Is Channel Fragmentation/Bonding in IEEE 802.22 Networks Secure?

S. Anand, K. Hong
Department of ECE
Stevens Institute of Technology
NJ 07030
Email: {asanthan,khong}@stevens.edu

S. Sengupta
Department of Mathematics & Computer Science
John Jay College, City University of New York
NY 10019
Email: ssengupta@jjay.cuny.edu

R. Chandramouli
Department of ECE
Stevens Institute of Technology
NJ 07030
Email: mouli@stevens.edu

***Abstract*—We address a unique security threat that arises due to channel fragmentation (or aggregation or bonding) in dynamic spectrum access (DSA) based IEEE 802.22 networks. Typically, channel fragmentation, aggregation and bonding have been studied in the literature as a means to enhance the spectrum utilization. However, the loss of orthogonality between the spectrum bands due to channel fragmentation, aggregation or bonding can be exploited by malicious attackers to cause a cognitive service disruption. We present an analysis of such a threat. We determine the optimal transmit powers a malicious attacker transmits on each fragment, so as to create maximum service disruption. Numerical results indicate that a malicious attacker can cause up to about 16% loss in the capacity of the system as a consequence of fragmentation. Detailed analysis is presented for channel fragmentation and can be easily applied to channel aggregation and bonding. To the best of our knowledge, this is the first analysis of such cognitive service disruption threats due to fragmentation.**

Index Terms – DSA Networks, IEEE 802.22, Channel Fragmentation, Aggregation, Bonding, Cognitive Service Disruption.

I. Introduction

Dynamic spectrum access (DSA) [1] based cognitive radio networks [2] were developed as a solution to the under utilization of spectrum due to fixed spectrum allocation. Unlicensed "secondary" users use the spectrum (called white spaces) unused by the licensed "primary" users. The IEEE 802.22 wireless regional area networks (WRAN) [3] emerged as the first standards for cognitive radios. The physical layer (PHY) and medium access control (MAC) specifications for secondary to use the white spaces in the television (TV) transmission band can be found in [4]. The IEEE 802.22 standard specify policies for channel fragmentation, bonding and aggregation (definitions of these terms are provided in the following paragraph). We identify a potential security vulnerability resulting due to these three features. We illustrate the practicality of the attack by test-bed experiments followed by a detailed theoretical analysis.

Channel fragmentation, aggregation and bonding were studied as a means to enhance the spectrum utilization in DSA networks [5]-[9] and the references therein as well as 802.11n wireless LANs [10]. Channel fragmentation refers to allocating a portion of a spectrum band , e.g., if a channel has a bandwidth of 6 MHz, fragmentation allows allocation of a portion of the spectrum band corresponding to a bandwidth of 2 MHz to a user. It is also possible to combine two contiguous spectrum bands of 2 MHz each to provide a user a channel with 4 MHz bandwidth. This is called channel bonding. Alternatively, non-contiguous spectrum bands can be aggregated and allocated to users. The IEEE 802.22 standard also specifies the policies for channel fragmentation, aggregation and bonding.

Sengupta *et al* [5] proposed a utility based graph coloring algorithm that presented the advantages using channel fragmentation and aggregation. In [6], Song and Lin present and enhanced MAC protocol for DSA networks, where the effectiveness of channel fragmentation, aggregation and bonding were demonstrated by achieving enhanced throughput. Bahl *et al* provided an experimental set up for channel assignment that utilizes the white spaces in the spectrum. An architecture for the utilization of DTV white spaces incorporating channel fragmentation was provided in [8]. A detailed study of channel fragmentation and related works can be found in [9].

