On Insider Misbehavior Detection in Cognitive Radio Networks

Kefeng Tan, Shraboni Jana, Parth H. Pathak and Prasant Mohapatra
University of California, Davis, CA 95616
Email: {kftan, sjana, phpathak and pmohapatra}@ucdavis.edu

Abstract—As long-envisioned idea of cognitive radio becomes reality, increasing number of security threats are being identified. Most of the security threats identified in literature deal with external malicious users and provide solutions to mitigate the threats. In this paper, we elaborate on a newer kind of threat referred as *insider attack* in which cognitive users themselves misbehave in order to gain unauthorized or unfair access of the spectrum resources. We show that insider attacks are comparatively easier to carry out in both licensed and unlicensed cognitive operations, and they can severely damage the expected system performance. We discuss how these threats can be mitigated, and outline the specific challenges that need to be addressed when designing a detection and mitigation strategy.

1 Introduction

With recent initiative by spectrum management authorities such as Federal Communications Commission (FCC [1]), the idea of cognitive radio which was proposed long ago has become a reality. Cognitive radio has been proposed to alleviate the problems of spectrum underutilization and scarcity. In its true essence, a cognitive radio (as defined in [2]) is a radio which obtains the knowledge of radio environment, establishes policies of usage and monitors usage needs, and utilizes these factors to adjust its operational parameters and protocols.

The concept of cognitive radio operations can be applied for both licensed and unlicensed bands. We will elaborate how the characteristics of cognitive radio network differ when they are operating in licensed and unlicensed bands. In our discussion, we consider infrastructure-based cognitive radio operations with a central authority known as fusion center/spectrum broker responsible for spectrum management in both licensed and unlicensed bands.

Cognitive Radio in Unlicensed Band (CRUB): In CRUB, there are no licensed users. Instead, users interested in accessing the spectrum resource can do so with some pre-determined guidelines. When there are multiple cognitive users interested in dynamic spectrum access, their mutual priority of access can be determined by them collaboratively.

One popular approach for spectrum resource assignment is to utilize a spectrum broker as shown in Figure 1. Since there are no primary users in unlicensed case, we refer to all the users as cognitive users. Each cognitive user forwards its traffic demand to the spectrum broker. Here, we take the example of an enterprise 802.11 network operating in ISM band where each Access Point (AP) collects the traffic demand of its clients, and forwards its total demand to the spectrum broker. The spectrum broker will dictate when and how the cognitive users will transmit. It allocates channel width to each AP depending on its traffic requirements (e.g. an AP with higher demand is provided with a larger channel width to facilitate faster data transmission), and the process is repeated periodically to adapt to changing requirements of cognitive users. **Cognitive Radio in Licensed Band (CRLB):** In contrast to CRUB, in CRLB, the spectrum resource is already assigned to licensed users (also referred as primary users), and their communication takes strict priority over any other users accessing the spectrum opportunistically (called secondary users (SUs)). Typically, authorities providing licensed access to primary users (PU) also dictate the terms on how SUs can access the spectrum such as IEEE 802.22 standard for TV-band. Figure 2 shows a cognitive radio system (as per IEEE 802.22) in which SUs sense the spectrum for any ongoing activity by primary users, and forward their reports to a fusion center. Based on the received reports, the fusion center allocates the spectrum to the SUs.

The functionality for spectrum resource assignment at fusion center is common for CRUB and CRLB. Hence, any security threat in such spectrum assignment in CRUB applies to CRLB as well but not necessarily vice versa. Note that in order to facilitate a common discussion for licensed and unlicensed spectrum, we use the terms secondary user (SU) and cognitive user interchangeably in the rest of the paper.

2 Major Security Threats

We now outline two types of major security issues in cognitive radio networks - outsider attacks and insider attacks.

