

An Attack-Defense Game Theoretic Analysis of Multi-Band Wireless Covert Timing Networks

S. Anand

Department of ECE
Stevens Institute of Technology
Hoboken, NJ 07030
Email: asanthan@stevens.edu

S. Sengupta

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

R. Chandramouli

Department of ECE
Stevens Institute of Technology
Hoboken, NJ 07030
Email: mouli@stevens.edu

Abstract—We discuss malicious interference based denial of service (DoS) attacks in multi-band covert timing networks using an adversarial game theoretic approach. A covert timing network operating on a set of multiple spectrum bands is considered. Each band has an associated utility which represents the critical nature of the covert data transmitted in the band. A malicious attacker wishes to cause a DoS attack by sensing and creating malicious interference on some or all of the bands. The covert timing network deploys camouflaging resources to appropriately defend the spectrum bands. A two tier game theoretic approach is proposed to model this scenario. The first tier of the game is the sensing game in which, the covert timing network determines the amount of camouflaging resources to be deployed in each band and the malicious attacker determines the optimal sensing resources to be deployed in each band. In the second tier of the game, the malicious attacker determines the optimal transmit powers on each spectral band it chooses to attack. We prove the existence of Nash equilibriums for the games. We compare the performance of our proposed game theoretic mechanism with that of other well known heuristic mechanisms and demonstrate the effectiveness of the proposed approach.

Index Terms – Tactical covert network, attack, defense, adversarial game, pricing, Nash equilibrium.

I. INTRODUCTION

Covert channels [1] refer to transfer of information in a stealthy manner by hiding the communication as an underlay to another application like voice over internet protocol (VoIP), file transfer protocol (FTP), hyper-text transfer protocol (HTTP), etc. The stealth in data transfer can be achieved by deploying covert storage channels [2], [3] where the transmitter modifies certain bits in the headers of packets or modifies certain data in some memory locations to convey information to the receiver. Another means of covert data transfer is the timing channel [4]-[8] (and the references therein), in which a transmitter transmits covert information by modifying the inter-packet delays of the overlay application. As an example, transmitters could delay overlay packets by an amount of time, t_1 to transmit a covert “one” bit and a time amount, t_0 , to transmit a covert “zero” bit. Depending on the overlay application, the performance of the covert timing channel can be enhanced.

Capacity analysis of covert timing channels is presented in [4], where bounds are provided for the achievable capacity. This was extended by Wang and Lee [5] to include the syn-

chronization overheads. Transfer of covert information using arrival times in queues is presented in [6]. In [7], Wagner and Anantharam consider the exponential service timing channel (ESTC) and compute the zero reliability rate and propose a distance metric to achieve bounds on the probability of error. Additional references on covert timing channels can be found in [8].

A major threat against wireless multi-band covert timing networks is the jamming based denial of service (DoS) attack. In order to effect such a DoS attack, a malicious attacker acts in two steps. In the first step, called the *sensing step*, the attacker senses each band to detect anomalies in the time delays between packets. Upon successful detection of anomalies corresponding to covert communication in a spectrum band, the attacker jams the band in the second step called the *jamming step*. The transmitter and the receiver of the covert timing channel can then switch the frequency of operation. The recent developments in cognitive radio enabled dynamic spectrum access (DSA) networks [9] enables the implementation of such a system. The effectiveness can further be enhanced when, in addition to the flexibility provided by DSA, the other nodes in the covert timing network camouflage the covert timing communication by conducting auxiliary communications.

In order to illustrate this, we present the results of experiments conducted by implementing a cognitive radio prototype based on a software abstraction layer over off-the-shelf IEEE 802.11 a/b/g supported by Atheros hardware chip sets. The details of the test bed implementation can be found in [8]. To illustrate the difference between normal data traffic and covert timing data traffic, we conducted two experiments: (i) standard FTP communication without any underlay covert timing data and (ii) FTP with underlay covert timing traffic. Fig. 1 presents the packet count distribution at various inter-arrival time intervals for a single-transmitter-single-receiver system in the absence of underlay timing channel. It is observed that the packet count resembles a Gaussian distribution. We then introduce the underlay covert timing communication in the testbed and sniff the inter-arrival timing of the packets in the network. In order to effect covert timing communication, packets are transmitted with two distinct inter-packet delays. Fig. 2 presents the packet count distribution in the presence of underlay covert timing communication. Two distinct Gaussian-

like distributions are observed. Thus, it is inferred that sensing the inter-arrival time of the packets in the network can reveal the existence of a covert timing channel in the network.

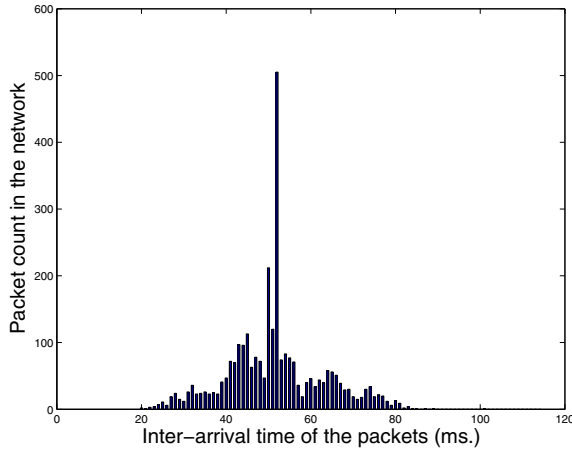


Fig. 1. Packet count distribution for different inter-packet time delays in a single-transmitter-single-receiver system with no underlay covert timing traffic.

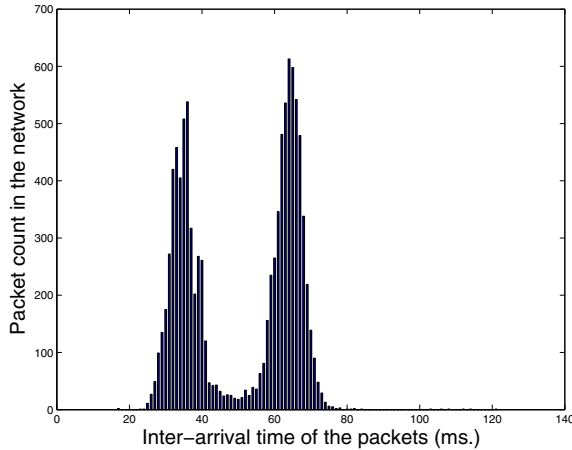


Fig. 2. Packet count distribution for different inter-packet time delays in a single-transmitter-single-receiver system with underlay covert timing traffic.

