



**HAL**  
open science

# Analysis of the Vulnerability of the Incumbent Frequency to Inference Attacks in Spectrum Sharing

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

► **To cite this version:**

Azza Ben-Mosbah, Timothy A. Hall, Michael Souryal, Hossam Afifi. Analysis of the Vulnerability of the Incumbent Frequency to Inference Attacks in Spectrum Sharing. The 14th Annual IEEE Consumer Communications & Networking Conference, Jan 2017, Las Vegas, NV, United States. hal-01494122

**HAL Id: hal-01494122**

**<https://hal.science/hal-01494122v1>**

Submitted on 4 Apr 2017

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Analysis of the Vulnerability of the Incumbent Frequency to Inference Attacks in Spectrum Sharing

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

**Abstract**—Sharing between commercial and Federal incumbent users, such as in the 3.5 GHz band, is expected to increase the availability of spectrum for wireless broadband use. However, the spectrum coordination needed between incumbent and commercial users gives rise to several privacy concerns. This paper analyzes the vulnerability of the incumbent’s operational center frequency to disclosure from inference attacks. We evaluate the inherent protection provided by two channel assignment schemes in terms of the time required for an attacker to infer the incumbent’s frequency. We account for the activity of secondary users in a dynamically-shared environment. This analysis allows the Spectrum Access System to quantify privacy for a given secondary load. It also provides an analytical framework to quantify the effectiveness of countermeasures such as limiting the query rate of secondaries.

**Index Terms**—3.5 GHz, channel assignment, Federal bands, inference attack, privacy protection, spectrum sharing.

## I. INTRODUCTION

Recently, spectrum sharing has been proposed in order to make more efficient use of statically managed frequency bands. For example, in the U.S., the Federal Communications Commission (FCC) has selected a multi-tiered shared access model, managed by a Spectrum Access System (SAS), to assign spectrum resources in the 3.5 GHz band without causing interference to incumbent operations [1].

While the main concern in the scientific literature has been interference management, additional concerns have been raised. Incumbents such as military and public safety users require full protection of their operations, not only from harmful interference, but also from exposure of confidential information. Bahrak et al. [2] define an inference attack, where knowledge acquired from the sharing environment can be used to infer sensitive information about the incumbent. The operational parameters of primary users, such as location, frequency, and time of operation are sensitive and should not be revealed. Specifically, protecting the operational frequency of an incumbent against inferences can be critical to mitigate intentional interference (a jamming attack).

Our contributions consist of modeling secondary activity as an Erlang queueing system, analyzing inference attacks

on the incumbent’s operational frequency to evaluate inherent obfuscation and the effectiveness of countermeasures. In Section II, we present our system modeling to quantify the privacy vulnerability. Section III demonstrates the analysis of simulation results. Finally, Section IV summarizes the findings and discusses future works.

## II. VULNERABILITY ANALYSIS

### A. Channel Assignment Schemes

We consider two channel assignment schemes that can be used by the SAS:

- *Random channel assignment* assigns channels to secondaries randomly from the list of available channels.
- *Ordered channel assignment* assigns channels to secondaries in an order-wise fashion, and any particular order can be employed.

### B. Simulation Model

We divide the band into  $n$  equal channels. We consider a sample system including one incumbent, one SAS and one adversary within the same area. The incumbent is operating on a single channel. Secondaries share the use of the remaining  $n - 1$  channels. The SAS manages access to those channels. Secondaries query the SAS according to a Poisson process with aggregate rate  $\lambda$ , and the service time is exponentially distributed with rate  $\mu$ . Once all channels are occupied, new access requests will be denied. This is known as an Erlang loss system [3].

We assume that the attacker is one of the secondaries and is trying to infer the operational channel of the incumbent. We also assume that the channels available for use by secondaries do not change during the incumbent’s active period. For each query, the SAS replies with one available channel. The attacker does not know a priori the channel assignment scheme used by the SAS. It only uses the information given by the SAS and does not have access to any external knowledge. Its initial knowledge is a list of all potential incumbent channels (i.e., all  $n$  channels). Once the SAS returns a channel in reply to a query, the attacker knows that channel is not used by the incumbent. Hence, the attacker updates its knowledge by removing the returned channel from the list of potential channels used by the incumbent.

<sup>\*</sup>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.

### C. Privacy Metrics

1) *Distance of inference*: The inference process can be regarded as a discovery process of all channels available for use by secondaries. Therefore, we can evaluate privacy as a measure of “distance,” that is, the number of channels remaining to be discovered.

2) *Cost of inference*: In spectrum sharing, the attacker invests effort to infer sensitive data. We measure the inference cost to the attacker in terms of how long the attacker takes to acquire the inferred knowledge and the number of queries to acquire that knowledge.

## III. RESULTS AND DISCUSSION

We conducted this work to analyze the vulnerability of the incumbent’s frequency to inference attacks and determine inherent privacy-preserving techniques to thwart them. We conclude that the values of system parameters have a significant effect on the privacy of incumbents.