Although channel fragmentation, aggregation and bonding resulted in larger throughput, we identify an important security vulnerability resulting due to these features. Typically the IEEE 802.22 and 802.11n networks use orthogonal channels for transmission. However, fragmentation, aggregation or

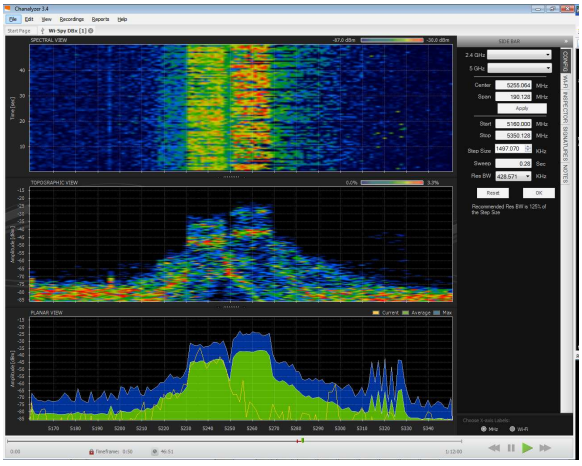

Fig. 1. Test-bed experiment demonstrating leakage on other channels due to bonding.

bonding of channels can result in loss of orthogonality and hence, mutual interference or "leakage" from one channel to the other. To illustrate this, we conduct test bed experiments by implementing a cognitive radio prototype [11] based on a software abstraction layer over off-the-shelf IEEE 802.11 a/b/g supported by Atheros hardware chip sets. We bond two channels (corresponding to 5.24 GHz and 5.26 GHz) and measure the power on all the other channels. Fig. 1 provides the wispy image of our experimental results. The green color in the bottom-most picture in the wispy image in Fig. 1 represents the average power on the channels and the blue color represents the peak powers measured on the channels. It is observed that a power of -40 dBm on the bonded channel results in a significant leakage on the neighboring spectrum bands. This is a consequence of the loss of orthogonality between spectrum bands resulting due to bonding. Similar consequences can also be expected for channel fragmentation and aggregation.

The leakage demonstrated in Fig. 1 can result in a unique denial of service (DoS) threat in IEEE 802.22 based DSA networks. A malicious attacker can exploit the correlation between the non-orthogonal fragments (resulting due to fragmentation or aggregation or bonding) and cause service disruption. Service disruption in wireless networks have traditionally been viewed as jamming attacks [12]. Cognitive radios are also susceptible to multi-channel jamming [13] where the jammer can switch channels to jam multiple channels or the attacker chooses a particular set of channels and jam them [14]. However, the service disruption threat due to fragmentation is significantly different because a malicious attacker can now transmit on channel j to cause service disruption on channel i. The attack exploits the loss of orthogonality between channels which is a consequence of fragmentation, aggregation and bonding. The service disruption need not be a complete DoS, but can be a loss in the channel capacity or loss in throughput, thus resulting in degraded quality-of-service (QoS).

In this paper, we present an analysis of the service disruption caused by a malicious attacker in an IEEE 802.22 based DSA network with fragmentation. We study the loss in capacity due to the attacks. We formulate an optimization problem in which the malicious attacker launches attacks on the channels so as to maximize the leakage in the system. We use the correlation between the channels (obtained using standard inner product definition of correlation [15]). Numerical results indicate that at low transmit powers, malicious attackers do not cause significant loss in the capacity due to fragmentation. However, for larger transmit power of malicious attackers, fragmentation can result in service disruption causing upto about 16% loss in the channel capacity. In terms of data rates, this could be between 200 Kbps to 9 Mbps. *To the best of our knowledge, this is the first analysis on service disruption due to fragmentation.* While the analysis presented in this paper is applicable to any DSA network in general, it is particularly applicable to IEEE 802.22 WRAN where the policies for fragmentation, aggregation and bonding has been specified. Detailed analysis is presented for fragmentation and can also be easily applied to channel aggregation and bonding.

The rest of the paper is organized as follows. The description of the system and the analysis of the service disruption attack is provided in Section II. Numerical results are provided in Section III and conclusions are drawn in Section IV.

II. Cognitive Service Disruption

Consider a DSA network (e.g, an IEEE 802.22 WRAN) with N orthogonal channels which can be used by secondary users when the primary users are inactive. Each of these N channels can be fragmented into K sub-channels. Henceforth, throughout the paper, "channel" refers to one of the NK fragments in the system, unless explicitly mentioned otherwise. The NK fragments need not be mutually orthogonal, in general. Therefore, when signals are transmitted in the i^{th} fragment $(1 \leq i \leq NK)$, it causes energy leakage in the j^{th} fragment $(j \neq i)$. This kind of energy leakage can be exploited by malicious nodes in the network to disrupt the communication of the other good secondary users in the system.