We then deploy multiple transmitters and receivers communicating in separate spectrum bands (e.g., for the illustration considered here, we use 2.462 GHz and 5.28 GHz bands). One of the transmit-receive pairs share a covert timing channel and the other communications are auxiliary communications to camouflage the timing channel. Fig. 3 presents the distribution of the packet count when 5 camouflaging auxiliary communications are deployed. It is observed that the distribution is similar to the case when no underlay covert timing channel is present. Thus, it is difficult for the attacker to detect the presence of timing anomalies when the covert timing channel is camouflaged by auxiliary communications.

Sarkar *et al* [10] presented an information concealing game to model jamming in multi-band networks, when the attacker has more information about the spectrum bands than the

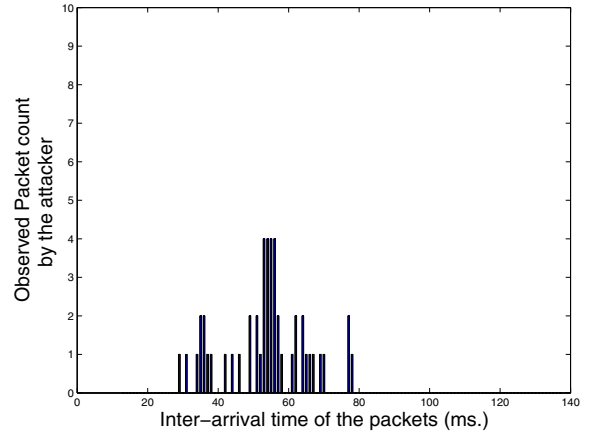


Fig. 3. Packet count distribution for different inter-packet time delays as observed by an attacker in a sensing window of 1 second in the presence of 5 auxiliary communications.

defending nodes. The defending nodes did not have a means of preventing the attacker from learning about the network. In multi-band covert timing networks considered here, the tactical covert network and the attacker have the same information about the spectrum bands. Moreover, the covert timing network can deploy camouflaging resources to prevent the covert communication from being detected by the attacker. In [8], we studied the DoS in DSA based multi-band covert timing networks with a single point of attack. The attacker senses the spectrum bands and the covert timing network deploys camouflaging resources in the form of auxiliary communications in the different spectrum bands. After sensing the spectrum bands, the attacker attacks at most one of the spectrum bands by transmitting spurious signals. This attack-defense scenario was modeled as a two-tier game namely sensing and jamming game.

In this paper, we present the more generalized multi-point attack scenario. We extend our model in [8] to study the problem in which an attacker can jam multiple spectrum bands in the system. We determine the Nash equilibriums of the sensing and jamming games. In the sensing game, the Nash equilibrium is the optimal allocation of the attacker’s sensing resources and the covert timing network’s camouflaging resources in each spectrum band. In the jamming game the Nash equilibrium is the optimal transmit power used by the attacker on each spectrum band and the optimal probability of attacking each spectrum band. We compare the performance of the proposed game theoretic approach with that of other well known heuristics to demonstrate the effectiveness of the proposed mechanism.

While the analysis presented in this paper is valid for any system using multiple spectrum bands, it is particularly applicable to DSA networks. This is because in most networks using multiple spectrum bands, there are network specific policies and policing mechanisms that prevent the kind of attacks discussed in this paper. However, the flexibility provided by DSA (in admitting users from different heterogeneous

networks) inherently prevents the use of network specific policies and hence makes DoS attacks as those discussed in this paper, easier to effect.

The rest of the paper is organized as follows. The system model is presented in Section II. We describe the game theoretic model and the related analysis in Section III. The numerical results are presented in Section IV. Conclusions are drawn in Section V.

II. SYSTEM MODEL

Consider a covert timing working on a set of N bands, specified by $\mathcal{N} = \{1, 2, \dots, N\}$. A malicious agent or an attacker senses some or all of the N spectrum bands and decides to attack a subset \mathcal{A} of size $\hat{S} \leq S \leq N$ bands, specified by $\mathcal{A} = \{i_1, i_2, \dots, i_{\hat{S}}\} \subset \mathcal{N}$. S refers to the maximum number of bands that the attacker can attack. Each spectrum band has a utility associated with it, which indicates the critical nature of the covert timing communication in the band. The network deploys camouflaging resources in some or all of the spectrum bands to protect the underlay covert timing communication in the band. The camouflaging resources could be the amount of time the covert timing network uses auxiliary communications in a frame. Alternatively, the camouflaging resources could also be the number of auxiliary communications assisting the covert communication. Thus, the network can deploy only a finite amount of camouflaging resources. The attacker first senses a subset of the N spectrum bands in order to detect the presence of information. In order to sense the spectrum band, the attacker deploys sensing resources. The sensing resources could be the number of time slots the attacker would spend sensing each spectrum band in a frame and hence, the total sensing resources available to the attacker is finite. Upon sensing the bands, the attacker determines the subset \mathcal{A} of bands which it shall attack. The attacker also determines the optimal power it needs to spend on each band in \mathcal{A} in order to successfully launch an attack.

We model the above scenario as a two-tier game. In the first tier of the game (called the sensing game), the objective is to determine the sensing resource the attacker deploys in each spectrum band and the camouflaging/protective resource the covert timing network deploys on each band. This is done by modeling the sensing game as a zero sum game played by the covert timing network and the attacker. In the second tier of the game (called the jamming game), the objective is to determine the optimal transmit powers the attacker uses on each spectrum band it decides to attack. It is also essential to determine the optimal probabilities with which the attacker chooses to attack each spectrum band. In order to determine the optimal transmit powers and attack probabilities on each band, the jamming game is modeled as a non-zero sum game where the attacker acts as virtual players (one corresponding to each spectrum band in the set \mathcal{A}).

The sensing and jamming stages are decoupled in the analysis. This is because, wireless devices operate in half-duplex mode, i.e., at any instant of time, wireless devices can act as transmitters or receivers but cannot transmit as well as

receive at the same time. Therefore, the malicious attacker, which is a wireless node, can act as a receiver to perform the sensing or act as a transmitter to effect jamming on a spectrum band. Thus, in practice, it would not be possible to couple the sensing and the jamming stages. However, it is of interest to provide a two-tier game framework to model the inter-play between the two stages. We make the following assumptions to carry out the game theoretic analysis.

- The network deploys camouflaging resource M_i in the i^{th} spectrum band, $1 \leq i \leq N$.
- The total camouflaging resources available to the network is M .
- The attacker deploys sensing resource s_i on spectrum band, i .
- The total sensing resources that can be deployed by the attacker is s .

III. GAME THEORETIC ANALYSIS

The covert timing network deploys camouflaging resource, M_i , in band i and the attacker deploys sensing resource, s_i , in band i . After successful sensing, the attacker attacks band i with probability, π_i and power, P_i . We describe the sensing game in Section III-A and the jamming game in Section III-B.

