On Adversarial Games in Dynamic Spectrum Access Networking based Covert Timing Channels *

S. Sengupta, S. Anand, K. Hong and R. Chandramouli
Department of ECE, Stevens Institute of Technology, Hoboken, NJ 07030
{*Shamik.Sengupta,asanthan,khong,mouli*}*@stevens.edu*

In this paper, we study tactical covert timing networks *with dynamic spectrum access capability amidst adversaries. We present a two-tier game framework to model the attack-defense scenario. There are very few studies available in the literature on covert timing channels with multiple parallel transmissions. This paper presents a new paradigm combining the time diversity provided by covert timing channels and frequency diversity provided by dynamic spectrum switching, to combat jamming. The dynamic sensing of different spectrum bands and subsequent jamming by the attacker, and the camouflaging defense by the covert network are modeled as a two-tier game. We present a dynamic* minimax camouflaging *strategy for the covert network and sensing and jamming strategies for the attacker. We compare the performance of our proposed equilibrium strategies with that of other well known strategies and demonstrate the effectiveness of our proposed solution. We use theoretical analysis, simulations and testbed experiments to illustrate our ideas.*

I. Introduction

Security in wireless networking now presents increased challenges to maintain confidentiality of the large volume of information flow. Encryption has been a traditional method to achieve secrecy but reaults in additional complexity and larger energy consumption. Accordingly, there is growing interest in devising new "light-weight" yet secure mechanisms for data transfer in wireless networks. This motivates the study of key-less security mechanims e. g., information theoretic security by randomly changing code books or by using covert communication.

Covert communication primarily refers to the notion of transferring hidden information. The main focus here is to hide secret, valuable information underneath "normal" information. The hidden information is desired to be invisible to the external world. There are five different types of covert channels widely known (viz., *covert storage*, *covert timing*, *covert termination*, *covert resource exhaustion* and *covert power*). Of these, covert storage and covert timing are most popular. Covert storage channels are based on the use of a shared data storage area and rely on locks or semaphores. As an example, in order to trasfer covert information in storage channels, a node could modify some portions of a particular packet (e. g., a header) or modify parts of information in a storage location (e. g., a disk or a folder). Covert timing channels on the other hand, use timing to convey information and can be utilized as key-less secirity in processor sharing, shared message buffers or standard network communications. In a typical timing covert channel scenario, two or more nodes may communicate using standard streaming media applications (e.g., video). The inter-packet transmission time of the packets may be modulated in such a way that the it affects the inter-arrival times of the packets at the receiver, thus conveying different secret messages (e. g., bit sequences). Though the outside world perceives a traditional streaming media application, valuable information may be transfered securely as underlay.

Dynamic spectrum access (DSA) [1, 2] based on cognitive radios has been investigated by radio engineers. DSA is seen as a solution that can harness the spectrum bands dynamically in a spatial and temporal manner. Cognitive radio nodes continuously perform spectrum sensing to dynamically identify the available spectrum bands that they can use, when un-used by the primary incumbent radio systems [3]. The dynamic sensing and switching of spectrum bands not only enhances the capacity of the network, but also inherently provides a means to combat jamming because nodes can switch channels when jammed.

This paper presents a new pardigm combining multi-terminal covert timing channels and DSA. As mentioned eariler, DSA inherently provides a means to combat jamming. Moreover, the lack of pre-defined spectrum bands for the covert timing operations in DSA networks makes the task of detecting covert timing operations harder in DSA. However, if the at-

*This work was partially supported by the National Institute of Justice (NIJ).

tacker is also a congitive radio node, then whenever the network switches channels, the attacker can also switch accordingly and intelligently detect covert timing operations to continue jamming them [4]. Most networks have internal system-level means to detect malicious nodes and prevent jamming. The lack of well defined policing mechanisms in DSA poses a difficult challenge to detect the presence of an attacker. Thus DSA poses intersting challenges to the networks to detect the presence of an attacker and also poses challenges to the attacker in terms of sensing the presence of covert timing channels and jam them. We propose a *tactical covert network* with multiple transmitter-receiver pairs involved in covert timing transmissions in different spectrum bands. The attacker aims to detect the covert timing transmissions and jam them while the covert network deploys camouflaging resources (in the form of communication between auxillary cognitive radio nodes) in different spectrum bands to avoid being detected. The model in this paper combines in an effective manner, the diversities obtained by time (timing channels) and frequency (DSA) to enhance security.

We first present results from a testbed experiment to motivate the problem. The experimental results show that increase in auxiliary communications (camouflage resource) makes detection of covert timing channels harder. We apply the experimental findings to drive a statistical sensing/detection formulation using the *Dose-Response-Immunity* model [5]. We then present a two-tier game-theoretic framework to model this attack-defense scenario. In the first tier of the game (called the sensing game), the attacker determines the set of channels that it needs to sense to detect the presence of covert communication and the covert network determines the set of channels it needs to camouflage using auxillary communication. This is modeled as a zero-sum game of incomplete information and the statistical sensing/detection formulation mentioned above is used to define the utilities for the covert network and the attacker. We determine the Nash equilibrium of this game and present a dynamic *minimax camouflaging* strategy for the covert network and sensing and jamming strategies for the attacker. In the second tier of the game (called the jamming game), we model the objective of the jamming attacker as a nonzero-sum game and provide sufficient conditions for the existence of a unique Nash equilibrium. We show that it is in the best interest of the attacker and the covert network to adhere to the proposed strategies to achieve Nash equilibrium [6]. We compare the performance of our proposed strategies with that of other well known strategies and demonstrate the effectiveness of the proposed solution.

The rest of the paper is organized as follows. Section II provides the current state-of-the-art on covert channels. In Section III, we present experimental results to analyze the robustness of the timing channel with auxiliary communications camouflaging the covert operation. Section IV presents the two-tier game to model the conflict between the covert network and the attacker. The game is analyzed and equilibrium strategies are proposed in Section V. In Section VI, we present numerical and simulation results to analyze the benefits obtained by covert network and the attacker. Conclusions are drawn in Section VII.

II. Related Work

The concept of covert channels was first introduced by Lampson [7]. More detailed definitions of covert channels can be found in [8]. While covert storage channels have been studied in detail ([9]-[13] and references therein), there are relatively fewer studies on covert timing channels. Research on covert timing channels have been primarily focused on analysis of capacity. The performance of timing covert channels in the presence of noise was investigated in [14]. In [15], discrete, memoryless and noiseless timing covert channels were studied. The authors present different methods of defining channel capacity and bounds for *simple timing channels*. In [16], the authors compute the covert capacity of security aware transmission scheduling. A quantifiable measure for covert information flows and a study of its relationship with the statistical properties of the transmission schedules were provided. In [17], the authors propose *TCPScript*, as an approach to embed covert information in a TCP flow. They analytically compute the channel capacity for TCPScript, IPTime, and JitterBug. Statistical detection of covert timing channel encoding in network packet delays is presented in [18].