Implementing an ordered channel assignment scheme is effective in all cases, regardless of the spectrum load  $\rho$  or the attacker’s query rate  $\lambda_a$ . Since randomness in the channel assignment scheme adds diversity to the query responses, it allows the attacker to infer the incumbent’s channel in less time. Hence, the use of the ordered scheme raises both the distance (Fig. 1) and the cost (Fig. 2) of inference, i.e., an attacker will take more time to infer the same information.

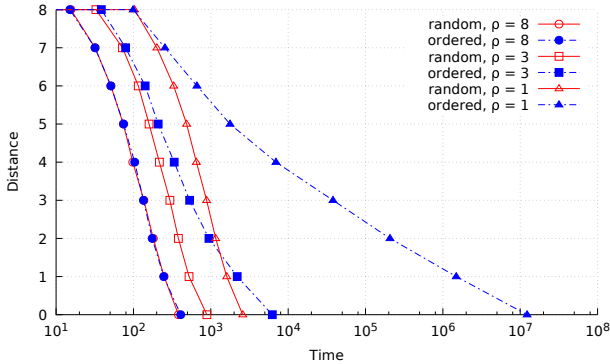


Fig. 1. Effect of the time on the inherent obfuscation ( $n = 10$ )

An attacker can fake different identities, get help from other secondaries or just flood the system with queries in order to speed up the inference process. Limiting the secondary users query rate can be an efficient way to mitigate the inference of the incumbent frequency during the operational period. For example, Fig. 3 suggests that if, in a system with  $\rho = 5$ , the incumbent needs  $\frac{10}{\mu}$  time units to use the channel and leave, the SAS should limit a user’s query rate to  $3\mu$  when using random channel assignment and to  $10\mu$  when using ordered channel assignment, under moderate load. For  $\rho = 1$ , using an ordered channel assignment scheme is the best approach.

As a result, the SAS should implement effective privacy-preserving techniques by calibrating some adjustable parameters (channel assignment scheme, query rate of secondaries) to the system load.

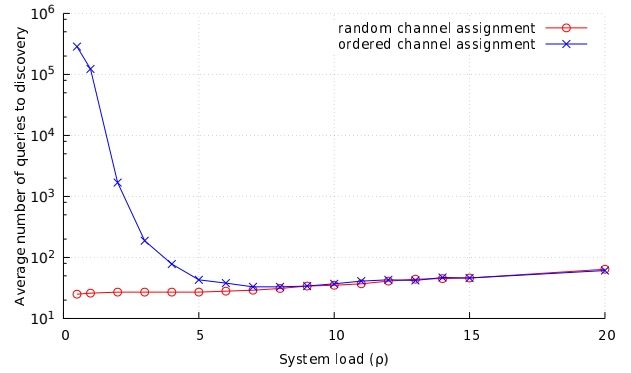


Fig. 2. Effect of the spectrum load on the inherent obfuscation ( $n = 10$ )

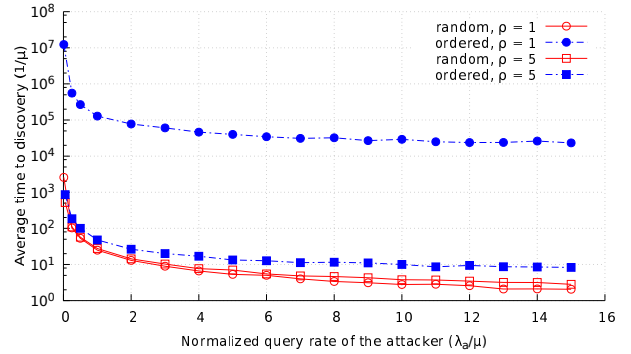


Fig. 3. Effect of the attacker’s query rate on the inherent obfuscation ( $n = 10$ )

## IV. CONCLUSIONS

Spectrum sharing in Federal bands can be productive yet challenging because of the privacy needs of the incumbents. This analysis sheds light on the impact of different system parameters on the privacy of the incumbent. Ordered channel assignment significantly enhances privacy as measured by an attacker’s ability to infer the channel used by the incumbent. However, when the system load is high, the channel assignment scheme is irrelevant. One way to mitigate the inference risk is to limit the query rate (i.e., number of queries) per secondary user. This will prevent aggressive attackers from expediting the inference process.

In a real world scenario, an attacker may have other sources of information. So, it may be necessary to use additional obfuscation techniques to increase the cost of inference or the anonymity of the incumbent’s channel.

## REFERENCES

- [1] “Amendment of the commission’s rules with regard to commercial operations in the 3550-3650 mhz band, gn docket no. 12-354,” Federal Communications Commission (FCC),” Report and Order and Second Further Notice of Proposed Rulemaking, Apr. 2015.
- [2] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, and D. Gurney, “Protecting the primary users’ operational privacy in spectrum sharing,” in *IEEE International Symposium on Dynamic Spectrum Access Networks (DYSpan’14)*, McLean, VA, Apr. 2014, pp. 236–247.
- [3] J. M. Chaiken and E. Ignall, “An extension of Erlang’s formulas which distinguishes individual servers,” *Journal of Applied Probability*, vol. 9, no. 1, pp. 192–197, Mar. 1972.