A. Sensing Game

The i^{th} spectrum band has an associated utility, U_i , which denotes the critical nature of the covert timing data transmitted in the i^{th} band. As an example, if there is covert communication on band i , then U_i can be written as [4]

$$U_i = f \left(\ln \left(1 + 2^{\frac{H(q_{j0}) - H(q_{j1})}{q_{j1} + q_{j0} - 1}} \right) + \frac{(1 - q_{j0})H(q_{j1}) - q_{j1}H(q_{j0})}{q_{j1} + q_{j0} - 1} \right), \quad (1)$$

where $H(x)$ is the entropy of the output of a binary symmetric channel (BSC) with bit error rate (BER), x , $f(\alpha)$ is an increasing, concave function of α , q_{j0} is the probability that the j^{th} transmitted bit is received as a “one” when a “zero” is transmitted and q_{j1} is the probability that the j^{th} transmitted bit is received as a “zero” when a “one” is transmitted.

The probability of successful detection of the covert communication in band i depends on the sensing resource, s_i , deployed by the attacker and the camouflaging resource, M_i , deployed by the covert timing network. In order to model the inter-play between s_i , M_i and p_i , we use the dose-response-immunity model [11] which is explained as follows.

Let the ability of a drug to destroy a disease be X_1 and let X_2 denote the immunity parameter of the subject to the drug. Let the event $Y = 0$ denote the survival of a subject when a drug is used on the subject and let the event $Y = 1$ denote the death. Let $\mathbf{X} = [X_1 \ X_2]^T$. Let $\underline{\beta} = [\beta_1 \ -\beta_2]^T$ be the vector of regression parameters. The negative sign for β_2 indicates that the dose and the immunity act against each other. If $\Pr\{Y = 1\} = p = 1 - \Pr\{Y = 0\}$, then, according

to the dose-response-immunity model,

$$\text{logit}(p) = \ln\left(\frac{p}{1-p}\right) = \underline{\beta}^T \mathbf{X}. \quad (2)$$

In the sensing game, the sensing resources are analogous to the dose of the drug and the camouflaging resources are analogous to the immunity. The event $Y = 1$ (death of the subject in the dose-response-immunity model) models the successful detection of covert communication and $Y = 0$ (i. e., survival of the subject) models the failure of the attacker to detect the covert communication in the band. Then, $\mathbf{X} = [\ln(s_i) \ \ln(M_i)]^T$. Hence, from the dose-response-immunity model the probability of successfully detecting the communication in band i , p_i , can be obtained from (2) as

$$p_i = \frac{s_i^{\beta_1}}{s_i^{\beta_1} + M_i^{\beta_2}}. \quad (3)$$

The probability p_i should satisfy the following properties

- 1) When the attacker deploys no sensing resources in a spectrum band, it will be unable to detect the covert communication in the band. Thus, $s_i = 0$ should result in $p_i = 0$.
- 2) When the covert timing network deploys no camouflaging resources in a band, the attacker will be able to detect the presence of covert communication with probability 1. Thus $M_i = 0$ should result in $p_i = 1$.

The expression for p_i in (3) satisfies the properties mentioned above. As an example, let the attacker perform the sensing according to a Poisson process, X_1 , of rate, s_i , in the spectrum band i . Similarly, let the network deploy auxiliary communications at a time X_2 , which is exponentially distributed with rate M_i . The attacker detects the covert communication successfully if the covert network deploys camouflaging resources after the attacker begins to sense. Thus, the sensing resource and camouflaging resources used in a band are the rate at which the attacker senses the band and that at which the network defends the band, respectively. Then the probability that the attacker successfully detects the covert communication in band i , p_i , is $p_i = \Pr\{X_1 < X_2\} = \frac{s_i}{s_i + M_i}$, which can be obtained from (3) when $\beta_1 = \beta_2 = 1$.

In general, the values β_1 and β_2 in (3) denote the attacker's anomaly detection capability and the covert timing network's camouflaging capability, respectively. If the attacker uses more accurate detecting mechanisms, it results in a larger β_1 . Similarly, a covert timing network with better strategies for auxiliary communications represents a higher value of β_2 . The scenario $\beta_1 > \beta_2$ represents a relatively less effective camouflaging capability of the covert timing network compared to the accuracy of the attacker in detecting the timing anomalies. $\beta_1 = \beta_2$ represents equal ability for the attacker and the camouflaging network.

The net utility obtained by the attacker by sensing band i , which is also the net impact experienced by the covert timing

network if the attacker attacks band i , E_i , can be written as

$$E_i = U_i p_i = U_i \left(\frac{s_i^{\beta_1}}{s_i^{\beta_1} + M_i^{\beta_2}} \right). \quad (4)$$

The expected impact on the covert timing network can then be written as

$$E = \sum_{i \in \mathcal{A}} E_i = \sum_{i \in \mathcal{A}} U_i \left(\frac{s_i^{\beta_1}}{s_i^{\beta_1} + M_i^{\beta_2}} \right). \quad (5)$$

The strategy for the covert timing network is the vector, $\mathbf{M} = [M_1 \ M_2 \ M_3 \ \cdots \ M_N]^T$ and that for the attacker is the vector, $\mathbf{s} = [s_1 \ s_2 \ s_3 \ \cdots \ s_N]^T$. Note that the values of s_i are zero for $i \notin \mathcal{A}$.

The optimal strategy of the attacker is the vector \mathbf{s} that solves the optimization problem

$$\max_{\mathbf{s}, \mathcal{A} \subset \mathcal{N}} \sum_{i \in \mathcal{A}} U_i \left(\frac{s_i^{\beta_1}}{s_i^{\beta_1} + M_i^{\beta_2}} \right), \quad (6)$$

subject to the constraints

$$\sum_{i \in \mathcal{N}} s_i \leq s. \quad (7)$$

The utility for the covert timing network is the negative of that of the attacker because the covert timing network loses in the form of impact, whatever the attacker gains as utility by jamming band i . Thus, the optimal strategy for the covert timing network can be determined by solving the optimization problem

$$\min_{\mathbf{M}} \max_{\mathbf{s}, \mathcal{A} \subset \mathcal{N}} \sum_{i \in \mathcal{A}} U_i \left(\frac{s_i^{\beta_1}}{s_i^{\beta_1} + M_i^{\beta_2}} \right), \quad (8)$$

subject to the constraints,

$$\sum_i M_i \leq M. \quad (9)$$

Lemma 3.1: The attacker obtains maximum utility only when it uses all the sensing resources, i. e., constraint (7) is met with equality.