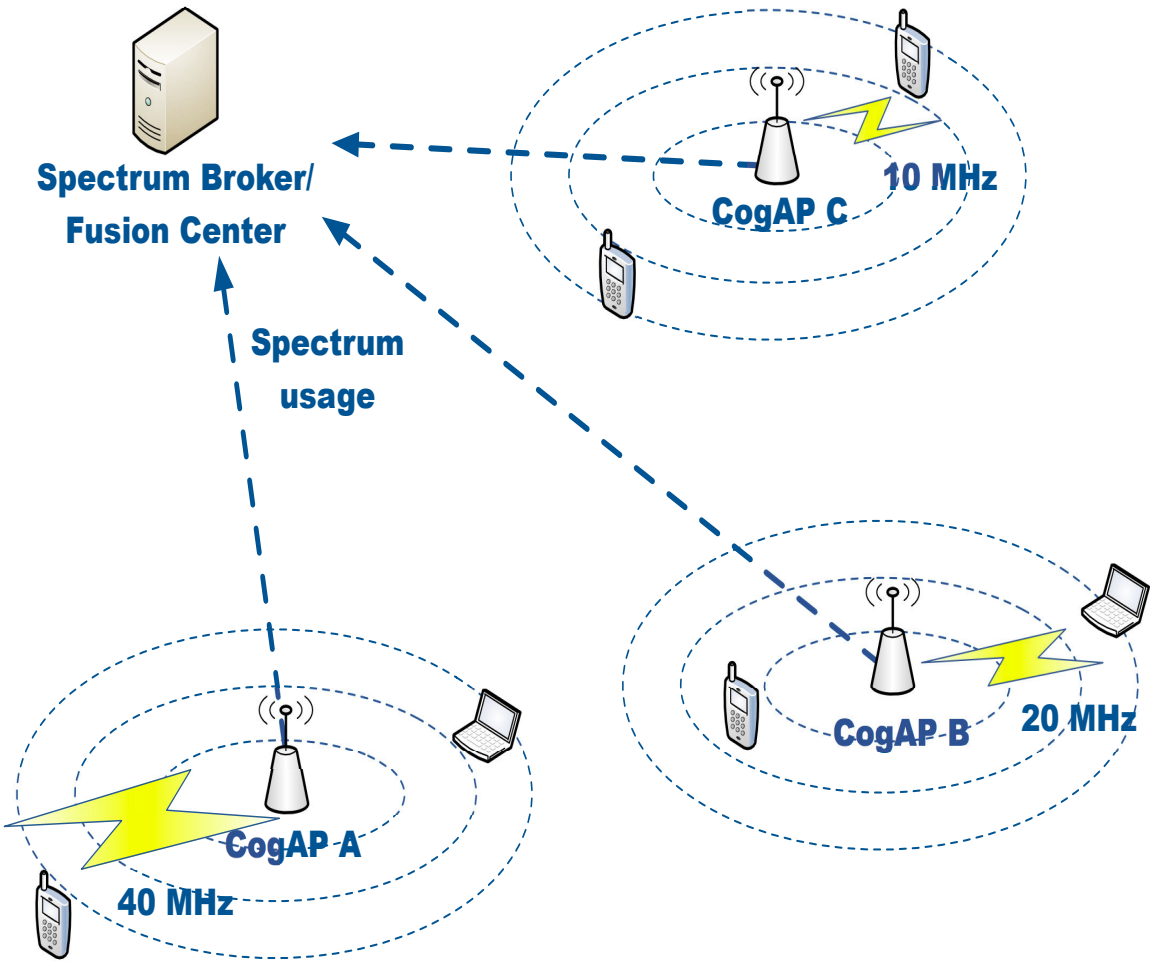

Fig. 1: Cognitive Radio over Unlicensed Band

2.1 Outsider Attacks

In outsider attacks, an adversary can either launch primary user emulations (PUE) attack or jamming attack on secondary networks. When emulating PU, a malicious entity can reduce the availability of spectrum for SUs. In jamming, the attacker (jammer) transmits packets to hinder legitimate communication sessions of SUs and thus creates a denial of service situation. While PUE is limited to CRLB, jamming can be exploited against CRLB or CRUB. Majority of current research efforts are addressing these outsider attacks, for example, in [3], correlation of RF signals and acoustical signals is used to verify the presence of PU. Such and many other outsider attacks are not a part of our study.

2.2 Insider Attacks

In insider attacks, a cognitive user with valid identity provides incorrect information. We refer to such an action on the part of cognitive user as *cognitive user misbehavior*.

Under cognitive user misbehavior, the SUs themselves act maliciously by providing false information about sensing and resource requirements. By doing so, they can either access more resources or prevent other SUs from gaining a fair access. In this work, we are especially interested in highlighting the security threats due to SU misbehavior in licensed and unlicensed bands. Both CRLB and CRUB scenarios are prone to insider misbehavior attacks albeit in different manner.