Most of the above mentioned research study single-terminal covert timing channels. Covert networks consisting of multi-terminal timing channels have seldom been discussed. The deployment of covert timing channels in DSA networks has not been studied to the best of our knowledge. Due to the fact that DSA flexibly allows users from multiple networks to co-exist, we envisage that using stealth in transferring information would become even more essential. Deployment of covert DSA networks pose interesting challenges to the network as well as the attacker. This is the first attempt to study covert timing DSA networks.

III. Timing Channel with Camouflage

We briefly discuss the timing channel operation and then investigate the sensitivity and robustness of this channel in the presence of camouflage. We primarily focus on *binary assymetrical* timing channel although the study can be generalized easily to multiple symbol timing covert operations.

In binary timing channels, the hidden message (bit sequence) is represented using distinct inter-arrival timing of the packets as observed by the receiver [15, 19]. As an example, the receiver decodes a bit zero ('0') if the inter-arrival time of the packets is t_1 and a bit one ('1') if the inter-arrival time of packets at the receiver is $t_2 \neq t_1$. Since hidden information are transmitted using inter-arrival timings of the packets and not by the actual packet content, mere sniffing of the packet content in the spectrum band to detect any kind of anomaly does not provide any information to the attacker. Therefore, the attacker needs to analyze the inter-arrival timings of the packets and check for distinct timing distributions over the spectrum band. With this in mind, we implement a tactical covert network with DSA capability based on cognitive radios (CR). In accordance with the statistical detection theoretical analysis presented in [18], we present our testbed results and study the sensitivity, i.e., risk of exposure of the timing channels under the presence as well as absence of camouflage.

III.A. Testbed experiment

For this experiment, we have implemented a cognitive radio prototype based on a software abstraction layer implemented over off-the-shelf IEEE 802.11a/b/g stack supported by Atheros hardware chipsets (Orinoco 802.11 a/b/g wireless card). For implementing the covert timing channel transmitter, we modify the Atheros Hardware Abstraction Layer (HAL) to build special hardware queues (sync queue). These sync queues, in turn, ensure transmissions corresponding to covert timing operations. CRs can access frequency bands dynamically in the IEEE 802.11a/b/g network (all 16 channels), providing us the ability to study the effectiveness of DSA and camouflage over timing channels. For our testbed setup, we implement CR nodes transferring messages using FTP communications as visible to the outside world. However, packets are transmitted at distinct time intervals thus devising near–invisible timing covert operation underlay to the FTP operation.

To model the sensitivity of timing covert channel and to differentiate between normal data traffic and timing covert data traffic, we first conduct two experiments: (i) standard FTP communication without any timing channel and then (ii) FTP with timing channel underlay. For both these cases, we consider only one transmitter and one receiver as shown in Fig. 1. Solid line indicates the normal FTP communication without timing channel while the dotted line indicates FTP communication with timing channel underlay.

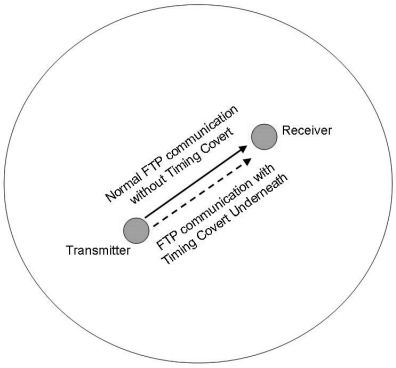


Figure 1: Single transmitter and single receiver

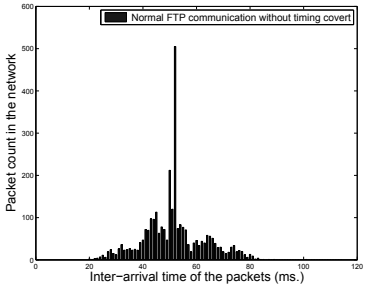


Figure 2: Single transmitter and single receiver with normal data traffic (no timing channel)

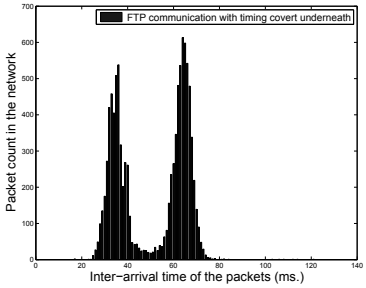


Figure 3: Single transmitter and single receiver with binary timing channel underlay

Fig. 2 presents the packet count distribution vs inter-arrival timing of the packets over the entire duration of the experiment in the absence of timing channel. It is observed that in the absence of timing channel, the packet count resembles a Gaussian distribution with single mean. Large channel noise is expected to induce a Gaussian distribution with higher variance, while low channel noise results in a Gaussian curve with low variance. We then introduce the timing channel in the testbed (with single

transmitter and single receiver) and sniff the inter-arrival timing of the packets in the network. For our binary asymmetrical timing covert channel, packets are transmitted at two distinct time intervals. Fig. 3 presents the packet count distribution in the presence of timing channel where two distinct Gaussian distributions are observed.

From the above results, it is inferred that sensing the inter-arrival time of the packets in the network can reveal the existence of a timing covert channel in the network. Note that, an interesting observation from the above result is that the further away the Gaussian distributions are the easier it would become to detect the existence of timing covert channel. In contrast, the closer the Gaussian distributions are, the harder it is to detect any anomaly from normal data traffic.

III.B. Camouflage with multiple transmitters and receivers

In this timing covert channel system design, we now 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) as depicted in Fig. 4. We implement only one link as the intended timing covert channel in each of the spectrum bands (e.g., A → B and C → D) while other normal communications act as auxiliary operations to camouflage the timing channel.