Proof: Consider a strategy $\tilde{\mathbf{s}} = [\tilde{s}_1 \ \tilde{s}_2 \ \tilde{s}_3 \ \cdots \ \tilde{s}_N]$, where for any chosen subset $\mathcal{A} \subset \mathcal{N}$ of size S , $\tilde{\mathbf{s}} = \sum_{i \in \mathcal{A}} \tilde{s}_i < s$. Let $\phi = s - \tilde{\mathbf{s}}$. Note that $\phi > 0$. Let the utility obtained by the attacker under strategy $\tilde{\mathbf{s}}$ be \tilde{U} . Consider the strategy $\hat{\mathbf{s}} = [\hat{s}_1 \ \hat{s}_2 \ \hat{s}_3 \ \cdots \ \hat{s}_N]$, where, for any subset $\mathcal{A} \subset \mathcal{N}$ of size S , $\hat{s}_i = \tilde{s}_i + \frac{\phi}{S}$, $\forall i \in \mathcal{A}$. Note that $\sum_{i \in \mathcal{A}} \hat{s}_i = s$ and $\hat{s}_i > \tilde{s}_i$, $\forall i$ and hence,

$$\sum_{i \in \mathcal{A}} U_i \left(\frac{\hat{s}_i^{\beta_1}}{\hat{s}_i^{\beta_1} + M_i^{\beta_2}} \right) > \sum_{i \in \mathcal{A}} U_i \left(\frac{\tilde{s}_i^{\beta_1}}{\tilde{s}_i^{\beta_1} + M_i^{\beta_2}} \right).$$

Thus, $\tilde{\mathbf{s}}$ is a sub-optimal strategy. □

Theorem 3.1: If $\exists \hat{\mathcal{A}} \subset \mathcal{N}$ such that $\forall i \in \hat{\mathcal{A}}, E_i > \sum_{k \in \bar{\mathcal{A}}} U_k^1$, $\bar{\mathcal{A}} \triangleq \mathcal{N} \setminus \hat{\mathcal{A}}$, $|\bar{\mathcal{A}}| \leq S$, then the attacker's optimal strategy is $s_k = 0, \forall k \in \bar{\mathcal{A}}$.

Proof: Let the attacker deploy a strategy $\tilde{\mathbf{s}} = [\tilde{s}_1 \ \tilde{s}_2 \ \tilde{s}_3 \ \cdots \ \tilde{s}_N]^T$ where $\tilde{s}_k > 0, k \in \bar{\mathcal{A}}$. Let $\tilde{s} \triangleq \sum_{k \in \bar{\mathcal{A}}} \tilde{s}_k$. The utility obtained by the attacker under this strategy is

$$\begin{aligned} \tilde{U} &= \sum_{i \in \hat{\mathcal{A}}} \tilde{E}_i + \sum_{k \in \bar{\mathcal{A}}} \tilde{E}_k \\ &\leq \sum_{i \in \hat{\mathcal{A}}} \tilde{E}_i + \sum_{k \in \bar{\mathcal{A}}} U_k. \end{aligned} \quad (10)$$

Consider the strategy, $\hat{\mathbf{s}} = [\hat{s}_1 \ \hat{s}_2 \ \hat{s}_3 \ \cdots \ \hat{s}_N]^T$ where $\hat{s}_k = 0 \ \forall k \in \bar{\mathcal{A}}$ for some $i' \in \hat{\mathcal{A}}, \hat{s}_i = \tilde{s}_i + \tilde{s}$ and $\forall i \in \hat{\mathcal{A}}, i \neq i', \hat{s}_i = \tilde{s}_i$. Thus the attacker deploys all its sensing resources and hence, obeys Lemma 3.1. Let the impact on band i according to this strategy be \hat{E}_i . Note that $\hat{E}_i = \tilde{E}_i, \forall i \in \hat{\mathcal{A}}, i \neq i'$ and $\hat{E}_{i'} > \tilde{E}_{i'}$. The utility obtained by the attacker for this strategy is

$$\begin{aligned} \hat{U} &= \sum_{\substack{i \in \hat{\mathcal{A}} \\ i \neq i'}} \hat{E}_i + E_{i'} \\ &> \sum_{\substack{i \in \hat{\mathcal{A}} \\ i \neq i'}} \tilde{E}_i + \sum_{k \in \bar{\mathcal{A}}} U_k \\ &> \tilde{U}. \end{aligned} \quad (11)$$

In the above, the second step follows from the hypothesis while the third follows from (10). Thus $\tilde{\mathbf{s}}$ is a sub-optimal strategy for the attacker. \square

Each spectrum band in $\hat{\mathcal{A}}$ specified in Theorem 3.1 represents a spectrum band whose impact is much larger than the sum of the utilities of another set of bands. Thus, the set of bands in $\hat{\mathcal{A}}$ denote a set of bands with highly critical covert communication. These bands thus form the critical bands of the covert timing network. Theorem 3.1 then signifies the fact that the attacker perceives more benefits by deploying all its sensing resources on critical spectrum bands instead of distributing them over all the bands.

Following the argument provided in the proof of Lemma 3.1, the following lemma can be obtained.

Lemma 3.2: The covert timing network perceives minimum impact only when it deploys all its camouflaging resources, i. e., constraint (9) is met with equality.

Proof: Consider a strategy $\tilde{\mathbf{M}} = [\tilde{M}_1 \ \tilde{M}_2 \ \tilde{M}_3 \ \cdots \ \tilde{M}_N]$, where for any chosen subset $\tilde{M} = \sum \tilde{M}_i < s$. Let $\chi = s - \tilde{M}$. Note that $\chi > 0$. Let the utility obtained by the attacker under strategy $\tilde{\mathbf{M}}$ be \tilde{U} . Consider the strategy $\hat{\mathbf{M}} = [\hat{M}_1 \ \hat{M}_2 \ \hat{M}_3 \ \cdots \ \hat{M}_N]$, where, $\hat{M}_i = \tilde{M}_i + \frac{\chi}{N}$. Note that $\sum \hat{M}_i = s$ and $\hat{M}_i > \tilde{M}_i, \forall i$ and hence,

$$\max_{\mathbf{s}} \sum_{i \in \hat{\mathcal{A}}} U_i \left(\frac{s_i^{\beta_1}}{s_i^{\beta_1} + \hat{M}_i^{\beta_2}} \right) < \max_{\mathbf{s}} \sum_{i \in \hat{\mathcal{A}}} U_i \left(\frac{s_i^{\beta_1}}{s_i^{\beta_1} + \tilde{M}_i^{\beta_2}} \right).$$

¹It is noted that it is possible that the set $\bar{\mathcal{A}}$ is empty. In this case, $s_i > 0, \forall i$.

Thus, $\tilde{\mathbf{M}}$ is a sub-optimal strategy for the network. \square

Theorem 3.2: Let $\hat{\mathcal{A}}$ and $\bar{\mathcal{A}}$ be as defined in Theorem 3.1. Then, the optimal strategy for the covert timing network results in $M_k = 0 \ \forall k \in \bar{\mathcal{A}}$.

