An Analytical Model for Inference Attacks on the Incumbent's Frequency in Spectrum Sharing

Azza Ben-Mosbah, Timothy A. Hall, Michael Souryal, Hossam Afifi

An Analytical Model for Inference Attacks on the Incumbent's Frequency in Spectrum Sharing

Azza Ben Mosbah*†‡, Timothy A. Hall†, Michael Souryal†, Hossam Afifi‡
†National Institute of Standards and Technology, Gaithersburg, Maryland, USA
{azza.benmosbah, tim.hall, michael.souryal}@nist.gov
‡Télécom SudParis, Évry, France
hossam.afifi@telecom-sudparis.eu

***Abstract*—In spectrum sharing, incumbents with sensitive parameters require full protection of their operations. The incumbent's protection includes the protection of its privacy (e.g., operational frequency) against inference attacks carried out by malicious authorized secondary users. In this paper, we develop an analytical model to analyze the vulnerability of the incumbent's frequency to inference attacks and validate it by simulation. Specifically, we study random and ordered channel assignment schemes and compare results for both schemes.**

***Index Terms*—3.5 GHz band, analytical evaluation, incumbent vulnerability, inference attack, privacy, spectrum sharing.**

I. Introduction

The 3550 MHz to 3700 MHz band in the United States has a three tier access model managed by a spectrum access system (SAS) with the assistance of an environmental sensing capability (ESC). Tier 1 users includes authorized Federal users. Tier 2 and tier 3 users are collectively referred to here as secondary users (SUs). The ESC determines channel availability while the SAS manages access of SUs to the spectrum. Introducing these SUs into the band affects the privacy of the Federal incumbent. Specifically, a malicious SU may gain authorized access to the spectrum and carry out attacks to infer sensitive information about the incumbent by just fusing information given by the SAS. Such an attack is referred to as an *inference attack*.

In a previous work [1], we used simulations to model inference attacks and demonstrated that the privacy of the incumbent can be improved by adjusting the system parameters (i.e., inherent obfuscation). In this paper, we mathematically model attacks that attempt to infer the incumbent's operational frequency through repeated requests for spectrum and validate our analytical model with simulations.

II. System Model

A. Network Model

The SAS manages n channels within a given area. Only l channels are available for use by SUs. We model the SU activity using an $M/M/l/l$ queue [1]. When a SU requests spectrum resources, the SAS replies with an available channel. If no channel is available, the request is denied.

*This paper was written in partial fulfillment of Mrs. Ben Mosbah's doctoral program at Télécom SudParis (France) while working as a guest researcher at NIST.

B. Attack Model

The attacker is a legitimate SU sending queries requesting access to the spectrum. Its initial knowledge is a list of all channels in the band. Once the SAS returns an available channel, the attacker knows that the given channel is not used by the incumbent. Hence, the attacker updates its knowledge by removing it from the list of potential incumbent channels. Let X be the random variable representing the number of queries needed to discover all channels available to secondaries and, hence, the channels used by the incumbents.

III. Analytical Evaluation

In this Section, we show how to compute the expected number of queries needed to infer the incumbent's channel $E[X]$ for two SAS channel assignment schemes: one where the SAS assigns an idle channel at random, and the other where the SAS assigns the lowest-numbered idle channel [1]. In order to calculate this, we use the $M/M/l/l$ queue model and assume the system is in equilibrium.

A. Analysis of the Random Channel Assignment

In the case of the random assignment scheme, the SAS returns a channel at random in reply to an attacker's request. The blocking probability P_B is the probability that all channels are busy at the time of a request and is calculated as follows

$$P_B = \frac{\rho^l}{l!}\left(\sum_{k=0}^{l}\frac{\rho^k}{k!}\right)^{-1}, \tag{1}$$

where $\rho = \lambda/\mu$ is the system load, λ is the aggregate arrival rate, and $1/\mu$ is the individual service time.

In the above system, when the attacker makes a request, the SAS will either return one of the available idle channels or, if all the channels are busy, will respond saying no channel is available. In this case we can express $E[X]$ as

$$E[X] = E[X_b] + E[X_r]\,, \tag{2}$$

where X_b is the number of queries made when all channels were busy, i.e., the request was blocked, and X_r is the number of queries for which an available idle channel was returned by the SAS. We know that

$$E[X_b] = P_B E[X]\,. \tag{3}$$

978-1-5090-2830-6/17/$31.00 ©2017 IEEE

All that remains is to calculate $E[X_r]$. When $1 \leq k \leq l$ channels are idle, then each channel is idle with probability k/l, and if idle will be returned by the SAS with probability $1/k$. Thus each channel has probability $1/l$ of being returned. $E[X_r]$ can then be calculated using the solution to the coupon collector's problem with equal probabilities.

$$E[X_r] = l \sum_{k=1}^{l} \frac{1}{k} = lH_l \,, \tag{4}$$

where H_l is the l^{th} harmonic number [2]. Thus, we have

$$E[X] = \frac{lH_l}{1 - P_B} \,. \tag{5}$$

B. Analysis of the Ordered Channel Assignment

In the case of the ordered assignment scheme, channels are assigned to incoming requests with unequal probabilities. We need to find the probability p_j that the SAS will return channel j in reply to an attacker's request. This is equivalent to the probability that channel j is the lowest available idle channel at the time of an attacker's request.