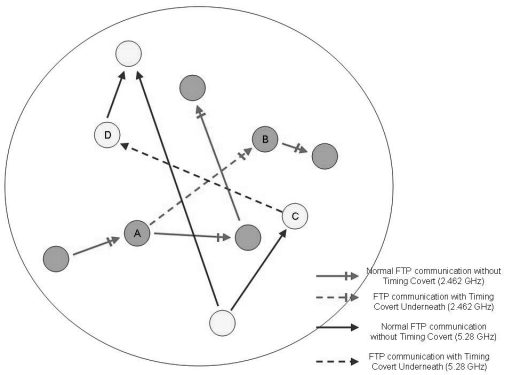


Figure 4: Multiple transmitters–receivers scenario

There are several advantages for taking the camouflage approach with multiple transmitters and receivers in a covert network. Note that, an attacker, who wants to destroy any such timing covert communication, does not have prior knowledge about whether any timing covert communication is present in any particular spectrum band and also does not have knowledge about who the covert transmitter and receiver might be. Thus an attacker must observe the inter-arrival timing of the packets in the network to distinguish Gaussian distributions of packet counts to detect if any "anomaly" exists in the packet count distribution from the normal data traffic. Moreover, in a DSA network, the attacker can not remain in one spectrum band for the entire duration; rather the attacker must switch rapidly across different spectrum bands to sense the inter-arrival timing of the packets in each of the bands. Unfortunately, for the attacker, even fast switching will cause losing some traffic information due to the finite physical switching time, resulting in incomplete information. In addition to that, if the attacker switches from one channel (e.g., channel x) and hop to another channel (e.g., channel y), the attacker will not be able to "hear" any traffic that is occurring on channel x until the attacker returns to that channel as part of the channel-switching schedule.

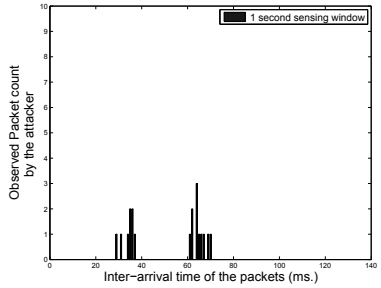


Figure 5: Packet count as observed by the attacker in a sensing window of 1 second in the presence of single timing channel without any camouflage

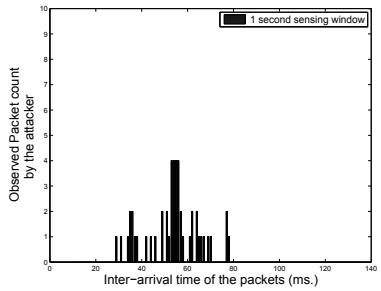


Figure 6: Packet count as observed by the attacker in a sensing window of 1 second in the presence of 5 auxiliary communications camouflaging in 2.462 GHz

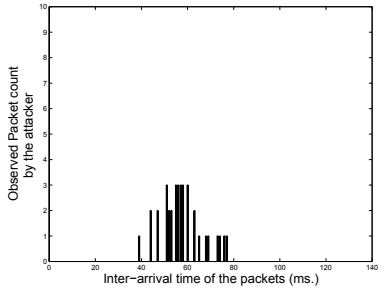


Figure 7: Packet count as observed by the attacker in a sensing window of 1 second in the presence of 4 auxiliary communications camouflaging in 5.28 GHz

In Fig. 5, 6 and 7, we present the packet count results with inter-arrival times as observed by the attacker for comparison purpose. The duration of attacker staying and sensing in each of the 16 bands (all 16 frequency channels in IEEE 802.11a/b/g are used for this experiment setup) is considered as 1 second while, fast switching across spectrum bands consumes average $5 - 10$ ms for each of the switching. In Fig. 5, there is no camouflage (only single transmitter and receiver with timing covert communication). As evident from the packet count distributions, it is easy to detect timing channel in single transmitter and receiver scenario without any camouflage.

Next, we introduce multiple auxiliary communications for camouflaging in both the spectrum bands. Fig. 6 and 7 present the results in terms of packet counts with inter-arrival timing of the packets. Note that, with increase in number of auxiliary operations, successful sensing/detection becomes harder as the packet count distribution with inter-arrival timing of the packets look more similar to the distribution in normal data traffic. It is evident from the figures that with multiple auxiliary transmitter–receiver communications, camouflaging for the intended (actual) timing channel is easier and the sensing/detection from the attacker's perspective becomes hard. Thus it is clear that camouflaging can be used effectively to defend the timing channel underlay from the attacker.

However, in a DSA system, there might be potentially multiple timing channels in multiple spectrum bands. Though it is shown experimentally that camouflaging timing covert communication in a spectrum band with other auxiliary communications is beneficial for secrecy of the timing covert communication, but the number of auxiliary communications (defense resource) can not be increased indefinitely in one spectrum band (limitation due to the total finite capacity of auxiliary communications to be deployed over the spectrum bands, limitation due to interference and self-coexistence in the spectrum band). Thus it is necessary to use the auxiliary camouflage resources judiciously and dynamically across the multiple spectrum bands. The question that can naturally be raised is: *what would be an optimal camouflage strategy for such a covert network in a DSA system?* We present a game-theoretic framework to answer this question.

IV. Timing Covert Game in DSA

To explore the risk of detection of timing covert operations (both from the defense as well as the attack perspectives), we consider the most generic abstraction of "always greedy and profit seeking" model for the defender of the timing covert channels and the attacker. Consider a set of $\mathcal{N}$ timing covert communications over $\mathcal{N}$ available spectrum bands. These spectrum bands are the set of targets. Each of the timing channels is characterized by a valuation associated with it, which indicates the importance of the covert information it carries, or, in other words, indicates the incentive the attacker would gain on successful detection. This is described in more detail in Section IV.C. The attacker with finite sensing resource senses all the spectrum bands and chooses to destroy (jam) the covert operation in any one particular band, such that it results in maximum loss to the covert network. The covert network, on the other hand, enables multiple auxiliary cognitive radio nodes to communicate dynamically in different spectrum bands to camouflage the intended covert operations. Note that the covert network needs to deploy camouflaging communication dynamically across different spectrum bands. The attacker also has to switch rapidly across the spectrum bands (dynamically), to detect covert communication in each of the bands. Dynamic spectrum access (DSA)/ cognitive radio networking (CRN) inherently provide the necessary flexibility to make the above framework feasible. Thus, this problem is of particular significance in DSA/CRN.

IV.A. Dose-Response-Immunity Model

It is necessary to develop a statistical model for sensing/detection of the timing covert operations. We apply the most generic *Dose-Response-immunity model* [5] in our analysis. Dose-Response-Immunity or Dose-Response model is a very popular model from Pharmacodynamics [5] and Bio-Medical [20] for analyzing mortality rate of subjects with respect to the dosage of a drug. Here, we present the simple dose-response probabilistic formulation based on the logistic regression in accordance with the study presented in [21, 22]. Throughout this paper, we follow this probabilistic sensing/detection model for our attack−defense scenario in timing covert operations. The dose-response model is as follows. Let $Y = 1$ denote the death of the subject due to the dosage of a drug and let $Y = 0$ denote the survival. Let $\Pr\{Y = 1\} = p = 1 - \Pr\{Y = 0\}$. If $\overrightarrow{\mathbf{X}}$ signifies the vector of treatment variables (i.e., concentration of doses, immunity, etc), and $\overrightarrow{\beta}$ denotes the unknown parameter vector for regression fit, the dose-response relationship [5] is given by

$$logit(p) = \ln\left(\frac{p}{1-p}\right) = \overrightarrow{\beta}\,\overrightarrow{\mathbf{X}}. \qquad (1)$$

With the above insight, the attack-defense scenario in the covert network can be looked upon as follows. The malicious attacker uses resources to sense and the amount of sensing resources is analogous to the "dose" of a drug. Similarly, the camouflage used by the defender is analogous to the "immunity" because a higher camouflage demands that the attacker needs to deploy additional sensing resources to successfully detect the covert communication. Finally, the probability of successfully detecting the covert communication is the probability of "death" caused by the dose against the immunity.