Proof: : The proof follows by applying Lemma 3.2 and is identical to the proof of Lemma 1 in [8]. \square

Theorem 3.2 implies that the network must also deploy camouflaging resources only on the critical spectrum bands. After identifying the set of bands that need to be camouflaged by the covert timing network and sensed by the attacker, it is essential to determine the optimal allocation of the sensing and camouflaging resources among the bands in the set $\hat{\mathcal{A}}$. Theorem 3.3 below provides the relation between the sensing and jamming resource deployed in each band in $\hat{\mathcal{A}}$.

Theorem 3.3: The equilibrium for the zero-sum sensing game occurs when $\frac{s_i}{M_i} = \frac{s}{M}, \forall i \in \hat{\mathcal{A}}$.

Proof: Let the equilibrium strategies be $\underline{\mathbf{s}} = [s_i]_{i \in \hat{\mathcal{A}}}$ and $\underline{\mathbf{M}} = [M_i]_{i \in \hat{\mathcal{A}}}$ for the attacker and the network, respectively. Thus $\underline{\mathbf{s}}$ is a solution to the optimization problem (6) subject to the constraints (7) with $\mathbf{M} = \underline{\mathbf{M}}$. Similarly, $\underline{\mathbf{M}}$ is a solution to the optimization problem (8) subject to the constraints (9) with $\mathbf{s} = \underline{\mathbf{s}}$. From Lemmas 3.1 and 3.2, constraints (7) and (9) are met with equality. Thus, writing the Lagrangian for the equality constrained optimization problem specified by (6) and (7) and applying the first order necessary conditions, we obtain

$$\left(\frac{s_i^{\beta_1} + M_i^{\beta_2}}{s_j^{\beta_1} + M_j^{\beta_2}} \right)^2 = \frac{M_i^{\beta_2} s_i^{\beta_1 - 1}}{M_j^{\beta_2} s_j^{\beta_1 - 1}}, \quad (12)$$

$\forall i, j \in \hat{\mathcal{A}}$. Similarly, writing the Lagrangian for the equality constrained optimization problem specified by (8) and (9) and applying the first order necessary conditions,

$$\left(\frac{s_i^{\beta_1} + M_i^{\beta_2}}{s_j^{\beta_1} + M_j^{\beta_2}} \right)^2 = \frac{M_i^{\beta_2 - 1} s_i^{\beta_1}}{M_j^{\beta_2 - 1} s_j^{\beta_1}}, \quad (13)$$

$\forall i, j \in \hat{\mathcal{A}}$. From (12) and (13),

$$\frac{s_i}{M_i} = \frac{s_j}{M_j}, \quad (14)$$

$\forall i, j \in \hat{\mathcal{A}}$. Applying the constraints (7) and (9) and Lemmas 3.1 and 3.2 to (14), $\frac{s_i}{M_i} = \frac{s}{M}, \forall i \in \hat{\mathcal{A}}$. \square

Theorem 3.3 provides a means for adjusting the sensing and camouflaging resources according to the varying utilities. In other words, if the utility of a particular band changes, then the sensing and camouflaging resources for that band are both scaled by the same factor to obtain a new equilibrium point.

B. Jamming Game

After sensing the spectrum bands and forming the subset $\hat{\mathcal{A}}$ of bands which the attacker decides to attack, the objective of the jamming game is to determine the optimal transmit powers on each spectrum band in order to successfully jam the band. In order to formulate the jamming game, we list the following details which we consider about the system, in addition to those mentioned in Section II.

- The attacker attacks band i with probability π_i and transmit power, P_i .
- The attacker can spend a total power, P_{tot} , in order to attack the spectrum bands.
- In the i^{th} spectrum band, there is one intended and $n - 1$ camouflaging transmitters corresponding to a receiver. The channel gain vector $\mathbf{h}_i = [h_{i1} \ h_{i2} \ h_{i3} \ \dots \ h_{in}]^T$, where h_{i1} denotes the gain from the intended transmitter and $h_{i2} \dots h_{in}$ denote the gain from the camouflaging transmitters.
- The gain from the attacker to the receiver is \hat{h}_{i1} .
- The channel noise is additive white Gaussian noise (AWGN) with noise power, \mathcal{W} .
- The intended transmitter on the i^{th} band transmits with power e_{i1} and the camouflaging transmitters transmit with powers, $e_{i2}, e_{i3}, \dots, e_{in}$.
- The SIR on the i^{th} band perceived at the receiver of the covert timing communication due to the intended transmitter of the covert timing communication is τ_i and that at the receiver of the covert timing communication due to the attacker's transmission is γ_i .

Successful jamming takes place when the attacker transmits at power P_i on band i such that it results in $\gamma_i > \tau_i$ [12]. From the definition of SIR in wireless networks [13], τ_i and γ_i can be written as

$$\tau_i = \frac{e_{i1}h_{i1}}{\mathcal{W} + \sum_{j \neq 1} e_{ij}h_{ij}} \quad (15)$$

$$\gamma_i = \frac{P_i \hat{h}_{i1}}{\mathcal{W} + \sum_{j \neq 1} e_{ij}h_{ij}}. \quad (16)$$

The jamming problem can be formulated as a non-cooperative game between S virtual players. The strategy chosen by each player is the power transmitted and the probability of attack on each band. It is essential to define a utility function which should be an increasing concave function of the strategy [14]. In order to limit the transmit power applied by the attacker on each band, we also propose a penalty function which is an increasing function of the transmit power and the probability of attacking the band. With all these considerations, we define the following net utility function, U_i^{net} , in the i^{th} band to be

$$U_i^{net} = a \ln(1 + \pi_i E_i) + \lambda u(\gamma_i - \tau_i) \ln(\gamma_i - \tau_i) - \mu P_i \pi_i, \quad (17)$$

where E_i is given by (4), $u(y)$ is the modified unit step function, i. e.,

$$u(y) = \begin{cases} 1 & y > 0 \\ 0 & y \leq 0, \end{cases} \quad (18)$$

$a > 0$ and $\lambda > 0$ are utility parameters and $\mu > 0$ is the pricing parameter. The expression for the net utility, U_i^{net} in (17) is derived based on the following considerations.

- 1) The attacker can jam band i successfully only when $\gamma_i > \tau_i$.
- 2) The attacker should obtain larger utility when the SIR, γ_i is greater than τ_i by a larger margin, i. e., the information received from the attacker is much larger than that received from the transmitter.
- 3) The utility should increase when the impact created on the network increases and when the probability of attacking the critical band is larger.
- 4) The penalty for transmitting higher power should be more and that for attacking a band with higher probability should be more.

It is noted that the magnitude of λ should be very small. This is to assure that the attacker does not have much incentive in transmitting exorbitantly large power. Also, the magnitude of μ should be very large so that the penalty for transmitting larger powers is large.