It is of interest to determine the service disruption caused by a malicious attacker to the good secondary users in the system. In order to perform the analysis, we consider the following system.

- There are NK fragments such that the correlation between fragments i and j is ρ_{ij}. If the corresponding fragments are orthogonal, then $\rho_{ij} = 0$.
- On channel i, the attacker transmits a signal with signal strength, E_i, that corresponds to a power, $P_i = |E_i|^2$.
- The total power that can be transmitted by the attacker on all the channels is P_{tot}.

Let $\mathbf{C} = [c_{ij}]_{\substack{1 \leq i \leq NK \\ 1 \leq j \leq NK}}$, where $c_{ij} = \rho_{ij}$, $\forall\ i \neq j$ and $c_{ii} = 0$, $\forall\ i$, represent the co-variance between channels i, j, $\forall\ i \neq j$. Let Let $\mathbf{e} = [E_i]_{1 \leq i \leq NK}$ represent the vector of field strengths on all the channels and let $\mathbf{p} = [P_i]_{1 \leq i \leq NK}$ be the vector of corresponding powers. Signals transmitted on any channel cause a leakage on the other channels since the fragmented channels are not orthogonal in general. The leakage caused by the attacker on the i^{th} channel, l_i, can be written as

$$l_i = \textstyle\sum_{i=1}^{NK} C_{ij} E_j, \quad \forall i, \tag{1}$$

which, can be written as the matrix equation,

$$\mathbf{l} = \mathbf{Ce}, \tag{2}$$

where $\mathbf{l} = [l_i]_{1 \leq i \leq NK}$. *If the channels are all mutually orthogonal, then $c_{ij} = 0$, $\forall\ i \neq j$. Since $c_{ii} = 0$, $\forall\ i$, the leakage, $l_i = 0$, $\forall\ i$. Since fragmentation results in non-orthogonal channels, $l_i \neq 0$, in general.* The power leaked on the i^{th} channel can be obtained as l_i^2. The average power leaked on all the channels in the system, $\overline{P}_{\text{leaked}}$, can be written as

$$\overline{P}_{\text{leaked}} = \frac{1}{NK} \sum_{i=1}^{NK} l_i^2 = \frac{1}{NK} \mathbf{l}^H \mathbf{l} = \frac{1}{NK} \mathbf{e}^H \mathbf{C}^H \mathbf{C} \mathbf{e}, \tag{3}$$

where $(.)^H$ represents the Hermitian of a vector or a matrix.

Ideally, the malicious attacker allocates its total transmit power, $P_{\rm tot}$, on all the channels, such that the impact on each of the channels is highest. In order determine the impacts on all the channels, the attacker should have an exact knowledge of all the applications on all the channels in the system, which may not be possible in general. A more practical scenario is when the attacker tried to maximize the average power due to leakage, $\overline{P}_{\rm leaked}$, which can be formulated as the following optimization problem

$$\max_{\mathbf{e}} \mathbf{e}^H \mathbf{C}^H \mathbf{C} \mathbf{e} = \max_{\mathbf{e}} \mathbf{e}^H \mathbf{A} \mathbf{e}, \tag{4}$$

(where $\mathbf{A} \stackrel{\triangle}{=} \mathbf{C}^H \mathbf{C}$), subject to the constraint,

$$\sum_{i=1}^{NK} P_i = \mathbf{e}^H \mathbf{e} \leq P_{\rm tot}. \tag{5}$$

The matrix, $\mathbf{A}$, is a Hermitian matrix (i.e., $\mathbf{A}^H = \mathbf{A}$ and hence, has real eigen values [16]. Let $\mathbf{P}$ be the matrix whose columns are the eigen-vectors of $\mathbf{A}$. Since $\mathbf{A}$ is a Hermitian matrix, $\mathbf{P}$ can be chosen to be unitary [16] (i.e., $\mathbf{P}^H\mathbf{P} = \mathbf{P}\mathbf{P}^H =$the identity matrix, $\mathbf{I}$. The vector, $\mathbf{e}$ can be written as [16]