Let $Y = 1$ denote the successful detection of timing covert operation by the attacker and $Y = 0$ denote timing channel not detected. Let s be a function of the attacker's sensing resource and M be a function of the defender's camouflaging resources. We model $\ln(s)$ to be the dose component and $\ln(M)$ to be the immunity component. Thus,

$$\overrightarrow{\mathbf{X}} = \begin{bmatrix} \ln(s) \\ \ln(M) \end{bmatrix}, \tag{2}$$

signifies the treatment variable vector. Since the sensing and camouflaging resources act against each other to determine the detection/not detection outcome, $\overrightarrow{\beta} = \begin{bmatrix} \beta_1 & -\beta_2 \end{bmatrix}$. From (1) and (2),

$$p = \frac{s^{\beta_1}}{s^{\beta_1} + M^{\beta_2}}. \tag{3}$$

Note that β_1 and β_2 signify the effectiveness of attacker's anomaly detection capability and covert network's efficient camouflaging, respectively.

IV.B. Game conflict/decision model

Consider a set of $\mathcal{N}$ timing covert operations in the available spectrum bands and a finite number of total auxiliary cognitive radio communications for camouflage. In this paper, we assume a single point attack model, in which, an attacker can sense all the spectrum bands by switching its radio dynamically, but, can only destroy (jam) one band at a time.

As a rational agent, the attacker's objective would be to destroy that timing channel which would impact the covert network the most. Thus as an attacker, the decision problem is to select the best target out of all potential targets. On the other hand, the decision problem for the covert network would be to compute a strategy to use the total finite camouflage resources dynamically across all the spectrum bands, such that the attack, when successful causes minimum impact. By devising utility functions and strategies for both the attacker as well as the covert network, it is of interest to investigate the game and find the Nash equilibrium if one exists. We present both zero-sum as well as non-zero-sum games to model the attack-defense problem and analyze the proposed strategies.

IV.C. Game Formulation

Consider a geographical region in which the covert network operates with its $\mathcal{N}$ timing channels. Each of the timing covert operation is allocated a spectrum band dynamically. If multiple timing covert operations are allocated the same spectrum band, then the valuation of this multiple timing covert operation in the band can be modeled as a weighted sum of the valuations of each individual timing covert operation in the band. Hence, without loss of generality, we can consider each timing covert operation to be allocated a different spectrum band. As mentioned earlier, each of these timing covert operations has a valuation.

The valuation of a timing covert operation in a band is a function of the perceived capacity of the timing covert operation in that band. Note that, the capacity perceived by the binary assymetrical timing covert channels in different spectrum bands may be different due to varying physical channel characteristics in different bands. This results in different valuations for the timing covert operation in different bands.

Following the capacity analysis in [18], we consider the valuation of a binary assymetrical timing covert operation in the jth spectrum band to be be a function of the capacity of the j^{th} spectrum band, C_j, and given by [18]

$$U_j(C_j) = f(C_j) = f\left(\ln\left(1 + 2^{\frac{H(q_{j0}) - H(q_{j1})}{q_{j1} + q_{j0} - 1}}\right) + \frac{(1 - q_{j0})H(q_{j1}) - q_{j1}H(q_{j0})}{q_{j1} + q_{j0} - 1}\right), \tag{4}$$

where $H(x) = -x \ln x - (1 - x)\ln(1 - x)$, $f(\cdot)$ is an increasing function, q_{j0} denotes the bit error rate of receiving a 0 as a 1 and q_{j1} denotes the bit error rate of receiving a 1 as a 0.

The zero-sum game is then formulated as follows:

- The covert network has a total camouflage resource, M, and as mentioned in the decision model in subsection IV.B, the decision problem of the covert network would be to find a strategy to distribute the camouflage resources dynamically such that a resource M_i is allocated to spectrum band i.
- The attacker has a sensing resource, s, and switches across spectrum bands to sense/detect

timing covert operation. Upon successful detection of a timing covert operation, the attacker chooses any one spectrum band and destroys (jams) that band.

- If the i^{th} spectrum band is allocated camouflage resource M_i, the probability of successfully sensing/detection a timing covert operation in i^{th} spectrum band, p_i, is given by (3) with p replaced by p_i and M replaced by M_i.
- The expected loss for the covert network when the attacker successfully senses and attacks the timing covert operation in the i^{th} spectrum band, $E[I_i]$, is given by

$$E[I_i] = \left(\frac{s^{\beta_1}}{s^{\beta_1} + M_i^{\beta_2}}\right) U_i(C_i). \tag{5}$$

- The attacker can sense only one spectrum band at a time and can destroy only one spectrum band. Therefore, the maximum impact for the timing covert network occurs when the attacker attacks the band with the largest $E[I_i]$. Therefore, the objective of the covert network is to minimize the expected impact, $E[I]$, given by $E[I] = \max_i^{\mathcal{N}} E[I_i]$ As rational players in the zero-sum game, the objective of the covert network would be to minimize $E[I]$ while that of the attacker would be to maximize $E[I]$.

In the following section, we analyze the zero-sum game and describe the equilibrium strategies.

V. Equilibrium Strategies

The game formulation described in Section IV.C defines the decision problems for the covert network and the attacker. However, the covert network does not know before-hand, the attacking strategy of the attacker. We first define a sensing game in which the covert network allocates camouflage resources to the spectrum bands. We then describe a jamming game in which the attacker chooses a spectrum band to attack.

V.A. Sensing game

Following the arguments in Section IV.C, the decision problem for the covert network can be modeled as the following optimization problem

$$\min_{\mathbf{M}} \max_{i=1}^{\mathcal{N}} \left(\frac{s^{\beta_1}}{s^{\beta_1} + M_i^{\beta_2}}\right) U_i(C_i) \tag{6}$$

subject to the constraints

$$\sum_{i=1}^{\mathcal{N}} M_i = M, \tag{7}$$

where $\mathbf{M} = \begin{bmatrix} M_1 & M_2 & \cdots & M_{\mathcal{N}} \end{bmatrix}$. The following Lemma provides the optimum decision rule for the covert network.