With the above considerations, the Nash equilibrium strategy for the jamming game can be obtained as the solution to the following optimization problem

$$\max_{\mathbf{P}, \boldsymbol{\pi}} \sum_{i \in \hat{\mathcal{A}}} U_i^{net} = \max_{\mathbf{P}, \boldsymbol{\pi}} \sum_{i \in \hat{\mathcal{A}}} a \ln(1 + \pi_i E_i) + \lambda u(\gamma_i - \tau_i) \ln(\gamma_i - \tau_i) - \mu P_i \pi_i, \quad (19)$$

subject to the constraints

$$\sum_{i \in \hat{\mathcal{A}}} P_i \leq P_{tot}, \quad (20)$$

$$\sum_{i \in \hat{\mathcal{A}}} \pi_i \leq 1 \quad (21)$$

and

$$\begin{aligned} P_i &\geq 0 \quad \forall i \\ \pi_i &\geq 0 \quad \forall i. \end{aligned} \quad (22)$$

In (19), $\mathbf{P} = [P_i]_{i \in \hat{\mathcal{A}}}$ and $\boldsymbol{\pi} = [\pi_i]_{i \in \hat{\mathcal{A}}}$.

The following theorem provides a sufficient condition for existence of a Nash equilibrium for the jamming game specified by the optimization problem (19) subject to the constraints (20)-(22).

Theorem 3.4: Let $\epsilon_i \triangleq \gamma_i - \tau_i$ and

$$\hat{\mu}_{max} \triangleq \min_{i \in \hat{\mathcal{A}}} \left(\frac{\sqrt{\lambda a}}{\epsilon_i} \right) \left(\frac{\tau_i}{e_{i1}} \right) \left(\frac{E_i}{1 + E_i} \right). \quad (23)$$

If $\mu < \hat{\mu}_{max}$, then a unique Nash equilibrium exists for the jamming game specified by the optimization problem (19).

Proof: The objective function for the jamming game is U_i^{net} specified by (17). The Hessian matrix for each term in the objective function, \mathcal{H} , is given by

$$\mathcal{H} = \begin{bmatrix} \frac{\partial^2 U_i^{net}}{\partial P_i^2} & \frac{\partial^2 U_i^{net}}{\partial P_i \partial \pi_i} \\ \frac{\partial^2 U_i^{net}}{\partial \pi_i \partial P_i} & \frac{\partial^2 U_i^{net}}{\partial \pi_i^2} \end{bmatrix}, \quad (24)$$

which, from (17), can be obtained as

$$\mathcal{H} = \begin{bmatrix} -\frac{\lambda}{(\gamma_i - \tau_i)^2} \left(\frac{\gamma_i}{P_i}\right)^2 & -\mu \\ -\mu & -\frac{aE_i^2}{(1 + \pi_i E_i)^2} \end{bmatrix}. \quad (25)$$

From the above, the determinant of the Hessian matrix can be written as

$$\det(\mathcal{H}) = \left(\frac{\lambda a}{\epsilon_i^2}\right) \left(\frac{\tau_i}{e_{i1}}\right)^2 \left[\frac{E_i}{1 + \pi_i E_i}\right]^2 - \mu^2, \quad (26)$$

which is positive if $\mu < \hat{\mu}_{max}$ specified in (23). Note from (25) that the trace of \mathcal{H} is negative. Thus, when $\mu < \hat{\mu}_{max}$, the Hessian matrix \mathcal{H} is negative definite, and hence U_i^{net} (and, in turn, $\sum_{i \in \hat{\mathcal{A}}} U_i^{net}$) is a concave function. Hence, the optimization problem specified by (19) has a unique Nash equilibrium [14].

□

Corollary 3.1: When $\epsilon_i \rightarrow 0$, $\forall i$, the jamming game has a unique Nash equilibrium.

Proof: When $\epsilon_i \rightarrow 0$, $\hat{\mu}_{max} \rightarrow \infty$ and the condition $\mu < \hat{\mu}_{max}$ in Theorem 3.4 is satisfied. This results in a unique Nash equilibrium.

□

Although the condition in Theorem 3.4 provides an upper bound on μ to result in a Nash equilibrium, it still does not ensure that the Nash equilibrium thus determined satisfies the constraints (20)-(22). The following theorem provides another upper bound and a lower bound on μ that determines the value of the unique Nash equilibrium that satisfies the constraints (20)-(22).

Theorem 3.5: Let $\epsilon_i = \epsilon$, $\forall i$ and let $\epsilon \rightarrow 0$. Let

$$\mu_{max} \triangleq \min_{i \in \hat{\mathcal{A}}} \frac{a \hat{h}_{i1} E_i}{e_{i1} h_{i1}} \quad (27)$$

and

$$\mu_{min} \triangleq \frac{a \sum_{i \in \hat{\mathcal{A}}} \frac{\hat{h}_{i1}}{e_{i1} h_{i1}}}{1 + \sum_{i \in \hat{\mathcal{A}}} \frac{1}{E_i}}. \quad (28)$$

Then $\forall \mu \in (\mu_{min}, \mu_{max})$, there exists a unique Nash equilibrium for the jamming game that satisfies the constraints (20)-(22).

Proof: The Lagrangian, \mathcal{L} , for the constrained optimization problem (19) subject to the constraints (20)-(22) can be written as²

$$\mathcal{L} = \sum_i a \ln(1 + \pi_i E_i) + \sum_i \lambda \ln(\gamma_i - \tau_i) + \sum_i \mu P_i \pi_i - \nu_1 (\alpha^2 - P + \sum_i P_i) - \nu_2 (\beta^2 - 1 + \sum_i \pi_i), \quad (29)$$

where ν_1 and ν_2 are the Lagrangian variables corresponding to the constraints and α , β are slack variables to account for the

²In (29), \sum_i indicates $\sum_{i \in \hat{\mathcal{A}}}$. We omit this detail in (29) for simplicity.

inequality in the constraints. According to the Karush-Kuhn-Tucker (KKT) conditions [15], it is essential to equate the partial derivatives of \mathcal{L} with respect to P_i , π_i , ν_1 , ν_2 , α and β to zero in order to determine the Nash equilibrium.