Misbehavior in CRLB: In CRLB, when SUs report their sensing information to the fusion center, it can employ misbehavior detection techniques to identify if any of the SUs have falsely reported their sensing information. As we discuss later, it is necessary to be careful when employing such strategies because it is possible that radio characteristics (such as path-loss, shadowing etc.) can vary in different regions where SUs are situated for example, behind the building etc (Figure 2). Apart from these spatial variations, other temporal variations can be introduced by the mobility of SUs. We will show in Section 3, that such misbehavior requires evaluating and incorporating trust for the cognitive users.

Misbehavior in CRUB: In CRUB, a cognitive user provides its expected usage requirement to the fusion center. Based on this information, the fusion center performs the radio resource allocation by assigning demand-proportional spectrum. Airtime utilization metric (proposed in [4]) is commonly used in providing the demand

information. We show later that if the cognitive users misbehave by misconfiguring their radio settings, they can in fact introduce significant inefficiency in spectrum utilization. As an example, if the cognitive user sets its wireless interface bit rate to be very low, its airtime utilization will increase, thereby preventing other users to use the spectrum efficiently. Such misbehavior can be handled by developing a monitoring system that can detect any anomalies in spectrum usage. In Section 4, we discuss such a misbehavior monitoring system and show it can be used to improve wireless spectrum utilization.

3 Insider Threats in CRLB

In this section, we discuss the insider threats arising in CRLB, particularly TV bands and emergency bands. FCC approved unlicensed operations in TV bands in 2008 [1]. Cognitive operations on these channels should be intelligent enough to not cause any harmful interference to the passive TV receivers. Efforts are also ongoing to make 700 MHz Emergency Bands to soon follow the suit of TV Bands [5]. During emergencies, cognitive radio technology based commercial devices should provide uninterrupted access to this spectrum to public safety agencies.

We can envision future cognitive radio network having PU with varied degree of mobility as shown in Figure 2. One of the most important operations in CRLB is that of spectrum sensing in which SUs sense the spectrum to detect any ongoing primary user activity. The sensing results are then reported to the fusion center. We now provide some details of how spectrum sensing works and subsequently discuss how it is prone to insider misbehavior attack. Though we study security in spectrum sensing with respect to TV Bands, the same principles can be applied to other licensed bands.

3.1 Spectrum Sensing

The SUs spectrum sensing techniques should be very sensitive to operate at low SNR values. The three main spectrum sensing techniques suggested in literature are - energy detection, matched filtering and cyclostationary feature. Even though many spectrum sensing techniques have been proposed in the literature, we focus on energy detection based sensing because of its simplicity of implementation and its capability to detect any shape of waveforms [6].

Energy detection depends on various radio propagation characteristics - path-loss, shadowing and multi-path fading of the wireless channels. The channel bandwidth (for example 6 MHz in TV Bands) is much larger than the coherent bandwidth, and hence the effect of multi-path fading is negligible. The received PU power sensed at SU at a distance d from PU due to path-loss and shadowing can be expressed as following in dB:

$$P_r(dB) = P_t(dB) - \{PL_0 + 10\alpha log_{10}(\frac{d}{d_0}) + \psi\} \qquad (1)$$

where PL_0 is a path-loss at a reference distance d_0 in dB and is close to $20log10(\frac{4\pi d_0}{\lambda})$, where λ is wavelength. Empirical measurements support the log-normal distribution (in dB) for shadowing ψ which can be typically in the range of 4 to 20 dB. Path-loss exponent α ranges from 2 to 5 [7]. Since the SNR can be as low as $-20dB$, path-loss and shadowing has a great impact on spectrum sensing report of SUs. To counteract such unreliability in spectrum sensing, collaborative spectrum sensing has been proposed to exploit the increased diversity in spectrum sensing measurements.

3.2 Insider attack in sensing

The sensing reports received from cognitive users, in collaborative spectrum sensing is used by the fusion center to determine spectrum availability and in turn perform the spectrum allocation.

Misbehavior of secondary users: It is possible in CRLB that SUs can intentionally report wrongful sensing measurements to the fusion center. Being selfish, an attacker (SU) may report the presence of the primary user when there is actually none in order to force other SUs to evacuate from the spectrum, thus occupying the whole bandwidth. While being malicious, an attacker may report an absence of the PU when there is one to make other SUs violate the primary systems. We hereby, refer to both the selfish and malicious SUs as malicious users.