Lemma 1: *The optimum strategy for the covert network is to distribute all the camouflage resources, M, to defend (camouflage) a subset of the timing covert channels, $\mathcal{S} \subset \{1, 2, \cdots, \mathcal{N}\}$, such that $E[I_i] = E[I_j] \; \forall \; i, j \in \mathcal{S}$, and $E[I_i] > U_k(C_k) \; \forall \; i \in \mathcal{S}, k \notin \mathcal{S}$.*

Proof: Let $\mathcal{S} = \{i_1, i_2, \cdots i_\omega\}$. such that $E[I_i] = E[I_j] \; \forall \; i, j \in \mathcal{S}$ and $E[I_j] > U_k(C_k) \; \forall \; j \in \mathcal{S}$, $\forall \; k \notin \mathcal{S}$. From (5), $E[I_k] \leq U_k(C_k) \; \forall \; k$. Therefore for any $k \notin \mathcal{S}$, $E[I_k] \leq U_k(C_k) < E[I_j] \; \forall \; j \in \mathcal{S}$. Therefore, $\text{argmax}_{k=1}^{\mathcal{N}} E[I_k] = j$ for $j \in \mathcal{S}$. Let π_j be the probability that the attacker attacks band j for $j \in \mathcal{S}$. The optimization problem in (6) subject to the constraint (7) can then be re-written as

$$\min_{\mathbf{M}} \sum_{j \in \mathcal{S}} \pi_j \left(\frac{s^{\beta_1}}{s^{\beta_1} + M_j^{\beta_2}}\right) U_j(C_j) \tag{8}$$

subject to the constraint (7). Consider a feasible solution $\tilde{\mathbf{M}} = \begin{bmatrix} \tilde{M}_1 & \tilde{M}_2 \cdots & \tilde{M}_{\mathcal{N}} \end{bmatrix}$ such that $\exists \; k \notin \mathcal{S}$ such that $\tilde{M}_k \neq 0$. Therefore, $\Delta \stackrel{\triangle}{=} M - \sum_{j \in \mathcal{S}} \tilde{M}_j > 0$. Consider another solution $\hat{\mathbf{M}} = \begin{bmatrix} \hat{M}_1 & \hat{M}_2 \cdots & \hat{M}_{\mathcal{N}} \end{bmatrix}$ such that $\hat{M}_k = 0 \; \forall \; k \notin \mathcal{S}$ and $\forall \; j \in \mathcal{S}$, $\hat{M}_j = \tilde{M}_j + \frac{\Delta}{\omega}$. Note that $\sum_{k=1}^{\mathcal{N}} \hat{M}_k = M$. Thus, $\hat{\mathbf{M}}$ is also a feasible solution. Also, note that $\hat{M}_j > \tilde{M}_j \; \forall \; j \in \mathcal{S}$ Hence,

$$\sum_{j \in \mathcal{S}} \pi_j \left(\frac{s^{\beta_1}}{s^{\beta_1} + \hat{M}_j^{\beta_2}}\right) U_j(C_j) < \sum_{j \in \mathcal{S}} \pi_j \left(\frac{s^{\beta_1}}{s^{\beta_1} + \tilde{M}_j^{\beta_2}}\right) U_j(C_j).$$

Thus $\tilde{\mathbf{M}}$ is not optimal. Hence the optimal strategy results in $M_k = 0 \; \forall \; k \notin \mathcal{S}$. □

With the best response strategy defined for the covert network, the natural question that arises is what would be the attacker's sensing strategy in this game.

Lemma 2: *Attacker's optimal dominant best response would be to prioritize sensing timing covert information in the defended spectrum band(s).*

Proof: Let, without loss of generality, the bands defended by the covert network be $\mathcal{S} = \{1, 2, \cdots, n\}$, where $n < N$. If the attacker spends sensing resources in a band $k \notin \mathcal{S}$, the utility obtained is $U_k(C_k)$. The utility obtained by the attacker when sensing a band $j \in \mathcal{S}$ is $E[I_j]$. From Lemma 1, $E[I_j] > U_k(C_k), \forall \; j \in \mathcal{S}, \forall \; k \notin \mathcal{S}$. Thus, the utility obtained by the attacker when sensing a defended spectrum band is larger than that obtained when sensing un-defended bands. □

With the sensing game and the dominant best responses from both covert network and the attacker defined, the second tier of the game needs to be explored next where attacker tries to jam (destroy) a spectrum band with potential existence of timing covert operation. The question that naturally arises is that which spectrum band should the attacker choose to destroy (jam) the potential timing covert operation in that band and at which power?

V.B. Jamming game

The objective of the jamming game model is to investigate about the probabilities with which the attacker would choose any spectrum band with potential timing covert operation and optimal signal transmit power for jamming the band in each game. In such a non-cooperative game model, this can be achieved by selfish maximization of the net utility function (utility attained minus the cost incurred) by the attacker. Note that the strategy of the defender does not change in this stage of the game. Also note that the jamming (with destruction of timing covert operation) of a spectrum band is successful in a game if the SINR due to the attacker (jammer) at the actual intended receiver of the timing covert operation is greater than some desired SINR threshold due to the intended transmitter of the timing covert operation at the intended receiver. The attacker must therefore transmit jamming signal with a power so as to exceed the SINR threshold. However, the transmit power can not be increased indefinitely as that would incur cost to the attacker which reduces attacker's net utility. To incorporate the rationality of the attacker and the cost involved in such jamming game, we then extend and generalize the attacker's net utility function as

$$E[I_i] = a\log\left(1+\pi_i p_i U(C_i)\right) + Q(\gamma_i,\tau_i) - \mu\pi_i A_i, \qquad (9)$$

where $\log\left(1+\pi_i p_i U(C_i)\right)$ represent the perceived benefit of the attacker and $\mu\pi_i A_i$ denotes the cost as the attacker plans to attack ith spectrum band. π_i denotes the probability with which the attacker chooses the ith spectrum band and A_i is the attacker's transmit power. As mentioned before in the dose-response-immunity model, p_i denotes the probability of successful sensing/detection of timing covert operation, while $U(C_i)$ is the timing covert operation capacity in the ith band. $Q(\gamma_i,\tau_i)$ is an indicator function denoting success/failure of the jamming attack. If $\gamma_i > \tau_i$, the attack is successful denoting the net utility of the attacker as

$$E[I_i] = a\log\left(1+\pi_i p_i U(C_i)\right) + \lambda\log(\gamma_i-\tau_i) - \mu\pi_i A_i. \qquad (10)$$