The condition $\epsilon_i = \epsilon \rightarrow 0$, $\forall i$ yields

$$P_i = \frac{e_i h_{i1}}{\hat{h}_{i1}}. \quad (30)$$

The value of P_i obtained above satisfies $P_i > 0$ in (22). In order to satisfy (20), only those bands, $i \in \hat{\mathcal{A}}$ are chosen that satisfy

$$\sum_i \frac{e_i h_{i1}}{\hat{h}_{i1}} < P. \quad (31)$$

In order to maximize the number of bands that can be attacked and minimize the total transmit power of the attacker, the attacker chooses the bands with the smallest values of $\frac{e_i h_{i1}}{\hat{h}_{i1}}$ such that (31) is satisfied. Note that the choice of P_i that satisfies (31), also satisfies (20) with inequality and hence, $\nu_1 = 0$. The condition in Theorem 3.4 results in $\nu_2 = 0$. Thus, equating the partial derivative of \mathcal{L} with respect to π to zero, using the fact that $\nu_1 = \nu_2 = 0$ and using the expression for P_i in (30), we obtain the optimal π_i as

$$\pi_i = \frac{a \hat{h}_{i1}}{\mu e_{i1} h_{i1}} - \frac{1}{E_i}. \quad (32)$$

When $\mu < \mu_{max}$ specified in (27), the constraint $\pi_i > 0$ in (22). The condition $\mu > \mu_{min}$ specified in (28) satisfies the constraint (21). Thus, the Nash equilibrium satisfies the constraints.

□

Remark 1: Since μ is a parameter that can be modified according to the network, one can choose μ that satisfies the condition provided in Theorem 3.5, and thus, obtain a unique Nash equilibrium for the jamming game.

Remark 2: Note that, in order to apply Theorem 3.5, it is essential that for the chosen set of bands $i \in \hat{\mathcal{A}}$ such that μ_{max} in (27) $>$ μ_{min} in (28). It is observed that this is satisfied if only one band is chosen. However, when multiple bands are chosen, it may not be true in general. Then, among the subset of bands chosen to determine the optimal P_i , a smaller subset is chosen which satisfies $\mu_{min} < \mu_{max}$. This gives a means to determine the maximum number of spectrum bands that can be attacked.

Remark 3: Note that π_i increases when $\frac{\hat{h}_{i1}}{h_{i1}}$ increases and e_{i1} and E_i are fixed. This means that the attacker is more likely to attack the band in which it is ‘‘closer’’ to the receiver, than the intended transmitter.

Remark 4: From (30) and (32), it is observed that for two bands with the same impact (E_i), the attacker is more likely to attack the band in which it has to use lesser power.

Remark 5: From (32), it is also observed that between two bands on which the attacker requires the same transmit power, it is more likely to attack the one in which it can create more impact.

IV. RESULTS AND DISCUSSION

We present the numerical results in two parts. The results for the sensing game are first presented in Section IV-A. Later, Section IV-B present the results for the jamming game. We consider the following numerical values in the computations. The network has $N = 25$ spectrum bands [8] and the attacker can attack at most $S = 10$ spectrum bands. The utility on each band is taken to be uniformly distributed in the interval [100, 500].

A. Sensing Game

As mentioned in Section III-A, we apply the dose-response-immunity model to obtain the probability of successfully detecting the covert communication in a spectrum band. We consider equally capable sensing and camouflaging abilities for the attacker and the covert timing network, respectively, i. e., $\beta_1 = \beta_2$. For the numerical computations, we consider $\beta_1 = \beta_2 = 1$. Fig. 4 presents the expected impact on the covert timing network with respect to the total available sensing resources, s , for $M = 150$. In order to compare the proposed game theoretic allocation of the sensing and camouflaging resources, we consider two well known schemes- (i) the equal allocation scheme where the sensing and camouflaging resources are equally divided among all channels and (ii) the adaptive proportional scheme where sensing and camouflaging resources are allocated to the i^{th} band according to the ratio,

$$\frac{U_i}{\sum_k U_k}.$$

From Fig. 4, it is observed that the proposed game theoretic scheme results in lesser average impact on the covert network than the adaptive proportional and the uniform allocation schemes. As an example, for $s = 100$, the expected impact on the covert timing network caused by the proposed scheme is about 1500 while that caused by the adaptive proportional allocation scheme is about 2000 and that caused by the uniform allocation scheme is about 2400. Thus, an improvement of about 25% is achieved over the adaptive proportional allocation scheme and an improvement of about 37.5% is achieved over the uniform allocation scheme. Similar improvements can be observed in Fig. 5, which depicts the results when the total sensing resources, $s = 150$, and the total camouflaging resources, M , is varied.

B. Jamming Game

In order to perform the numerical computations for the jamming game, we generate the channel gain vector, \mathbf{h}_i and the channel gain \hat{h}_{i1} from the attacker, using the Jake's propagation model [16]. We run 100000 Linux based simulation experiments and present the results averaged over these simulation experiments. Fig. 6 presents the average transmit power for the attacker for varying values of the total sensing resources, s , with $M = 150$. As in the sensing game, the performance is compared with that of the adaptive proportional and the equal resource allocation schemes. It is observed that the average transmit power required by the attacker to successfully jam the covert timing network is larger for the proposed game theoretic scheme than that for the adaptive

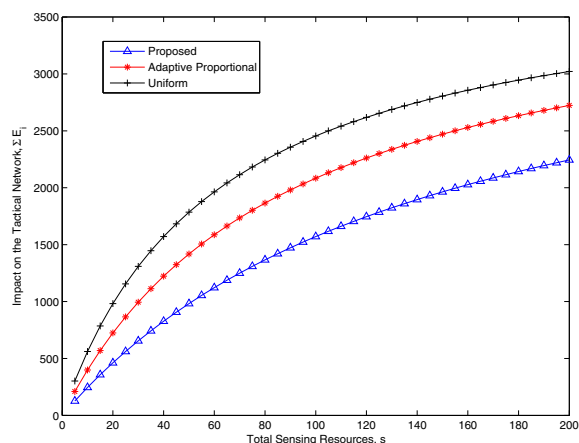


Fig. 4. Expected impact on the covert timing network when $M = 150$ and the utilities are uniformly distributed in [100, 500].

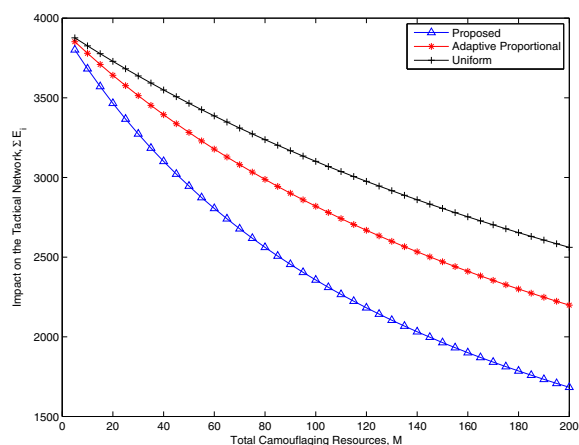


Fig. 5. Expected impact on the covert timing network when the $s = 150$ and the utilities are uniformly distributed in [100, 500].

proportional and the equal resource allocation schemes. As an example, for $s = 100$, the proposed game theoretic scheme requires the attacker to transmit at an average power of about -18.5 dBm while the adaptive proportional scheme results in about -19.5 dBm and the equal allocation scheme results in about -20 dBm. Thus the proposed scheme results in about 20% more average power than that of the adaptive proportional scheme and about 30% additional power compared to the equal allocation scheme. This is because, the conditions required for $\mu_{min} < \mu_{max}$ (mentioned in remark 1 in Section III-B) is satisfied for fewer channels in the adaptive proportional and the equal allocation schemes thus reducing the values of π_i and hence, the average power, $\sum_i P_i \pi_i$. Thus, the proposed scheme not only reduces the impact on the covert timing network but also forces the attacker to use larger average transmit powers. Similar results can be observed for varying M in Fig. 7.