$$\mathbf{e} = \mathbf{P}\mathbf{d}, \tag{6}$$

where $\mathbf{d} = [d_i]_{1 \leq i \leq NK}$ is another vector of length, NK. Let the set of eigen-values of $\mathbf{A}$ (called the spectrum of $\mathbf{A}$ [16]), $\sigma(\mathbf{A})$, be $\sigma(\mathbf{A}) = \{\lambda_1, \lambda_2, \cdots, \lambda_{NK}\}$ and without loss of generality, let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{NK}$. Such an ordering is possible since λ_i's are real.

It is then possible to formulate the optimization problem in (4) subject to (5), in terms of $\mathbf{d}$. The following lemma from matrix theory is used in describing the optimization problem and constraint with respect to $\mathbf{d}$.

Lemma 2.1: [16] If $\mathbf{P}$ is unitary in (6), then $\mathbf{e}^H\mathbf{e} = \mathbf{d}^H\mathbf{d}$. From Lemma 2.1, (5) can be written as

$$\mathbf{d}^H\mathbf{d} = \sum_{i=1}^{NK} d_i^2 \leq P_{\rm tot}. \tag{7}$$

The optimization problem in (4) can then be re-written in terms of $\mathbf{d}$ as

$$\max_{\mathbf{d}} \mathbf{d}^H \mathbf{P}^H \mathbf{A} \mathbf{P} \mathbf{d} = \max_{\mathbf{d}} \mathbf{d}^H \mathbf{D} \mathbf{d}, \tag{8}$$

where $\mathbf{D}$ is the diagonal matrix, diag$(\lambda_1, \lambda_2, \cdots \lambda_n)$. Therefore, the optimization problem described in (8) subject to (7), is the optimization problem,

$$\max_{\mathbf{d}} \sum_{i=1}^{NK} U(\mathbf{d}) = \max_{\mathbf{d}} \sum_{i=1}^{NK} \lambda_i d_i^2 \tag{9}$$

subject to

$$\sum_{i=1}^{NK} d_i^2 \leq P_{\rm tot}. \tag{10}$$

The following lemmas and theorem will be used to solve the optimization problem in (9) subject to (10), which, in turn, will be used to solve (4) subject to (5).

Lemma 2.2: If $\lambda_k < 0$, $d_k = 0$ at the optimum point.

Proof: Let $\tilde{\mathbf{d}} = \left[\tilde{d}_i\right]_{1 \leq i \leq NK}$ be a feasible solution such that $\tilde{d}_k > 0$. Consider another solution $\hat{\mathbf{d}} = \left[\hat{d}_i\right]_{1 \leq i \leq NK}$, where $\hat{d}_k = 0$ and $\hat{d}_j = \tilde{d}_j$, $\forall\ j \neq k$. Since $\tilde{\mathbf{d}}$ is a feasible point, $\sum_i \tilde{d}_i^2 \leq P_{\rm tot}$, i.e., $\sum_i \hat{d}_i^2 \leq P_{\rm tot}$. Therefore, $\hat{\mathbf{d}}$ is also a feasible point. The proof is complete if it can be shown that $U(\tilde{\mathbf{d}}) < U(\hat{\mathbf{d}})$.

$$\begin{aligned} U(\tilde{\mathbf{d}}) &= \sum_{i=1}^{NK} \lambda_i \tilde{d}_i^2 \\ &= \sum_{\substack{i=1 \\ i \neq k}}^{NK} \lambda_i \tilde{d}_i^2 + \lambda_k \tilde{d}_k^2 \\ &= \sum_{\substack{i=1 \\ i \neq k}}^{NK} \lambda_i \hat{d}_i^2 + \lambda_k \tilde{d}_k^2 \\ &< \sum_{\substack{i=1 \\ i \neq k}}^{NK} \lambda_i \hat{d}_i^2 \text{ since } \lambda_k < 0 \\ &= U(\hat{\mathbf{d}}). \end{aligned}$$

■

Lemma 2.2 implies that positive d_i's should be allocated only corresponding to positive eigen values. The following lemma provides a constraint on the positive d_i's.

