Interception of Frequency-Hopping Signals for TEMPEST Attacks

Corentin Lavaud, Robin Gerzaguet, Matthieu Gautier, Olivier Berder, Erwan Nogues, Stephane Molton

Interception of Frequency-Hopping Signals for TEMPEST Attacks

Corentin Lavaud*, Robin Gerzaguet*, Matthieu Gautier*
Olivier Berder*, Erwan Nogues**, Stephane Molton**
* Univ Rennes, CNRS, IRISA {surname.name@irisa.fr}
** DGA-MI {surname.name@intradef.gouv.fr}

***Abstract*—Any information system must ensure the confidentiality of its sensitive data during its operation. Among the vulnerabilities, TEMPEST attacks appear to be an important threat as this sensitive data can be emitted through unwanted electromagnetic waves generated by hardware operation and can therefore be intercepted by any distant radio frequency receiver. The menace is worst when sensitive data is mixed with an internal communication device as the leak is hidden within a legitimate communication channel and difficult to find. It can happen for instance when an audio processing unit like a microphone or amplifier is close to a transmission security (TRANSEC) transmitter, leading to the emanation of the audio signal through the TRANSEC which follows a frequency hopping scheme. This paper focuses on detection of the used channel of a frequency hopping system, when the system bandwidth is very large and the number of hops per second is very high (TRANSEC case). By obtaining this channel information, the audio stream can be recovered, leading to a potential high security break.**

***Index Terms*—TEMPEST, TRANSEC, Frequency Hopping, Software Defined Radio.**

I. Introduction

Information systems are now intrinsically linked to any operation from a private individual to the administration and the military. As a consequence, their confidentiality (i.e preserving that the data exchanged remained in the desired hands) is a vital issue at multiple scales. One of the most common mechanisms used to ensure confidentiality is the use of cryptography. It guarantees data protection by making it unreadable for any outside person who might intercept it. But are we sure that the data can not spread out of the system before being protected ?

While operating, information processing devices or communication systems may emit signals through unwanted electromagnetic waves. This activity may be correlated with the information being processed, leading to a potential information leakage. This leaked information is called a compromised signal and its presence can be spotted by the use of a radio frequency receiver [1] [2] in a so-called Electromagnetic (EM) side-channel. The proposed paper focus on EM TEMPEST attacks [3] where the compromised signal is hidden in a legitimate transmission making the interception trickier.

The existence of these side-channels are not new but several reasons make the threat even more terrifying: i) devices tend to work at higher frequency, increasing the number and the range of unwanted EM emission, ii) more and more communication chips can cohabit on the same device, leading to an increased number of possible active side-channels by internally mixing the compromised signal iii) Software Defined Radio (SDR) [4], programmable devices are now capable to intercept those signals at low cost with a high bandwidth.

Many studies of the literature focus on permanent emanation side-channels (a side-channel where the carrier continuously transmits at a constant frequency). This eases the interception as most of the state-of-the-art detection and estimation algorithms relies on averaging in order to better estimate the data. Some other articles focus on sporadic channels in time or frequency, but either maintain the frequency constant or a low number of hops per second [5] or force frequent re-emission through traffic overhead [6]. In this paper, we focus on a sporadic side-channel with frequency hopping (FH) carrier. This use-case may correspond to a scenario when a compromising signal (for instance an audio signal) is modulated by a transmission security (TRANSEC) transmission system due to the physical proximity between a microphone and a turned-on TRANSEC transmitter. Retrieving the TRANSEC carrier would provide the compromised signal (i.e the audio signal). However, it is overly complex to know the hop sequence of the TRANSEC and so it has to be estimated [7].

To recover the compromised signal, FH signal has to be firstly detected and extracted from the radio spectrum then the compromised signal has to be decoded depending of its nature (mainly driven by its relative bandwidth compared to the FH one). Some studies on FH channel detection exist but deals with few hops per seconds [8] or based on complex methods [9] that cannot cope with very large instantaneous bandwidths.

This paper proposes a low complex digital algorithm that allow to recover an audio signal modulated by a FH scheme. The rest of this paper is divided into four sections. Section II describes the leak model while Section III presents the proposed interception system. Section IV validates the channel detection performance, while Section V eventually draws some conclusions and perspectives.

II. Leak model

A baseband message $b(t)$ (e.g TRANSEC) of bandwidth F_b is mixed with the compromised signal assumed to be an audio signal $r(t)$. The audio bandwidth F_r is smaller than the one of

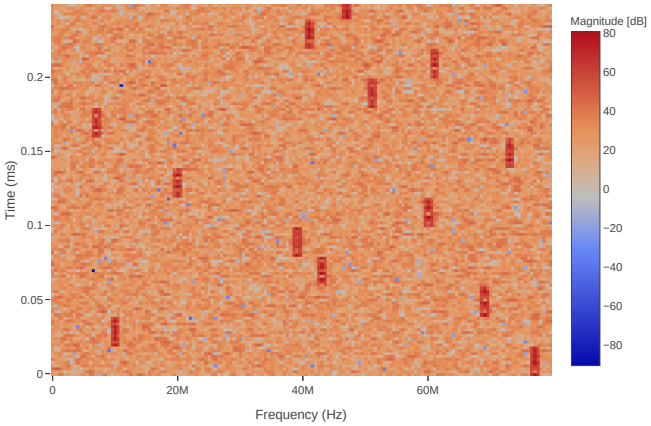

Fig. 1. Time-frequency instantaneous power of a FH signal.