From Figs. 6 and 7, it is observed that the average transmit power decreases with increasing values of the total sensing resources, s , and increases with increasing values of the total

camouflaging resources, M . This is because, when s increases, the impact on the covert timing covert network increases. From (27), μ_{max} increases. This allows larger values of the pricing parameter, μ , which, in turn, forces the attacker to transmit at lower average powers. Similarly, increasing the value of M reduces the impact on the covert timing network on each spectrum band, thus reducing μ_{max} allowing smaller values of μ . This, in turn, results in larger average transmit power for the attacker.

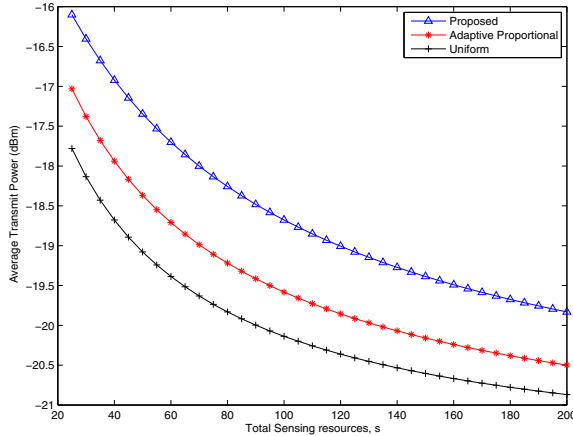


Fig. 6. Average transmit power for the attacker when $M = 150$ and the utilities are uniformly distributed in $[100, 500]$.

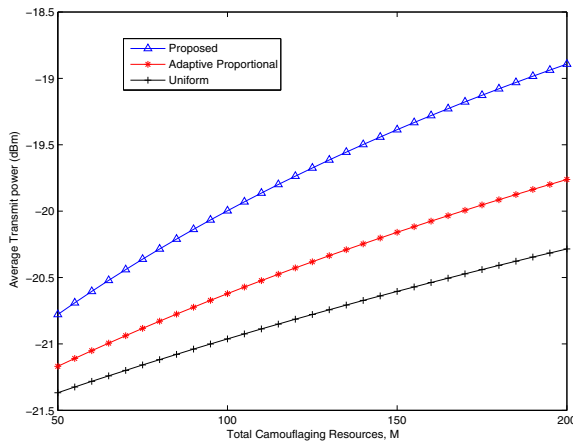


Fig. 7. Average transmit power for the attacker when $s = 150$ and the utilities are uniformly distributed in $[100, 500]$.

V. CONCLUSION

We presented a two tier adversarial game theoretic approach to study malicious interference based DoS attacks in multi-band covert timing networks. Nash equilibrium strategies were obtained for both the tiers of the game. The following key inferences are drawn from the analysis presented in this paper.

- The attacker needs to deploy all its sensing resources only on the critical bands.
- The covert timing network needs to deploy all its camouflaging resources only on the critical bands.

- At the equilibrium point, the ratios between the sensing and the camouflaging resources deployed in all the critical bands are equal.
- Between two bands with equal impact, the attacker is more likely to attack the band in which it is required to transmit at lesser power.
- Between two bands in which it has to transmit equal power, the attacker is more likely to attack the band which perceives higher impact.
- The proposed game theoretic scheme can result in about 25-40% reduced impact on the covert timing network when compared to other well known heuristics.
- The proposed game theoretic scheme results in about 20-30% increased transmit power for the attacker when compared to other well known heuristic schemes.

VI. ACKNOWLEDGEMENT

This research was partially funded by NSF # 0917008 and NSF # 0916180 and partially funded by 2009-92667-NJ-IJ.

REFERENCES

- [1] B. W. Lampson, "A note on the confinement problem," *ACM Commun.*, 1973.
- [2] K. W. Eggers and P. W. Mallett, "Characterizing network covert storage channels," *Fourth Aerospace Comp. Security Appl. Conf.*, Dec. 1988.
- [3] K. G. Lee, A. Savoldi, P. Gubian, K. S. Lim, and S. Lee, "Methodologies for detecting covert database," *Intl. Conf. on Intelligent Info. Hiding and Multimedia Signal Proc.*, Aug. 2008.
- [4] I. S. Morskowitz and A. R. Miller, "Simple timing channels," *Proc. IEEE Comp. Soc. Symposium on Research in Security and Privacy*, 1994.
- [5] Z. Wang and R. B. Lee, "Capacity estimation of non-synchronous covert channels," *25th IEEE Intl. Conf. on Distributed Computing Systems Workshops*, Jun. 2005.
- [6] V. Anantharam and S. Verdú, "Bits through queues," *IEEE Trans. on Info. Theory*, vol. 42, no. 1, pp. 4-18, Jan. 1996.
- [7] A. B. Wagner and V. Anantharam, "Zero-rate reliability of the exponential-server timing channel," *IEEE Trans. on Info. Theory*, vol. 51, no. 2, pp. 447-465, Mar. 2005.
- [8] S. Sengupta, S. Anand, K. Hong, and R. Chandramouli, "On adversarial games in dynamic spectrum access based timing covert channels," *ACM Mobile Computing and Communications Review: Special Issue on Cognitive Radio Technologies and Systems*, vol. 13, no. 2, pp. 96-107, Apr. 2009.
- [9] M. Buddhikot, P. Kolodzy, S. Miller, K. Ryan, and J. Evans, "Dimsumnet: New directions in wireless networking using coordinated dynamic spectrum access," *IEEE Intl. Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'2005)*, Nov. 2005.
- [10] S. Sarkar, E. Altman, R. El-Azouzi, and Y. Hayel, "Information concealing games," *Proc., IEEE Intl. Conf. on Computer Commun. (INFOCOM'2008) mini-conference*, Mar. 2008.
- [11] S. C. Chow, *Encyclopedia of Biopharmaceutical Statistics*. Informa Health Care, 2nd Edition, 2003.
- [12] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. on Info. Theory*, vol. 29, no. 1, pp. 152-157, Jan. 1983.
- [13] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Addison-Wesley, 1995.
- [14] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.
- [15] D. G. Luenberger, *Linear and Non-linear Programming*. Kluwer Academic Publishers, 1984.
- [16] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall Inc., New Jersey, 1996.