Lemma 2.3: Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$ and let $\lambda_i < 0$, $i > m$, $m \leq NK$. At the optimum point, $\sum_{i=1}^m d_i^2 = P_{\rm tot}$, i.e., (10) is met with equality.

Proof: From Lemma 2.2, $d_i = 0$, $\forall i > m$. Consider a feasible point $\tilde{\mathbf{d}} = \left[\tilde{d}_i\right]_{1 \leq i \leq m}$ such that $\sum_{i=1}^m \tilde{d}_i^2 = \tilde{P} < P_{\rm tot}$. Let $\Delta \stackrel{\triangle}{=} P_{\rm tot} - \tilde{P}$. It is noted that $\Delta > 0$. Consider $\hat{\mathbf{d}} = \left[\hat{d}_i\right]_{1 \leq i \leq m}$, such that $\hat{d}_m = \tilde{d}_m + \sqrt{\Delta}$ and $\hat{d}_i = \tilde{d}_i$, $i = 1, 2, \cdots, m-1, m+1, \cdots NK$. Therefore,

$$\begin{aligned} \sum_{i=1}^{NK} \hat{d}_i^2 &= \sum_{i=1}^{m} \hat{d}_i^2 \\ &= \sum_{i=1}^{m-1} \tilde{d}_i^2 + \hat{d}_m^2 \\ &= \sum_{i=1}^{m-1} \tilde{d}_i^2 + \tilde{d}_m^2 + Delta \\ &= \tilde{P} + \Delta = P_{\rm tot}, \end{aligned}$$

i.e., $\hat{\mathbf{d}}$ is also a feasible point with $\sum_{i=1}^m \hat{d}_i = P_{\rm tot}$.

$$\begin{aligned} U(\hat{\mathbf{d}}) &= \sum_{i=1}^{m} \lambda_i \hat{d}_i^2 \\ &= \sum_{i=1}^{m-1} \lambda_i \tilde{d}_i^2 + \lambda_i \hat{d}_m^2 \\ &= \sum_{i=1}^{m-1} \lambda_i \tilde{d}_i^2 + \lambda_i \tilde{d}_m^2 + Delta \\ &= U(\tilde{\mathbf{d}}) + \Delta \\ &> U(\tilde{\mathbf{d}}) \text{ since } \Delta > 0. \end{aligned}$$

■

From Lemmas 2.2 and 2.3, the following theorem which yields the optimum point, $\mathbf{d}^*$, can be obtained.

Theorem 2.1: Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$, $m \leq NK$ and $\lambda_i < 0$, $i > m$. The objective function in (9) subject to (10) is maximized for $\mathbf{d} = \mathbf{d}^* = [d_i^*]_{1 \leq i \leq NK}$ such that $d_1^* = \sqrt{P_{\rm tot}}$ and $d_i^* = 0$, $i = 2, 3, \cdots, NK$.

Proof: From Lemma 2.2, $d_i^* = 0$, $\forall\ i > m$. Let $\tilde{\mathbf{d}} = \left[\tilde{d}_i\right]_{1 \leq i \leq m}$ such that $\tilde{d}_i > 0$, $1 \leq i \leq m$ and $\sum_{i=1}^m \tilde{d}_i = P_{\rm tot}$, according to Lemma 2.3. Therefore,

$$U(\tilde{\mathbf{d}}) = \sum_{i=1}^{m} \lambda_i \tilde{d}_i^2 \leq \sum_{i=1}^{m} \lambda_1 \tilde{d}_i^2 = \lambda_1 P_{\rm tot} = \lambda_1 \left(d_1^*\right)^2 = U(\mathbf{d}^*).$$

■

Since $\mathbf{d}^H\mathbf{d} = \mathbf{e}^H\mathbf{e}$, the malicious attacker transmits on all the channels such that (5) is met with equality. The optimal vector, $\mathbf{e}^*$ that solves (4) subject to (5) can be obtained from (6) with $\mathbf{d}$ replaced by $\mathbf{d}^*$. The following theorem characterizes $\mathbf{e}^*$.