Let B_j be the probability that an arriving request finds the first j channels busy. The conditional probability that an arriving request finding the first $j-1$ channels busy also finds channel j busy is B_j/B_{j-1}. If $\gamma_j(z)$ is the Laplace-Stieltjes transform of the distribution function of elapsed time between successive times when an arriving request finds the first $j-1$ channels busy and is assigned channel j [3], then

$$\gamma_j(\mu) = \frac{B_j}{B_{j-1}} \,, \tag{6}$$

where $B_0 = 1$ and $\gamma_j(z)$ is defined by the recurrence relation.

$$\gamma_{j+1}(z) = \frac{\gamma_j(z+\mu)}{1 - \gamma_j(z) + \gamma_j(z+\mu)}, \quad j = 1, 2, \ldots \tag{7}$$

$$\gamma_1(z) = \tfrac{\lambda}{\lambda+z} \,.$$

Note that it follows from equation (6) and $B_0 = 1$ that

$$B_j = \gamma_1(\mu) \cdots \gamma_j(\mu), \; j = 1, 2, \ldots \tag{8}$$

Using the above, we calculate the probabilities p_j. Let I_j be a random variable representing the state of channel j, where 1 means the channel is busy and 0 means that it is idle. Then,

$$\begin{aligned} p_j &= Pr\{I_1 = 1, ..., I_{j-1} = 1, I_j = 0\} \\ &= (1 - B_j/B_{j-1})\, B_{j-1} \\ &= B_{j-1} - B_j \,. \end{aligned} \tag{9}$$

Note that $P_B = B_l$ and $P_B + \sum_{j=0}^{l} p_j = 1$.

We can find $E[X]$ by using the p_j as calculated above in the solution to the coupon collector's problem for unequal probabilities in [2]

$$E[X] = \sum_{i=1}^{l} \frac{1}{p_i} - \sum_{i<j} \frac{1}{p_i + p_j} + \sum_{i<j<k} \frac{1}{p_i + p_j + p_k} - \cdots \tag{10}$$

$$\cdots + (-1)^{l+1} \frac{1}{p_1 + \cdots + p_l} \,.$$

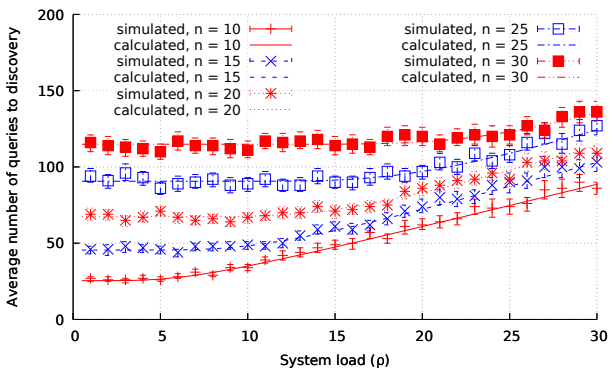

Fig. 1. Analytical results vs. simulation results for the random scheme

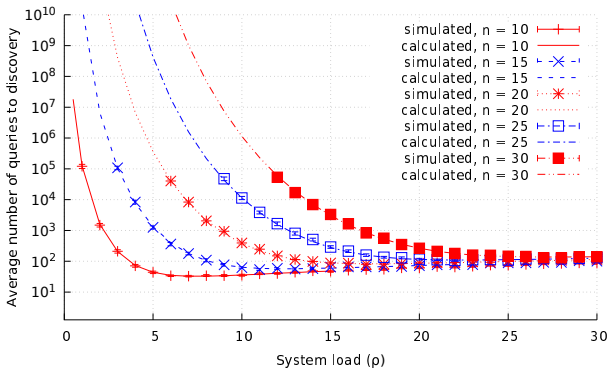

Fig. 2. Analytical results vs. simulation results for the ordered scheme

IV. Analytical Results

Our system includes one incumbent, one SAS and one attacker within the same area. The incumbent is operating on one channel. So, $n-1$ channels are available for use by SUs. We compute $E[X]$ analytically and by simulation with a confidence interval of 95 % for different values of n and ρ. In Fig. 1, where channels are randomly assigned, we note that the simulation results are within the confidence interval of the analytical model results for all values of ρ. In Fig. 2, where channels are assigned order-wise, simulation results also match the analytical model results.

V. Conclusions

We have proposed an analytical model to calculate the average number of queries needed to infer the operational channel of the incumbent. This model provides insight into the limit that the SAS may set on the query rate in order to minimize the risk of inference to the incumbent.

References

[1] A. Ben Mosbah, T. A. Hall, M. Souryal, and H. Afifi, "Analysis of the vulnerability of the incumbent frequency to inference attacks in spectrum sharing," in *IEEE Consumer Communications and Networking Conference (CCNC'17)*, Las Vegas, NV, Jan. 2017.

[2] M. Ferrante and M. Saltalamacchia, "The coupon collector's problem," *Materials matemàtics*, pp. 1–35, 2014.

[3] R. B. Cooper, "Queues with ordered servers that work at different rates," *Opsearch*, vol. 13, no. 2, pp. 69–78, 1976.