From Equation 1, if $\mathcal{R}$ is the sensing report received from a honest SU, then $\mathcal{R}$ is a function of PU status and P_r (path-loss and shadowing) based on SU's location during sensing. For static SUs and PUs, the sensing measurements from a location does not vary over the time when the PU is active. Several techniques have been suggested in the literature to churn out malicious SUs from honest SUs. Basically, the approaches, degrade trust value of a SU when its report deviates from common readings beyond a certain threshold (such as [8]). A dishonest attacker can thus be identified, and its negative impact on the spectrum sensing can be weakened or eliminated.

When the SUs are mobile with a static PU in the CRLB, their sensing reports are also impacted by their instantaneous locations unlike static SUs. The uncertainty imposed by different path-loss at different locations makes mobile malicious user detection different from static scenario. For example, existing trust-based solutions tend to over penalize an honest user who is at a bad location with large path-loss. Even when the user moves to a good location later on, its contribution to the spectrum sensing will be limited since it has been assigned a low trust value. In such scenarios, we propose a solution [9] to use two trust parameters, Location Reliability and Malicious Intention (LRMI). Location Reliability (LR) reflects path-loss characteristics of the wireless channel and Malicious Intention (MI) captures the true intention of SUs, respectively.

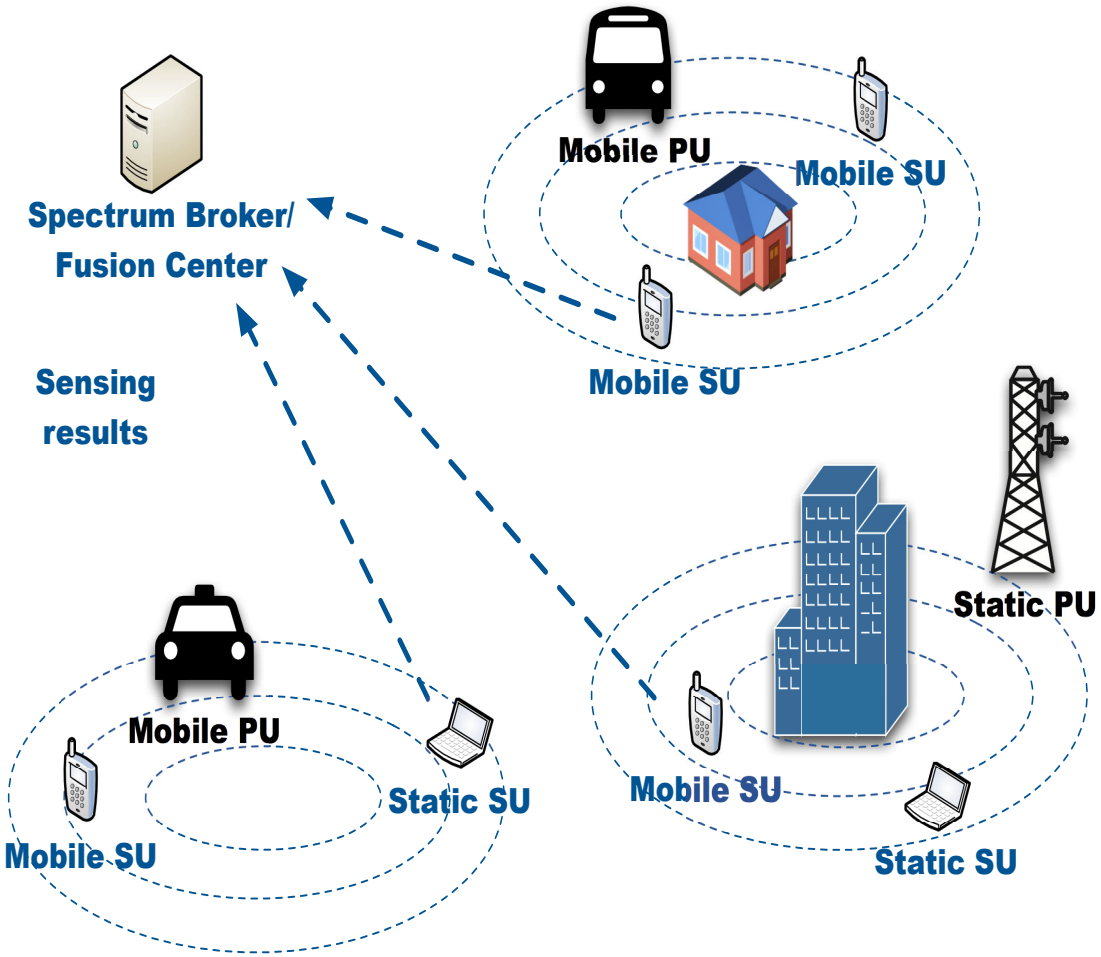

Fig. 2: Cognitive Radio over Licensed Band

Also, note that the scenario complicates when more than one primary user is present in CRLB or PUs are mobile. We will discuss these scenarios in Section 5.

