# Analysis of the Vulnerability of the Incumbent Frequency to Inference Attacks 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*—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 quantifies 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 access system, spectrum sharing.**

## I. Introduction

Spectrum sharing has been proposed in order to make more efficient use of statically managed frequency bands. Recently, in the U.S., the Federal Communications Commission (FCC) 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 literature on spectrum sharing 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. In other words, a legitimate secondary user may combine the query responses of the SAS to gain unauthorized access to operational parameters. 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 inference attacks can be critical in mitigating intentional interference (a jamming attack).

Our contributions consist of modeling secondary activity as an Erlang queueing system, and analyzing inference attacks on the incumbent's operational frequency to evaluate inherent obfuscation of various channel assignment schemes and the effectiveness of countermeasures. In Section II, we present our system model to quantify the privacy vulnerability. Section III demonstrates the analysis of simulation results. Finally, Section IV summarizes the findings and discusses future work.

## II. Vulnerability Model

### A. Channel Assignment Schemes

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

1) *Random channel assignment* assigns channels to secondaries randomly from the list of available channels. For example, as shown in Fig. 1, consider one incumbent $I$ operating on a channel $f_2$ and four secondaries $S_1$, $S_2$, $S_3$ and $S_4$, who requested channels in that order. Aside from channel $f_2$, which is not allowed for use by any secondary, channels are assigned randomly from the idle channels with uniform distribution.

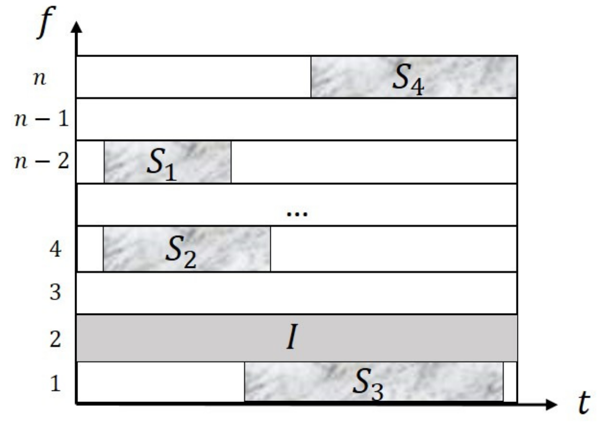

Fig. 1. Example of a random channel assignment

*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.

2) *Ordered channel assignment* assigns channels to secondaries in an order-wise fashion, and any particular order can be employed. To increase the obfuscation of this scheme, the order can change from one operational period to another. For example, in Fig. 2, we choose to illustrate an ascending channel assignment scheme without loss of generality. In other words, if we consider one incumbent and $n-1$ available channels, for each query, the SAS returns the lowest available channel at the time of query. Intuitively, this scheme will increase privacy by reducing an attacker's probability of visiting all available channels. However, since channels are prioritized, some channels may get over-utilized.

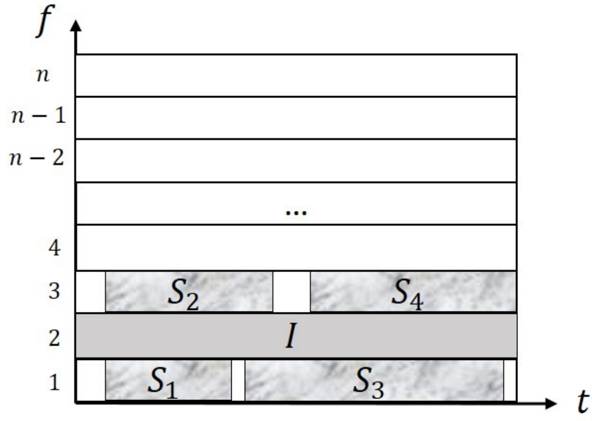

Fig. 2. Example of an ordered channel assignment

### 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 $\mu$. The system load is defined as $\rho = \frac{\lambda}{\mu}$. 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.

### 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 analyzed the effect of the channel assignment scheme and the attacker query rate on incumbent frequency privacy.

### A. Effect of the channel assignment scheme on privacy

The choice of channel assignment scheme has a significant impact on privacy. A random channel assignment scheme adds diversity to the query responses, allowing the attacker to infer the incumbent's channel in less time. Ordered channel assignment achieves significantly greater privacy at light system loads ($\rho = 1$ in Fig. 3 and $\rho = 5$ in Fig. 4) and at medium system loads ($\rho = 3$ in Fig. 3 and $\rho = 15$ in Fig. 4). At heavier system loads, the privacy achieved by the ordered channel assignment is nearly identical to that of the random channel assignment. Thus, it makes sense to use an ordered channel assignment instead of a random one in all cases.