Otherwise, if $\gamma_i \leq \tau_i$, the attack is failed denoting net utility as $E[I_i] = -\mu\pi_i A_i$ where τ_i is the SINR threshold at the intended receiver in the ith band that the attacker must exceed to successfully jam. γ_i signifies the SINR received at the intended receiver due to the attacker's transmission and can be given as

$$\gamma_i = \frac{A_i h_i}{\mathcal{W} + \sum_j e_{ij} h_{ij}}, \qquad (11)$$

where e_{ij}'s are the transmission powers of all other transmitters in the ith spectrum band, h_i is the link gain between attacker and the receiver (intended jamming point) while h_{ij}'s are the link gains from all other transmitters to the receiver under consideration. $\mathcal{W}$ is the additive white Gaussian noise. The coefficients a, λ and μ are nonzero positive parameters that indicate the relative importance of benefit and cost and act as weightage factors. Note that the magnitude of λ should be small and that of μ should be large. This is because, a small μ results in lower penalty suffered by the jammer for transmitting higher powers, which is counter-intuitive and is also against the requirement of pricing. Similarly, a large value of λ indicates a larger incentive for the jammer to increase its transmit power so that $\gamma_i >> \tau_i$. Since any $\gamma_i > \tau_i$ results in successful jamming, the payoff for the jammer should increase by an insignificant amount when $\gamma_i >> \tau_i$, which is ensured by keeping the magnitude of λ, small.

Note that, we could have chosen any other form for the attacker's perceived benefit that increases with probability of choosing a target and attacker's transmitting power. But we chose the log function because the perceived benefit increases quickly initially as the probability of choosing the target increases from zero and then increases slowly. Also, $\lambda\log(\gamma_i-\tau_i)$ reflects the intuition that the perceived benefit increases quickly initially as soon as the γ_i exceeds τ_i signifying success of jamming and then increases slowly and gradually saturating. This is because increasing transmitting power continuously beyond a certain value would not help the attacker in gaining any extra benefit; rather it will only increase the cost of transmission. Moreover, log function is analytically convenient, increasing, strictly concave and continuously differentiable.

With attacker's modified net utility function defined, it is now interesting to see if there exists any mixed strategy Nash equilibrium for the attacker, i.e., if any jamming power and probability of choosing a spectrum band exist that would maximize the attacker's net utility.

Lemma 3: *Mixed strategy Nash equilibrium exists for the attacker if* $\gamma_i = \tau_i + \epsilon, \forall i \in \mathcal{N}$, *where* $0 < \epsilon << 1$.

Proof: For proving the existence of Nash equilibrium, we need to investigate if there exist tuples of jamming power and probability of choosing spectrum bands that would maximize the attacker's net utility. In other words, we need to show that $E[I_i]$ is strictly concave under the coupled constraint tuples (A_i, π_i). In a game with coupled constraints, the prime criterion for proving strict concave nature is to check whether the Hessian of $E[I_i]$ is negative definite. Differentiating equation (10) with respect to A_i, we get

$$\frac{\partial E[I_i]}{\partial A_i} = \frac{\lambda h_i}{(\mathcal{W} + \sum_j e_{ij} h_{ij})(\gamma_i - \tau_i)} - \mu \pi_i. \quad (12)$$

Similarly, differentiating equation (10) with respect to π_i,

$$\frac{\partial E[I_i]}{\partial \pi_i} = \frac{a p_i U(C_i)}{1 + \pi_i p_i U(C_i)} - \mu A_i. \quad (13)$$

The Hessian of $E[I_i]$ is denoted as

$$\mathcal{H} = \begin{bmatrix} \frac{\partial^2 E[I_i]}{\partial A_i^2} & \frac{\partial^2 E[I_i]}{\partial A_i \partial \pi_i} \\ \frac{\partial^2 E[I_i]}{\partial \pi_i \partial A_i} & \frac{\partial^2 E[I_i]}{\partial \pi_i^2} \end{bmatrix}. \quad (14)$$

Differentiating equation (12) and (13) with respect to A_i and π_i again, and substituting in equation (14), $\mathcal{H}$ can be re-written as,

$$\mathcal{H} = \begin{bmatrix} -\frac{\lambda h_i^2}{(\mathcal{W} + \sum_j e_{ij} h_{ij})^2 (\gamma_i - \tau_i)^2} & -\mu \\ -\mu & -\frac{a p_i^2 U(C_i)^2}{(1 + \pi_i p_i U(C_i))^2} \end{bmatrix} \quad (15)$$

Then the Hessian, $\det(\mathcal{H})$, of $E[I_i]$ is given by

$$\frac{a \lambda h_i^2 p_i^2 U(C_i)^2}{(\mathcal{W} + \sum_j e_{ij} h_{ij})^2 (\gamma_i - \tau_i)^2 (1 + \pi_i p_i U(C_i))^2} - \mu^2. \quad (16)$$

The necessary and sufficient conditions for $\mathcal{H}$ to be negative definite are $\frac{\partial^2 E[I_i]}{\partial A_i^2} < 0$, and $\det(\mathcal{H}) > 0$ [23]. As obvious from equation (15), $\frac{\partial^2 E[I_i]}{\partial A_i^2} = -\frac{\lambda h_i^2}{(\mathcal{W} + \sum_j e_{ij} h_{ij})^2 (\gamma_i - \tau_i)^2} < 0$ thus satisfying the first condition. Now, if $\gamma_i = \tau_i + \epsilon$ where $0 < \epsilon << 1$, then $\frac{\lambda h_i^2 p_i^2 U(C_i)^2}{(\mathcal{W} + \sum_j e_{ij} h_{ij})^2 (\gamma_i - \tau_i)^2 (1 + \pi_i p_i U(C_i))^2} \rightarrow \infty$ signifying the positivity of $\det(\mathcal{H})$. Thus it is clear that $\mathcal{H}$ is negative definite and $E[I_i]$ is strictly concave in nature proving the existence of Nash equilibrium point [23]. □

For finding the optimized coupled constraint tuples of jamming power and probability of choosing a spectrum band can then be given by equating equation (12) and (13) to zero and solving for A_i^* and π_i^*, which are then given as,

$$A_i^* = \frac{\lambda}{\mu \pi_i^*} + \frac{\tau_i (\mathcal{W} + \sum_j e_{ij} h_{ij})}{h_i} \quad (17)$$

$$\pi_i^* = \frac{a}{\mu A_i^*} - \frac{1}{p_i U(C_i)}. \quad (18)$$

Thus, it is observed that the attacker can achieve mixed strategy Nash equilibrium under the given constraint and at the same time it can maximize the net utility by maintaining the optimized jamming power and probability of choosing a spectrum band.

