the previous mandatory allocation vector, the access point constructs a new mandatory allocation vector that specifies which channels will be considered allocated until the next detection cycle. The allocation vector is then distributed to all associated mobile terminals and the ones that want to get associated. It is very important that every mobile terminal receives the same allocation vector because otherwise the licensed system would be disturbed or the transmission within the rental system would fail. Hence, the author suggest a reliable and still fast transmission scheme for the task of distributing the allocation vector. First, the allocation vector is divided into disjoint parts. Each of these parts, a cyclic redundancy checksum (CRC) and the corresponding coding redundancy form one packet. Then, each packet is transmitted on at least three different channels. To select the channels that will be used to broadcast the new allocation vector, the access point uses the mandatory allocation vector that was broadcast in the previous detection cycle. The goal of broadcasting the allocation vector on multiple channels is to overcome the issues that arise due to fading and interference from new primary users.

We assume that the adversary can modify the allocation vector (including the check sums as well) received by the mobile terminals. This can be accomplished for instance by transmitting a “malicious” signal such that the superposition of the malicious signal and the signal transmitted by the access point leads to a signal corresponding to the

modulation of the modified allocation vector. The mobile terminals use the received mandatory allocation vector to decide which channels are idle. Hence, the adversary can easily disrupt the primary users by modifying the allocation vector and tricking the mobile terminals into using channels that are used by the primary users. Note that the adversary can use similar methods (e.g., using directional antennas) to mount a denial-of-service attack on the secondary network by modifying the allocation vector received by the different mobile terminals in a different manner. The mobile terminals will now use incompatible allocation vectors leading to a possible disruption of the secondary network.

B. ESCAPE

In [11], Liu and Ding have proposed a channel evacuation protocol ESCAPE (short for SpeCtrally Agile radio Protocol for Evacuation). As usual, there are two types of users in the considered setting: primary or licensed users that have strict priority on spectrum access, and secondary users that opportunistically access unused spectrum vacated by idle primaries. It is assumed that the secondary users are cognitive devices that are deployed in an ad-hoc manner with no central controller. An example of such setting would be multiple WLAN devices in a building that use an unoccupied TV band. The focus of the ESCAPE protocol is on evacuating channels that are used by the secondary users when the primary users return. It is assumed that the detection of primary users is achieved by at least one secondary cognitive user. Furthermore, it is not assumed that all secondary users that should evacuate can detect the return of a primary user. This is due to different detection capabilities of the secondary users. For instance, one cognitive radio can have a very sensitive detector and feature detection capabilities that others do not have. Another possibility is that some secondary users may fail to detect the primary transmissions due to channel fading or shadowing. Furthermore, certain secondary users might have light communication load and more power resource and can listen to a channel for a sizable duration. Therefore, such secondary users might be more suitable for primary detection tasks. In summary, joint spectrum sensing has the advantage of shared work load and more reliable primary detection. ESCAPE is specifically designed for a distributed primary detection and channel evacuation by sharing information about the return of the primary users.

The ESCAPE protocol operates as follows. Initially, there are some primary channels that are idle, and one or more groups of secondary users detect the idle channels and start to occupy them opportunistically. Later on, the primary users might return. This is detected by one or more secondary users, and the evacuation step begins. The secondary users that have detected a primary will transmit a warning message declaring "primary-active". Other secondary users that hear the announcement will repeat the same warning message "primary-active" until all secondaries are notified of the return of the primary user.

The parameters of the warning message such as the pattern of the warning message, CDMA spreading code to be used and the transmission power are pre-arranged by the secondary users that belong to a given evacuation group during an initialization phase. The size of the evacuation groups and the memberships in the evacuation groups are determined by the geographic area that need to be evacuated for active primaries. For example, all WLAN devices located in the same building may belong to the same group while the devices located in different building do not. The secondary users of a particular evacuation group may belong to different networks, and a secondary node may belong to more than one evacuation group.

After the initialization, secondaries would sense and utilize the idle primary spectrum. During its normal operational phase, a secondary user performs the following procedure individually.

1. If a secondary user has a packet to transmit, it transmits its packet according to its regular access protocol. Then, it goes to Step 2. If a user has no packet to transmit, it goes to Step 3.
2. The secondary user listens to the channel for a specific time.
   - If the user notices that the primary is back or it detects the warning signal, it goes to Step 4.
   - If the user has a packet to transmit or retransmit (e.g., due to a received or missing ACK/NACK or a newly generated packet), it goes to Step 1.
   - Otherwise, it goes to Step 3.
3. The secondary user listens to the channel.
   - If the user detects a primary or a warning message, it goes to Step 4.
   - If it has a packet to transmit, it goes to Step 1.
   - Otherwise, it stays in Step 3.
4. The secondary user sends/relays the warning signal at the predetermined power level a number of times. Then, it goes to Step 5.
5. The user leaves the current band and moves back to the default band.

Attacking the ESCAPE protocol. A malicious adversary can mount a denial-of-service attack on the secondary networks as follows. We assume that the adversary knows the parameters of the warning message (i.e., the pattern of the warning message, CDMA spreading code to be used and the transmission power) for any evacuation group in the system. He can learn these parameters by eavesdropping during the initialization phase or analyzing the warning messages sent during the normal operation phase. Suppose that a given channel is idle and used by secondary users in an opportunistic manner. The adversary can deprive the secondary users from using this channel by sending a fraudulent warning message. The warning message will be relayed by other secondary users and the channel will be quickly evacuated although it is idle. By repeating this procedure, the adversary can easily trick the secondary users to often evacuate the channels and spend most of their time searching for available spectrum instead of engaging in communication with other nodes in the network. An adversary that has compromised some of the nodes can

also mount a limited denial-of-service attack on the primary network. Suppose a primary user returns and starts using a channel that is used by some secondary users as well. If the compromised nodes do not report the return of the primary user and do not relay the warning messages generated by other secondary users, then it is possible that some of the secondary users will not be aware that the primary user has returned, and continue to use the channel even though it is no longer idle.