Theorem 2.2: Let $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_m > 0$, $m \leq NK$. Let the eigen-vector of $\mathbf{A}$ corresponding to λ_1 be $\mathbf{x}_1 = [x_{i1}]_{1 \leq i \leq NK}$. Then $\mathbf{e}^* = \sqrt{P_{\text{tot}}}\mathbf{x}_1$ and the optimal power on the i^{th} channel, $P_i^* = P_{\text{tot}} |x_{i1}|^2$.

Proof: From (6), $\mathbf{e}^* = \mathbf{P}\mathbf{d}^*$. Since $d_1^* = \sqrt{P_{\text{tot}}}$ and $d_i^* = 0$, $2 \leq i \leq NK$ from Theorem 2.1, $\mathbf{e}^* = d_1^*\mathbf{x}_1 = \sqrt{P_{\text{tot}}}\mathbf{x}_1$. Since $P_i^* = |E_i^*|^2$, $P_i^* = P_{\text{tot}} |x_{i1}|^2$ (resulting in $P_i^* \geq 0$, $\forall i$ and $\sum_{i=1}^{NK} P_i = P_{\text{tot}}$, i.e., feasible transmit powers on all the fragments). ■

It is noted that in general, x_{i1} can be non-zero, $\forall\, i$ and hence, the malicious attacker transmits non-zero powers on all the fragments to create maximum leakage.

In the case of aggregation or bonding with no fragmentation, a similar scenario arises, which is explained as follows. Let the system contain N channels and let channels m and n be aggregated to result in $N-1$ channels in the system. Let m^* denote the new channel obtained by aggregating channels m and n. The channel, m^* need not be orthogonal to the other channels in the system and this, in turn can cause leakage into other channels. Similarly transmission on other channels can cause leakage into m^*. The analysis described in this paper can then be used to determine the transmit power of the attacker on each channel.

Let $\tilde{N}$ be the white noise on all the channels in the absence of the leakage due to the transmission by the malicious attacker. Let the signal power on the i^{th} fragment be S_i. The signal-to-noise-ratio (SNR) on the i^{th} fragment, γ_i, is then given by $\gamma_i = \frac{S_i}{\tilde{N}}$. In the presence of leakage due to transmission by a malicious attacker, the signal-to-interference-noise-ratio (SINR) on the i^{th} fragment, $\hat{\gamma}_i$, can be written as $\hat{\gamma}_i = \frac{S_i}{l_i^2 + \tilde{N}}$, where $l_i = \sum_{j=1}^{NK} C_{ij} e_j^*$. Note that $\hat{\gamma}_i < \gamma_i$, thus resulting in a degraded signal quality. For a channel with bandwidth, B, This degradation can result in a degradation in the channel capacity by an amount, $B \log_2 \left(\frac{1+\gamma_i}{1+\hat{\gamma}_i}\right)$.

It is noted that jamming a particular channel also causes loss of capacity. However, fragmentation causes a larger threat because a malicious attacker can transmit on channel j to cause a loss of capacity on channel i. This kind of an attack is a result of fragmentation and aggregation because of loss of orthogonality between the fragments. Hence, the service disruption caused by the malicious attacker as a consequence of fragmentation and aggregation, is a cognitive service disruption where the attacker intelligently transmits powers on the channels to disrupt service on the other channels.

III. Results and Discussion

We consider two systems, one with $N = 3$ orthogonal channels (like the IEEE 802.22), each with bandwidth, 20 MHz, fragmented into $K = 3$ fragments, each with bandwidth, 6.66 MHz, thus resulting in $NK = 9$ fragments in the system. We also study a system with $N = 13$ orthogonal channels each fragmented into $K = 3$ fragments, to result in $NK = 39$ fragments in the system. We first consider a fixed value of P_{tot} and compute the optimal transmit powers on all the channels in the system with $NK = 9$ fragments. We then vary the total power that can be transmitted by the malicious attacker, P_{tot}, and study the average loss in the capacity due to leakage. The optimal transmit power of the malicious attacker hence, the leakage on each channel, is obtained using the analysis described in Section II. The covariance matrix, $\mathbf{C}$ is generated using the standard inner product of the carrier frequencies [15].