VI. Numerical Results and Interpretations

In this section, we present numerical results to evaluate the proposed methodology and also corroborate the results with simulation experiments. We investigate the strategies from both the covert network and the attacker's perspectives. For assessment of the benefit obtained by the proposed strategies, we compare our proposed method with two popular heuristic camouflage resource allocation strategies, i.e., uniform and adaptive proportional strategies. In uniform strategy, the total camouflage resource is shared uniformly among different targets while in adaptive proportional strategies, allocation of camouflage resource is proportional to the valuations of the timing covert communications.

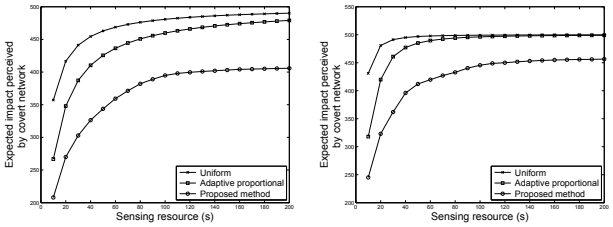
For simulation experiment and numerical study, random network topology is considered in a 200m. radius region where multiple timing channels are active in different spectrum bands. Moreover, we have assumed the transmitters and receivers (including transmitters and receivers carrying on camouflage traffic) in the covert network use directional antenna for transmission/receiving purpose. The attacker of the system uses omni-directional antenna for covert communication sensing while directional antenna is used for intended jamming. In Table I, we present the parameters for our experiments.

VI.A. Evaluating defense strategy

In Fig. 8(a), we present the impact perceived by the covert network vs. attacker's maximum sensing re-

Parameters	Values
Total spectrum band (N)	25
Valuation of the timing channels	50 - 500 units
Receiving radius	100 m.
Sensing radius	150 m. - 200 m.
Camouflage traffic	25 - 300
Max. sense resource capacity	10 - 200
DSA system transmit power	50 mW - 2 W
Covert transmission intervals	25 - 75 ms

Table 1: Parameters for simulations

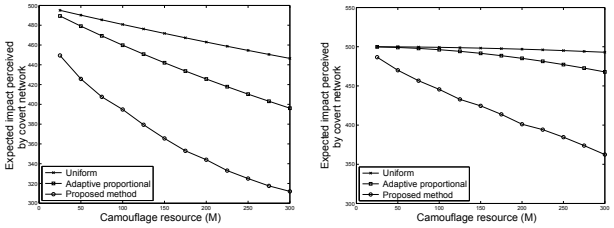


(a) (b)

Figure 8: a) Expected impact perceived by covert network ($\beta_1 = 1, \beta_2 = 1$), and b) Expected impact perceived by covert network ($\beta_1 = 2, \beta_2 = 1$)

source capacity while the camouflage resource is kept fixed as 100 and N is 25. β_1 and β_2 (in (3)) are assumed to be 1 here. As observed from the Fig. 8(a), with camouflage resource fixed, expected perceived impact increases with increase in sensing resource of the attacker; however, the expected perceived impact with the proposed mechanism is always smaller than the other two methodologies thus proving the effectiveness of the proposed scheme. In Fig. 8(b), we increase the value of β_1 to 2 and also present the expected impact perceived by the covert network. With total camouflage resource fixed, increased value of β_1 signifies higher probability of detection than the earlier case (when β_1 was 1) with unit increase in maximum sensing resource. It is seen from the figure that, even under increased effectiveness of sensing/detection from the attacker, the proposed mechanism clearly outperforms (with reduced expected perceived impact) the uniform and adaptive proportional camouflaging performance by almost $20 - 25\%$.

Next, we keep the maximum sensing resource capacity of the attacker fixed and vary the covert network's total camouflage resource. In Fig. 9(a) and 9(b), we present the expected impact perceived by the covert network with attacker's maximum sensing resource fixed as 100. While Fig. 9(a) shows the results with $\beta_1 = 1$ and $\beta_2 = 1$, Fig. 9(b) presents the results with β_1 increased to 2. It is observed that with the proposed minimax strategy of allocation of camouflage



(a) (b)

Figure 9: a) Expected impact perceived by covert network ($\beta_1 = 1, \beta_2 = 1$), and b) Expected impact perceived by covert network ($\beta_1 = 2, \beta_2 = 1$)

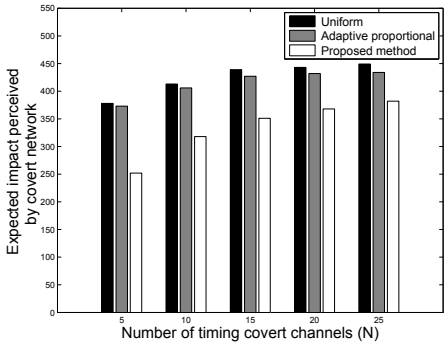
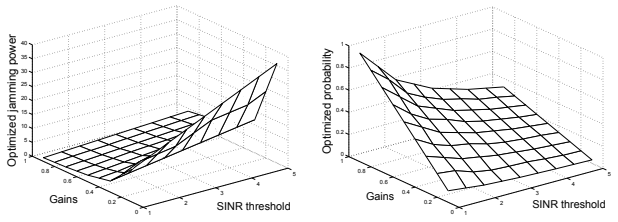


Figure 10: Expected impact perceived by covert network with varying number of timing covert channels

strategy, expected impact incurred by the covert network is reduced significantly indicating the improvement of the proposed methodology over uniform and adaptive proportional allocation. The most important observation is that when β_1 is increased to 2 signifying more efficient attacker with higher risk of detection of timing covert channels, even then the proposed method of minimax strategy demonstrates highly robust performance.

In Fig. 10 we compare the performance of the proposed strategy with that of the uniform and adaptive proportional strategies with varying number of timing covert communications from simulation experiments. The number of timing channels is varied from 5 to 25. The results presented are averaged over 100 simulation runs. It is observed that with increase in number of timing channels, the expected impact for all the strategies increase, which is expected. However, with the proposed minimax camouflage resource allocation, the covert network always incurs reduced expected impact resulting in better performance compared to the uniform and adaptive proportional strategy, which corroborates with the results presented from numerical analysis.



(a) (b)

Figure 11: a) Optimized jamming power, and b) Optimized probability

VI.B. Evaluating jamming strategy

In Fig. 11(a) and 11(b), we present the mixed strategy Nash equilibrium optimized jamming power and probability of attack respectively with both varying channel gain and SINR threshold (at the intended receiver node to be jammed). The timing covert channel valuation is assumed to be 200.

The probability calculation shows non-zero finite values thus proving the existence of mixed strategy space for achieving Nash equilibrium. It is also clear from the figure that with low channel gain between the attacker and intended jamming point and high SINR threshold, the attacker must transmit with high power thus resulting in higher cost for the attacker while with higher channel gain and low SINR threshold the attacker is better off with low transmit power for jamming. Fig. 11(b) strengthens the above claim where the mixed strategy Nash equilibrium probability of attack is plotted against varying channel gain and SINR threshold. With low channel gain and a high SINR threshold the attacker shows less inclination of attacking while with higher channel gain and low SINR threshold the optimal probability of attacking is high.