4 Insider Threats in CRUB

One of the popular ways of using cognizance in unlicensed band is to utilize the capability of cognitive radios to switch the central frequency and adjust the channel width depending on factors such as spectrum needs and co-channel interference. Cognitive users can report their spectrum usage needs to a fusion center, and the fusion center can calculate a spectrum allocation by which the entire spectrum is utilized in a demand-proportional manner. Such channel width assignment scheme opens door for an insider attack in which cognitive users can selfishly provide incorrect value of spectrum usage demand, thereby gaining more spectrum resources and preventing other spectrum users for a fair access of spectrum.

Spectrum usage can be evaluated by aggregate throughput, the number of associated cognitive users, or airtime utilization. Compared with the other two metrics, airtime utilization is a more accurate metric because it directly measures the effective bandwidth used to deliver data over the air.

Airtime utilization can truthfully reflect spectrum usage only if all cognitive users utilize the spectrum to its full capacity. The premise, however, can be easily violated in practice if a cognitive user is intentionally misbehaving. It is possible for a cognitive user to change certain wireless settings that will increase its expected airtime utilization demand. For example, if the data rate is set to a lower value, the expected airtime utilization value increases. This increased value in turn prevents other cognitive users to access their proportional share of spectrum.

4.1 Misbehavior of Cognitive Users

We now describe how cognitive users can misconfigure themselves to incur an insider attack.

(a) *Conservative bit rate*: If the bit rate at a cognitive user is set too conservatively, it will not only slow down its own transmissions, but also intensify contentions among all other cognitive users. As a result, the airtime usage increases.

(b) *Low transmit power*: Instead of setting the bit rate, lowering the transmit power also decreases the trans-

mission rate. Its effect is similar to lowering the bit rate, except that the bit rate can still be adjusted within a possibly reduced range, rather than be set to one value.

(c) *Bit rate and channel-width mismatch*: Assume a relatively wide channel is allocated to a cognitive AP, where all devices are operating properly. If one of the cognitive users moves further away from the AP, its frames will have to be delivered at a lower bit rate to ensure reliable transmissions. However, this is not an efficient way to utilize a wide channel. The same capacity can also be achieved over a narrower channel with increased bit rates.

We now use a case of conservative bit rate setting as an example to demonstrate the potential airtime inflation. A UDP traffic of 4 Mbps is loaded over a line-of-sight link between two laptops that are 20 feet apart. The bit rate is fixed at the sender, but is set to `auto` at the receiver. We plot the normalized airtime utilizations of all IEEE 802.11g bit rates, with regard to that of the auto bit rate. Figure 3 shows how the airtime usage increases with

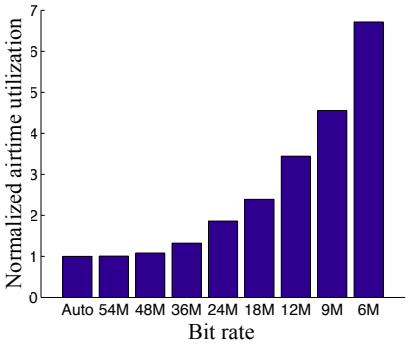

Fig. 3: Airtime varies with different bit rates.

the decrease of the bit rate. Through analysis of packet trace for the case of auto bit rate, we find the packet retransmission ratio is less than 0.02%, which indicates that the wireless link is highly reliable. In addition, the frames are sent at 54 Mbps most of the time (95%). This explains why the throughput is similar in the case of 54 Mbps and the case of auto bit rate. As the bit rate is gradually decreased, the airtime utilization is increased up to 7x at 6 Mbps. This shows how a cognitive user can reduce its data rate and thereby ask for more spectrum resources, creating a spectrum unavailability for other cognitive users.

4.2 Detecting Misbehavior

We proposed a detection system (Pinokio [10]) that can detect the misbehaving insider cognitive users. Pinokio uses a Misbehavior Detection System (MDS) which maintains a statistical profile on network system's normal behavior based on the training data [11]. When the network's recent behavior significantly deviates from its normal statistical profile, an alarm will be triggered about possible anomaly. Below, we describe how Pinokio can detect misbehavior using bit-rate.