TABLE I
TRANSMIT POWERS FOR THE MALICIOUS ATTACKER WITH $P_{\text{tot}} = 10$ WATTS, ON EACH FRAGMENT IN A SYSTEM WITH $N = 3$ ORTHOGONAL CHANNELS EACH FRAGMENTED INTO $K = 3$ FRAGMENTS.

Fragment	Power (P_i)
1	235 mW
2	945 mW
3	133.6 mW
4	1.536 Watts
5	430.8 mW
6	673.7 mW
7	2.374 Watts
8	3.397 Watts
9	274.7 mW

Table I presents the transmit powers on all the fragments for a malicious attacker with $P_{\text{tot}} = 10$ Watts in a system with $N = 3$ orthogonal channels, each fragmented into $K = 3$ fragments, thus resulting in $NK = 9$ fragments. It is observed that the transmit powers on all the fragments are non-zero, as argued in Section II. It is observed from Table I, that a small transmit power on any fragment (e.g., 133 mW in fragment 3) can also result in maximum leakage on that fragment when combined with a larger transmit power on another fragment (e.g., 3.4 Watts in fragment 8). This reinforces the argument presented in Section I about cognitive service disruption resulting as a consequence of fragmentation. The average loss in the capacity was found to be 20 Kbps.

We vary the total transmit power, P_{tot}, and determine the average loss in capacity. Fig. 2 presents the average loss in the capacity in a system with $N = 3$ orthogonal channels each fragments into $K = 3$ fragments, thus resulting in $NK = 9$ fragments. It is observed that the loss in capacity is negligible for low values of the total transmit power, P_{tot}, where as, for large values of P_{tot}, the loss is significant. The loss in capacity can be as large as 200 Kbps, which, for a system supporting 1-2 Mbps, is a loss of about 16%. The average loss is larger in the system with $N = 13$ orthogonal channels fragmented into $K = 3$ fragments (which typically supports 54 Mbps [4]), resulting in $NK = 39$ fragments, as observed from Fig. 3. Here, loss of the order of up to 9 Mbps is observed. In a system supporting 54 Mbps traffic, this corresponds to a loss in capacity by 11%. The larger loss in capacity is caused due to that fact that there are larger number of fragments and hence, correlations between multiple pairs of fragments. This enables the attacker to transmit in more fragments and cause service disruption.

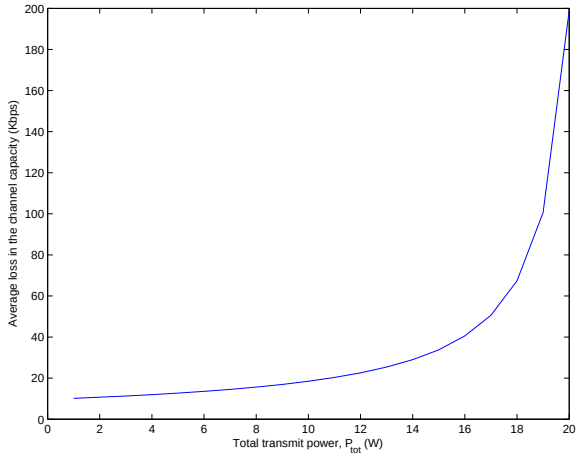

Fig. 2. Average loss in the capacity of due to cognitive disruption in a system with $N = 3$ orthogonal channels each fragmented into $K = 3$ fragments.

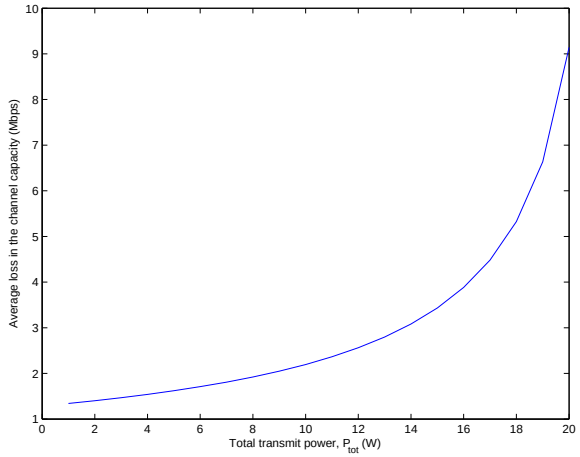

Fig. 3. Average loss in the capacity of due to cognitive disruption in a system with $N = 13$ orthogonal channels each fragmented into $K = 3$ fragments.