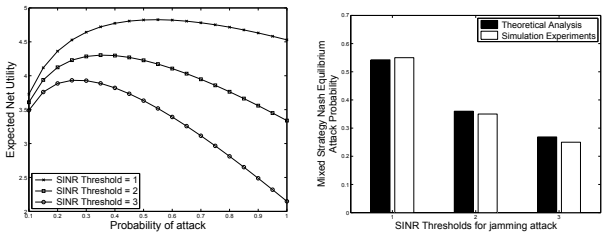
Next, we present the results from simulation experiments for the purpose of comparison with the theoretical analysis. In Fig. 12(a), we present the attacker's net utility from the simulation setup with channel gain 0.5. The probability of attack is varied for this simulation and correspondingly the average net utility is calculated over 100 simulation runs. One inference from the figure is that with increase in SINR threshold at the intended jamming point, the expected net utility achieved by the attacker decreases. This is due to the fact that with high SINR threshold successful jamming would require high transmitting power from the attacker thus increasing the cost of jamming as claimed earlier through numerical results. However, more interesting observation is the strictly concave nature of the curves with varying probability, proving that a point of maxima exists for each of the curves.

SINR threshold	Theoretical analysis	Simulation experiment
1	0.542429836	0.55
2	0.359953219	0.35
3	0.268714918	0.25

Table 2: Mixed strategy Nash equilibrium probability

This point of maxima corresponds to the probability of attack for the mixed strategy Nash equilibrium.

We calculate this probability of attack for achieving maximized utility Nash equilibrium from the simulation results (Fig. 12(a)) and compare them with that found through numerical analysis (Fig. 11(b)) in table 2. In Fig. 12(b), we plot the comparison results. It is found that the Nash equilibrium probabilities calculated through analysis corroborates with simulation experiments justifying the proposed mixed strategy for jamming attack from the attacker's perspective.



(a) (b)

Figure 12: a) Expected net utility; b) Mixed strategy Nash equilibrium probability comparison between theoretical and simulation results

VII. Conclusion

We presented a game theoretic framework to model attack-defense scenarios in tactical timing covert networks with dynamic spectrum access capability. We presented a sensing game to determine the optimal defense strategy for the network and a jamming game to determine the optimal attacking strategy for the adversary. We obtained necessary and sufficient conditions for the existence of a mixed strategy Nash equilibrium. We verified the accuracy of our analysis by simulations. We compared our strategy with other strategies and showed that our proposed strategy results in about 25% improvement. The extension of our proposed mechanism for simultaneous attacks on multiple spectrum bands and multiple overlapping networks are under investigation.

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 Intl. Symposium

on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 78-85, 2005.

[2] C. Cordeiro, M. Ghosh, D. Cavalcanti, K. Challapali, "Spectrum Sensing for Dynamic Spectrum Access of TV Bands," International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pp. 225-233, Aug. 2007.

[3] S. Huang, X. Liu, and Z. Ding, "Opportunistic Spectrum Access in Cognitive Radio Networks," In proceedings of IEEE INFOCOM, pp. 1427-1435, April 2008.

[4] T. Basar, "The Gaussian test channel with an intelligent jammer,", IEEE Transactions on Information Theory, vol. 29, Issue 1, pp. 152-157, Jan. 1983.

[5] S.C. Chow, "Encyclopedia of Biopharmaceutical Statistics," Informa HealthCare, Second edition, June 2003.

[6] J.F. Nash, "Equilibrium points in N-person games," Proc. of the National Academy of Sciences, vol. 36, pp. 48-49, 1950.

[7] B. W. Lampson, "A Note on the Confinement Problem," ACM Communication, 1973.

[8] National Computer Security Center, "A guide to understanding covert channel analysis of trusted systems," National Computer Security Center, Ft. George G. Meade, MD, Tech. Rep. NCSG-TG-030, Nov. 1993.

[9] K.W. Eggers, P.W. Mallett, "Characterizing network covert storage channels," Fourth Aerospace Computer Security Applications Conference, pp. 275-279, Dec. 1988.

[10] L. Frikha, Z. Trabelsi, W. El-Hajj, "Implementation of a Covert Channel in the 802.11 Header," International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 594-599, Aug. 2008.

[11] R.A. Kemmerer, P.A. Porras, "Covert flow trees: a visual approach to analyzing covert storage channels," IEEE Transactions on Software Engineering, vol. 17, pp. 1166-1185, Nov. 1991.

[12] K.-gi Lee, A. Savoldi, P. Gubian, K.S. Lim, S. Lee, S. Lee; "Methodologies for Detecting Covert Database," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 538-541, Aug. 2008.

[13] T. Takahashi, W. Lee, "An assessment of VoIP covert channel threats," Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm), pp. 371-380, Sept. 2007.

[14] I. S. Morskowitz and A. R. Miller, "The Channel Capacity of a Certain Noisy Timing Channel," In Proc. IEEE Transaction on Information Theory, vol. 38, Issue 4, pp. 13391344, 1992.

[15] I. S. Morskowitz and A. R. Miller, "Simple timing channels," In Proc. IEEE Computer Society Symposium on Research in Security and Privacy, pp. 5664, 1994.

[16] T. He, A. Agaskar, L. Tong, "On security-aware transmission scheduling," IEEE International Conference on Acoustics, Speech and Signal Processing, (ICASSP), pp. 1681-1684, 2008.

[17] X. Luo, W.W. Chan, K.C. Chang, "TCP covert timing channels: Design and detection," IEEE Intl. Conference on Dependable Systems and Networks, pp. 420-429, June 2008.

[18] V. Berk, A. Giani, and G. Cybenko, "Detection of covert channel encoding in network packet delays," Tech. Rep. TR2005-536, Dartmouth College, Hanover, NH., USA, August 2005.

[19] J. Giles, B. Hajek, "An information-theoretic and game-theoretic study of timing channels," IEEE Transactions on Information Theory, vol. 48, Issue 9, pp. 2455-2477, Sept. 2002.

[20] http://en.wikipedia.org/wiki/Dose-response_relationship.

[21] R. Derr, "Performing Exact Logistic Regression with the SAS System," Proceedings of the 25th Annual SAS Users Group International Conference (SUGI 25), 2000.

[22] O. Kuss, "How to use SAS for Logistic Regression with Correlated Data," Proceedings of the 27th Annual SAS Users Group International Conference (SUGI 27), 2002, Orlando.

[23] D. Fudenberg and J. Tirole, Game Theory, MIT Press, 1991.