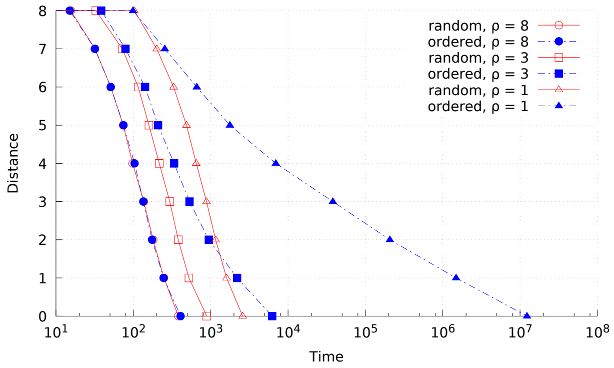

Fig. 3. Effect of the channel assignment scheme (10 channels)

### B. Effect of the query rate on privacy

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. 7 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. Under light

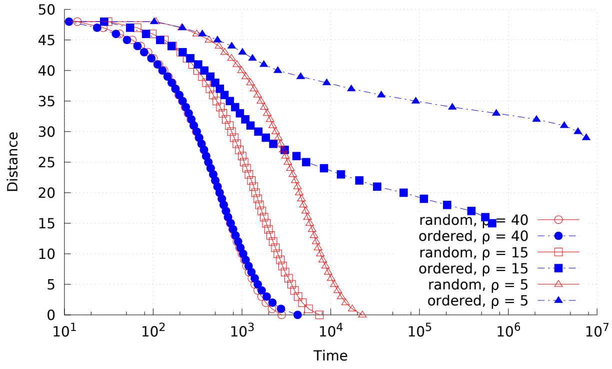

Fig. 4. Effect of the channel assignment scheme (50 channels)

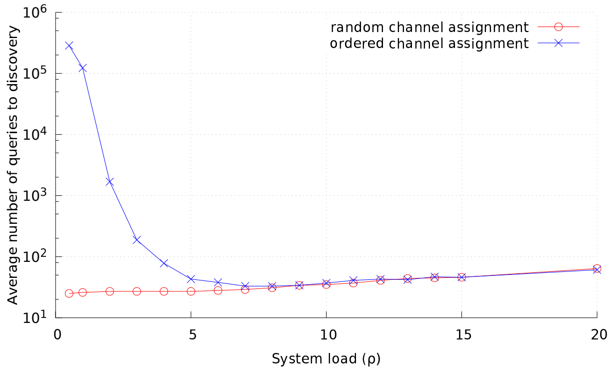

Fig. 5. Cost of inference vs. System load (10 channels)

load ($\rho = 1$ in Fig. 8), the query rate limit with ordered channel assignment can be much higher.

The results of this analysis highlight the merits of the ordered channel assignment in protecting the incumbent privacy, and more importantly, can be used to guide the selection of SAS query rate limits.

## 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.

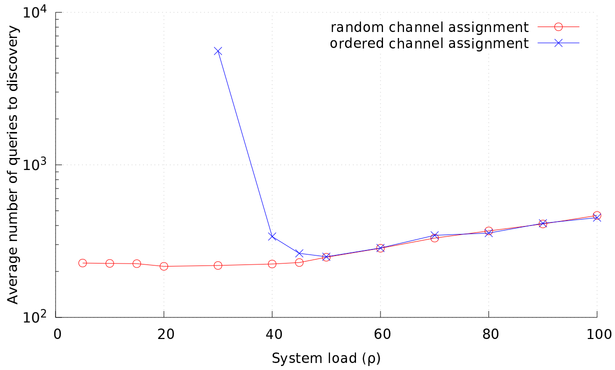

Fig. 6. Cost of inference vs. System load (50 channels)

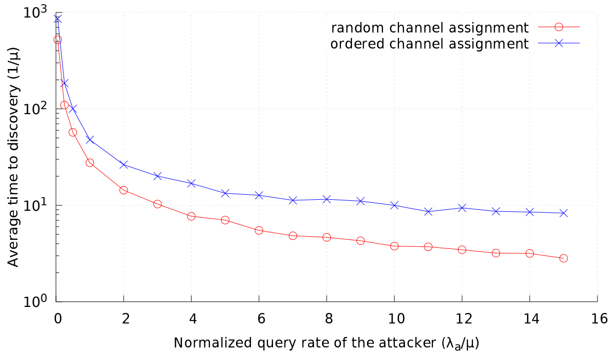

Fig. 7. Effect of the attacker's query rate on the time to discovery (10 channels, 50 % system load)

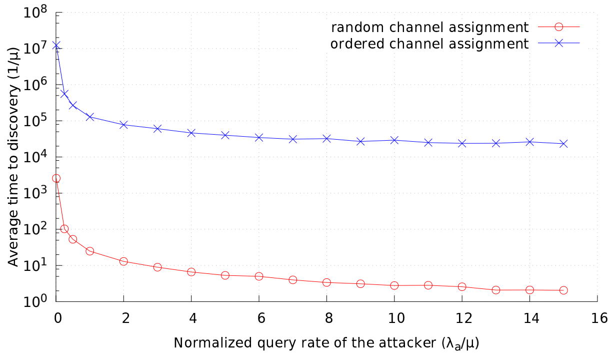

Fig. 8. Effect of the attacker's query rate on the time to discovery (10 channels, 10 % system load)

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.