IV. Conclusion

We presented the first discussion and analysis on a unique cognitive service disruption threat in IEEE 802.22 based DSA networks, arising as a consequence of channel fragmentation. We presented an experimental result to motivate the problem and presented an analysis to determine the transmit power of the malicious attacker to create maximum service disruption. Numerical results indicate that small transmit powers on a fragment can cause significant loss in capacity when combined with larger transmit powers on other fragments. It was also observed that fragmentation could result in loss of capacity of up to 16%. Mitigation of such threats is under investigation and is also a topic for further research.

References

[1] 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*, Oct. 2005.

[2] J. Mitola, *Cognitive Radio: An integrated agent architecture for software defined radio*. Ph.D. Dissertation, Swedish Royal Institute of Technology, 2000.

[3] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "Ieee 802.22: The first worldwide wireless standard based on cognitive radios," *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2005*, pp. 328–337, Nov. 2005.

[4] "IEEE draft standard for information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Part 22.1: Standard to enhance harmful interference protection for low power licensed devices operating in the TV broadcast bands," Feb. 2009.

[5] S. Sengupta, S. Brahma, M. Chatterjee, and N. S. Shankar, "Enhancements to cognitive radio based IEEE 802.22 air interface," *Proc. IEEE Intl. Conf. on Commun. (ICC'2007)*, pp. 5155–5160, Jun. 2007.

[6] H. Song and X. Lin, "A novel DSA driven MAC protocol for cognitive radio networks," *Wireless Sensor Networks*, vol. 61, no. 2, pp. 112–121, Feb. 2009.

[7] P. Bahl, R. Chandra, T. Moscibroda, R. Murthy, and M. Welsh, "White space networking withWi-Fi like connectivity," *Proc., SIGCOMM'2009*, Aug. 2009.

[8] S. Deb, V. Srinivasan, and R. Maheshwari, "Dynamic spectrum access in DTV white spaces: Design rules, architecture and algorithms," *Proc., ACM Intl. Conf. on Mobile Computing and Networking (ICMC('2009)*, Sep. 2009.

[9] E. Coffman, P. Robert, F. Simatos, S. Tarumi, and G. Zussman, "Channel fragmentation in dynamic spectrum access systems: A theoretical study," *ACM SIGMETRICS Perf. Eval. review*, vol. 38, no. 1, pp. 333–344, Jun. 2010.

[10] J. Geier, *Designing and Deploying 802.11n Wireless Networks*. Cisco Press, 2007.

[11] S. Sengupta, K. Hong, R. Chandramouli, and K. P. Subbalakshmi, "Spiderradio: A cognitive radio network with commodity hardware and open source software," *To appear in IEEE Commun. Mag.*, 2010.

[12] T. Basar, "A Gaussian test channel with an intelligent jammer," *IEEE Trans. on Info. Theory*, vol. 29, no. 1, pp. 152–157, Jan. 1983.

[13] A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao, "Multi-channel jamming attacks using cognitive radios," *Proc. IEEE Intl. Conf. on Computer Commun. and Networking (ICCCN'2007)*, Aug. 2007.

[14] S. Anand, S. Sengupta, and R. Chandramouli, "An attack-defense game theoretic analysis of multi-band wireless covert timing networks," *Proc. IEEE Intl. Conf. on Computer Commun. (INFOCOM'2010)*, Mar. 2010.

[15] Y. Shmaliy, *Continuous-time Signals (Signals and Communication Technology*. Springer, 2006.

[16] C. D. Meyer, *Matrix Theory and Applied Linear Algebra*. SIAM, 1972.