IV. Conclusion and future work

There is a plethora of proposed implementations of the radio network functions for DSA cognitive networks. We note that most of the proposed implementations are designed assuming that the participants involved in the protocols are not corrupt and that there is no malicious adversary that wants to attack the network(s). Hence, most of the proposed solution are vulnerable to denial-of-service attacks on both the primary networks and the secondary networks. That is, the secondary users can be tricked to use spectrum bands that are not idle, and therefore disrupt the services of the primary network. Also, the secondary users can be tricked into vacating idle channels leading to non-efficient utilization of the available spectrum or disruption of the communication in the secondary network(s). We demonstrate this using two examples: one involving an infrastructure-based cognitive radio networks, and one involving an ad-hoc cognitive radio networks.

The goal of our future work will be to design protocols for secure implementations of cognitive radio network functions for different topologies and different spectrum access scenarios. Our design will be primarily driven by the following goals:

- *Accurate and secure primary user detection.* The ability to scan the spectral band and identify vacant channels available for opportunistic transmission is one of the primary requirements of cognitive networks. We want our protocols to guarantee that a malicious outsider and a limited number of corrupt insiders cannot trick the secondary users into using a non-vacant channel and interfere with a primary user.
- *Resilience to non-jamming DoS attacks on the secondary networks.* Clearly, an adversary can trick a secondary network into thinking that a given channel is not vacant by pretending to be a primary user and transmitting a signal in the given frequency range. However, the primary design goal of the existing protocols is to minimize the disruption of the primary users. In most of the cases, this leads to networks where it is much easier to convince the secondary users to vacate idle channels by manipulating the protocols instead of impersonating a primary user. Hence, besides allowing accurate and secure primary detection, we want our protocols to be as resilient as possible to denial-of-service attacks on the secondary network(s).
- *Efficient and fair spectrum sharing.* The different networks and the users should use the available free spectrum (white space) in an efficient and fair fashion.
- *Efficient implementation.* We want to minimize the communication and computational overhead introduced by adding security to the implementations of the cognitive radio network functions.

References

[1] I. F. Akyildiz, W-Y. Lee, M. C. Vuran and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," Computer Networks, vol. 50, pp. 2127-2159, 2006.

[2] I.F. Akyildiz and Y. Li, "OCRA: OFDM-based cognitive radio networks," Broadband and Wireless Networking Laboratory Technical Report, 2006.

[3] R.W. Brodersen, A. Wolisz, D. Cabric, S.M. Mishra and D. Willkomm, "Corvus: a cognitive radio approach for usage of virtual unlicensed spectrum," Berkeley Wireless Research Center (BWRC) White paper, 2004.

[4] M.M. Buddhikot, P. Kolodzy, S. Miller, K. Ryan and J. Evans, "DIMSUMNet: new directions in wireless networking using coordinated dynamic spectrum access," IEEE WoWMoM 2005, pp. 78–85, 2005.

[5] C. Cordeiro, K. Challapali, D. Birru and S. Shankar, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," IEEE DySPAN 2005, pp. 328–337, 2005.

[6] C. Cordeiro and K. Challapali, "C-MAC: A Cognitive MAC Protocol for Multi-Channel Wireless Networks," IEEE DySPAN 2007, pp. 147–158, 2007.

[7] FCC ET Docket No 03-322: Notice of proposed rule making, 2003.

[8] S. Haykin, "Cognitive radio: brain-empowered wireless communications," IEEE Journal on Selected Areas in Communications, vol. 23, no. 2, pp. 201–220, 2005.

[9] X. Jing and D. Raychaudhuri, "Spectrum co-existence of IEEE 802.11b and 802.16a networks using CSCC etiquette protocol," IEEE DySPAN 2005, pp. 243–250, 2005.

[10] P. Leaves, K. Moessner, R. Tafazoli, D. Grandblaise, D. Bourse, R. Tonjes and M. Breveglieri, "Dynamic spectrum allocation in composite reconfigurable wireless networks," IEEE Comm. Magazine, vol. 42, pp. 72–81, 2004.

[11] X. Liu and Z. Ding, ESCAPE: A Channel Evacuation Protocol for Spectrum-Agile Networks," IEEE DySPAN 2007, pp. 292–303, 2007.

[12] J. Mitola III, "Cognitive radio: an integrated agent architecture for software defined radio," Ph.D Thesis, KTH Royal Institute of Technology, 2000.

[13] T.A. Weiss, J. Hillenbrand, A. Krohn and F.K. Jondral, "Efficient signaling of spectral resources in spectrum pooling systems," 10th Symposium on Communications and Vehicular Technology (SCVT), 2003.

[14] T.A. Weiss and F.K. Jondral, "Spectrum pooling: an innovative strategy for the enhancement of spectrum efficiency," IEEE Radio Communication Magazine, vol. 42, pp. 8–14, 2004.

[15] H. Zheng and C. Peng, "Collaboration and fairness in opportunistic spectrum access," IEEE ICC 2005, pp. 3132-3136, 2005.