4.2.1 Using Bit Rate Behavior for Misbehavior Detection

Next, we identify four key features of misbehavior detection using bit rate. Adding more features may increase the sensitivity of the detection system, but can also incur additional performance overhead.

Contiguous adjustment of bit rate. We are interested in knowing how much the bit rate changes at a time. In a normal case, the bit rate will only decrease one step at a time in case the channel deteriorates, or increase one step at a time when the channel quality improves. The consecutive adjustment of bit rate can avoid two things. On one hand, a dramatic bit rate jump can cause the loss of connectivity. On the other hand, a large bit rate reduction results in the delay of transmission. In an abnormal case, the bit rate may be set too high or too low, thus not change in a contiguous fashion.

Response to transmission failure. A transmission can fail due to two reasons: collision (with other packets in the air) or weak signal (at the receiver side). After the sender sends out a packet, it will expect an ACK from the receiver to confirm a successful reception. If the sender does not receive the ACK, it will first infer that the packet is lost due to collision. To reduce the possibility of further collisions, it will increase its own back-off window size and then will retransmit the packet. If it fails again, it may also start slowing down the data rate of retransmissions, besides increasing backoff window size. This is because the chances of collision become smaller as the back-off window increases, and the variation of wireless channels should be the main reason for the packet losses. In that case, reducing transmission rate will increase the probability of delivery. However, if the bit rate is fixed, the bit rate in retransmissions stay the same regardless of the failures.

Reciprocity of bit rates. It is widely believed that wireless channels exhibit certain reciprocity. Recent experimental results have also shown that the received signal strengths (RSS) between a communicating pair are highly correlated, whose similarity can even be exploited for generating secret keys [12]. The bit rates between a communicating pair should therefore also exhibit certain reciprocities. However, this reciprocity will be altered when anomalous behavior is present.

Percentage of low bit rates. A device pair demanding a large channel-width should be able to fully leverage the spectrum for high bit rate transmissions. Delivering traffic at low bit rates over a wide channel reduces the spectrum efficiency and thus should be avoided. We therefore use the percentage of low bit rate over a wide channel to detect the case. The definition of "wide channel" and "low bit rate" depends on whether the similar throughput can be achieved via a narrower channel.

4.2.2 Building Statistical Profile for Normal Behavior

In the MDS algorithm, building the statistical profile for normal behavior is through a long-term learning from

normal behavior. In the context of spectrum misbehavior detection, the training can be divided into two steps. One is to learn an empirical distribution for Q statistics, and the other is to acquire a proper threshold for each feature. Factors, such as signal propagation and transmit power, can strongly influence the bit rate behavior. The process of training can make the system better adapt to different networks and wireless environments. The initial training to obtain proper distributions and thresholds is thus essential to the detection.

The detection system also needs to adapt to another change - the evolution of network behavior. New bit rate schemes are constantly evolving and may not be matched with the historical profile. Fortunately, the MDS algorithm provides a scheme to allow the gradual adaptation to behavior changes. A fading factor is defined such that the normal statistical profile will eventually "forget" the ancient data. If, on the other hand, the system behavior changes abruptly, the detection system can discard all historical data and rebuild the profile through the training.

4.2.3 Performance of Misbehavior Detection System

Due to the space limit, we present the results for one misbehavior detection - detecting conservative bit rate setting. Indeed, we conduct experiments for all other cases of misbehavior detection and find the proposed system - Pinokio can achieve similar or better detection performance [10].

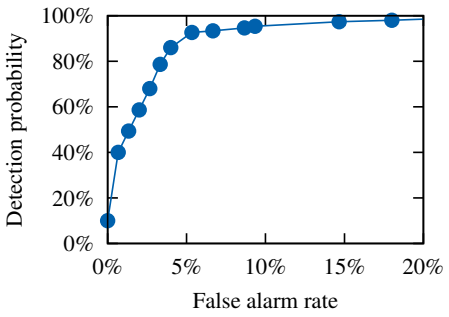

Fig. 4: Conservative bit rate: ROC curve of detection performance when the airtime increases by 20% with 40% of misuse.

Over a wireless link that can support 54 Mbps bidirectionally, we intentionally drop the bit rate to 24 Mbps (4 level difference) at one laptop to emulate the conservative bit rate setting. Over the same link, the bit rate adaptation at the other laptop maintains automatic and is observed to use 54 Mbps mostly. To assess the robustness, we also move around the misbehaving laptop at a walking speed (about 1 meter/second).

Figure 4 shows the Receiver Operating Characteristic (ROC) curve of dropping the bit rate with 40% packets (among all packets) are delivered at a lower rate, which roughly increases the airtime by 20%. While maintaining the same false alarm rate of 5%, Pinokio can detect

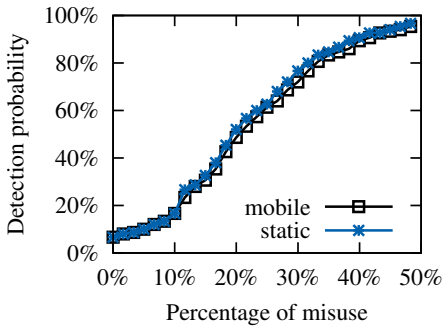

Fig. 5: Conservative bit rate: detection probability versus percentage of misuse.

the misbehavior at the probability of more than 90%. Figure 5 demonstrates the detection rates across different percentages of misbehavior. It also indicates that the system performs stably in both static and mobile scenarios. In this case, 50% of the misbehavior can increase the airtime by 25%.

5 Challenges

In this section, we discuss the challenges in addressing the insider attacks in CRLB and CRUB.

5.1 Challenges for CR over Licensed Band

The impact of malicious SUs, behaving independently, to falsify their sensing and location information was discussed in Section 3. But, the insider threat in CRLB becomes further more complicated when either more than one PU is present, or both SUs and PUs are mobile or SUs are colluding. Summarizing challenges required to be addressed for insider attacks in CRLB:

- Multiple PUs - We mentioned location reliability aids in evaluating secondary users' trust with only one PU in the network (Section 3). With more than one PUs in the network, it will be challenging to evaluate the location reliability itself.
- PUs & SUs Mobility - It is also possible that the PUs are mobile. PUs at different locations end up with different sensing measurements based on instantaneous shadowing and path-loss effects. In other words, the SU's sensing report is effected by not only its own mobility but PU's mobility as well. The received power (P_r) from PU at every location at every time will differ based on its location. Hence, location reliability cannot be used in such scenarios.
- Colluding SUs - Another challenge of misbehavior detection is when SUs are colluding among themselves. The SUs can collude in three major ways - mobility pattern and sensing measurements or both. In mobility-pattern collusion, the malicious nodes can use specific mobility pattern to lower or increase reliability of a location and hence, avoid getting detected. It is challenging to detect this type of collusion even with a single PU in the system.

In another collusion attacks, the sensing reports can be manipulated in a very organized manner by colluding SUs making it challenging for fusion center to detect such insider threats.

Figure 6 shows the factors effecting sensing measurements received by the fusion center. A complete solution for secured CRLB needs to accommodate each of these factors. When all parameters are correctly incorporated, it is possible to mitigate cognitive user(s) misbehavior in CRLB.

5.2 Challenges for CR over Unlicensed Band

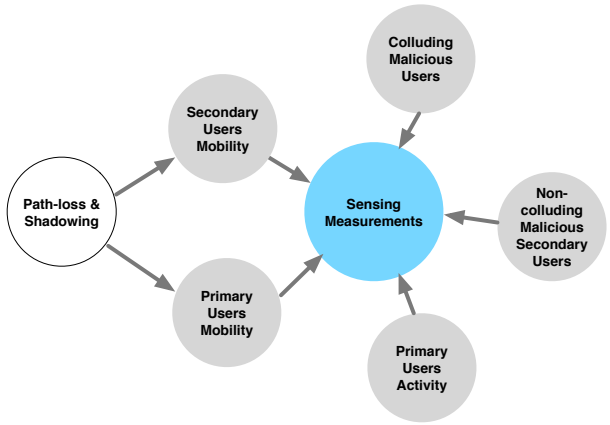

Fig. 6: Factors Impacting Sensing Measurements

Conceptually, a misuse detection system has two components: the features such as "contiguous bit rate changes" or "bit rates slow down in retransmissions", and the modeling algorithms such as statistical approach in IDES. Many previous research efforts have been made towards designing new features such as DOMINO [14], or new methods such as Watchdog and Pathrater [15], or new system architecture such as distributed IDS [13]. The proposed system - Pinokio [10] observes a set of new features of bit rates, and leverages it to enable the detection of insider attacks over the unlicensed band. However, it does not address following issues:

- The monitors (APs) of MDS are supposed to be trustworthy. In reality, they are not always impeccable, and AP itself can be a rogue AP.
- The mobile clients are only assumed to move at a low speed. When they move at a faster speed, their associations with AP change quickly. This results into frequent variations in AP's traffic demand. It therefore makes system's default behavior fluctuate at a faster speed, and statistical algorithms of MDS that depends on default system behavior (normal behavior) might not function correctly.
- The features used in MDS for anomaly detection are extracted from our own observations and analysis. In advanced wireless system, such as IEEE 802.22 or LTE system, the relationship of bit rate, channel width, dynamic power control and scheduling can be coupled in a complicated way. It is desirable to explore data mining based approach to help differentiate normal behavior and abnormal behavior.

In addition, ensuring MDS function effectively in highly mobile settings is a difficult problem in general. The high mobility will result in frequent network topology changes in mobile or vehicular ad-hoc networks (MANET/VANET), thus previous research has proposed to use a distributed monitoring system instead of centralized architecture [13]. Different from that, our techniques correlates sensing report with location reliability, and thus can deal with the mobility of SUs in CRN.

One important direction for future research is to utilize collaborative sensing and decision making when there is no central fusion center available. The distributed nature of such schemes make it even more difficult to detect insider attacks. This requires considering crowdsourcing as a way for network monitoring where each cognitive user monitors the behavior of a subset of other cognitive users, and the spectrum usage will be evaluated based on the monitoring results from multiple peers.

6 Conclusion

In this paper, we provide an overview of how cognitive radio operations differ in licensed and unlicensed bands. We also outline major security issues that are common in both cases. Though majority of the threats in current literature is due to outsiders (other malicious users not part of the system), significant security risks can emerge due to activities of insider users only (existing cognitive users). Such insider threat can be caused by selfish misbehavior of cognitive users. It is shown that in both licensed as well as unlicensed cases, cognitive users can provide false information (about sensing and resource requirement) that can prevent other cognitive users from successfully occupying the spectrum for their needs.

We discussed our solutions for insider threats in cognitive radio network and summarized the challenges faced by the fusion center to make such a system fully secure.

References

[1] FCC. In the matter of unlicensed operation in the TV broadcast bands: second report and order and memorandum opinion and order., Nov. 2008.

[2] S. Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE J.Sel. A. Commun.*, 23(2):201–220, September 2006.

[3] Shaxun Chen, Kai Zeng, and Prasant Mohapatra. Hearing is believing: Detecting wireless microphone emulation attacks in white space. *IEEE Transactions on Mobile Computing*, 12(3):401–411, 2013.

[4] Paramvir Bahl, Ranveer Chandra, Thomas Moscibroda, Rohan Murty, and Matt Welsh. White space networking with wi-fi like connectivity. *SIGCOMM Comput. Commun. Rev.*, 39(4):27–38, August.

[5] J. M. Peha. Fundamental Reform in Public Safety Communications Policy. *Federal Communications Bar Journal*, 59(3):517–45, June 2007.

[6] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Comput. Netw.*, 50(13):2127–2159, September 2006.

[7] Shridhar Mubaraq Mishra, Rahul Tandra, and Anant Sahai. Coexistence with primary users of different scales. In *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN - 2nd IEEE International Symposium on*, pages 158–167. IEEE.

[8] Praveen Kaligineedi, Majid Khabbazian, and Vijay K. Bhargava. Malicious user detection in a cognitive radio cooperative sensing system. *Trans. Wireless. Comm.*, 9(8):2488–2497, August.

[9] S. Jana, K. Zeng, and P. Mohapatra. Trusted collaborative spectrum sensing for mobile cognitive radio networks. In *INFOCOM 2012. IEEE 31st Conference on Computer Communications*.

[10] Kefeng Tan, Kai Zeng, Daniel Wu, and Prasant Mohapatra. Detecting spectrum misuse in wireless networks. In *MASS 2012. International Conference on Mobile Ad-hoc and Sensor Systems*. IEEE.

[11] Harold S Javitz and Alfonso Valdes. The SRI IDES statistical anomaly detector. In *Research in Security and Privacy, 1991. Proceedings., IEEE Computer Society Symposium on*, pages 316–326. IEEE.

[12] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, MobiCom '08, pages 128–139, New York, NY, USA, 2008. ACM.

[13] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 275–283, New York, NY, USA, 2000. ACM.

[14] Maxim Raya, Jean-Pierre Hubaux, and Imad Aad. DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, MobiSys '04, pages 84–97, New York, NY, USA, 2004. ACM.

[15] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 255–265, New York, NY, USA, 2000. ACM.