$b(t)$ and of the order of several kHz. Due to proximity between the FH emitter and the microphone, the two signals are mixed. The mixing is defined as a weighted addition parameterized by the mixing coefficient h whose typical value is lower than 1%. This signal is finally modulated following the FH sequence, resulting in a $F_s = 80$ MHz bandwidth transmitted signal:

$$x(t) = [b(t) + h \times r(t)]\, e^{2j\pi f_k t}, \tag{1}$$

with f_k the associated channel frequency of the current transmitted symbol of $b(t)$. Assuming that N channels can be used, then

$$f_k = k \times F_b = \frac{k \times F_s}{N},\ k = 0, \ldots, N-1. \tag{2}$$

The same FH index k is maintained constant for a slot duration T_b and thus is used for several consecutive symbols and $\lambda = \frac{T_b}{N}$ is denoted the so-called repetition factor. Figure 1 shows a typical time-frequency grid of a typical transmitted TRANSEC signal composed of 1 MHz FH channels covering the 80 MHz bandwidth with a slot duration of 1μs. In the following, the received signal $d(t)$ is delayed by τ and is supposed to only be impaired by an Additive White Gaussian Noise (AWGN) of variance σ_n^2 and is therefore expressed as

$$d(t) = x(t - \tau) + n(t). \tag{3}$$

III. Interception Method

Both a low complex FH estimator and audio recovering stage are proposed in this section. The proposed solution is described in Figure 2. This solution can cope with any FH systems and is not restricted to TRANSEC case. It can be for instance directly applied to a Bluetooth leakage. This method particularly targets systems with very low slot duration (low value of λ), more difficult to estimate.

To deal with the large bandwidth, the interception method is supposed to be implemented in a high performance SDR that embeds both hardware and software computational resource. The blue stages operate at the higher rate (F_s) and should therefore be implemented in the hardware resources, whereas the green and orange stages operate at lower rates and can be implemented in the software resource. The analog-to-digital converter (ADC) from the SDR device samples the signal at the maximum FH rate (i.e F_s).

The FH identification block aims to identify the main FH parameters: the slot duration T_b, the number of channels N, and the synchronisation delay τ. The two first parameters may be known when the target FH standard is known (for instance Bluetooth) and the associated estimations may be deactivated in this case. The latter parameter τ has always to be estimated to be synchronized with the hops. This processing has only to be done at the beginning of the operation as the estimated parameters are not likely to change. In this paper, this block will not be described and a synchronized signal will be assumed.

The time synchronisation block aims to shift the incoming buffers to match the FH hop, based on the delay estimation τ. The blocks provide a synchronized input $\hat{d}[s]$ sampled at F_s of size λN associated to an unknown FH center frequency f_k to estimate.

The FH detector estimates which channel is used. The detector is based on the instantaneous periodogram, averaged by the repetition factor λ. Considering the input $\hat{d}[s]$, the associated estimated channel index $\hat{p}$ is expressed as

$$\hat{p} = \underset{p \in [0; N-1]}{\arg\max} \left\{ \sum_{l=0}^{\lambda-1} \left| \sum_{m=0}^{N-1} \hat{d}[lN + m] e^{\frac{-j2\pi mp}{N}} \right|^2 \right\}. \tag{4}$$

Then the chosen index (linked to the central frequency by $\hat{f}_k = \frac{\hat{p}F_s}{N}$) is used in the de-rotor that shifts the modulated channel into baseband (circle operator in Figure 2):

$$\hat{d}_{\mathrm{BB}}[s] = \hat{d}[s] e^{\frac{-j2\pi s \hat{f}_k}{F_s}}. \tag{5}$$

The filtering stage lowers the rate of the detected signal from F_s to F_b. If the correct FH channel has been chosen, and assuming an ideal filtering operation, the resulting signal is the weighted sum of the TRANSEC message $b(t)$ and the audio message $r(t)$. Finally, to recover the audio signal, two solutions can be used. The first one consists in decoding $b(t)$ and applying an interference cancellation scheme. This is however costly and requires the full $b(t)$ decoding stage (especially when $b(t)$ is of an unknown nature if not unstandardized). The other solution relies on the fact that the compromising signal $r(t)$ has a lower rate than the legitimate signal $b(t)$. Hence, a harsh low pass filter can applied around the audio frequencies without lowering too much the decoding quality.

The proposed structure aims to recover the FH signal while initially being sampled at the full bandwidth (at F_s). It requires a perfect time-frequency localisation. To that goal, the frequency estimation is averaged by a factor λ and is therefore enhanced. It is important to monitor the required time/frequency precision to ensure good decoding performance.

IV. Simulation results

The performance of the detector is evaluated in terms of Channel Error Rate (CER), defined as the probability that the

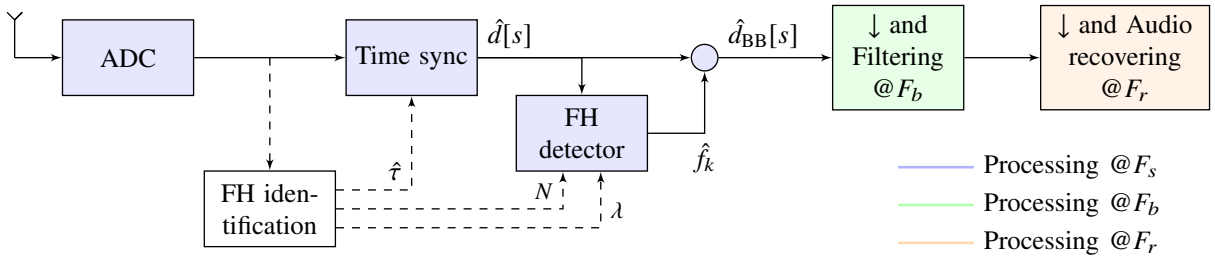

Fig. 2. Proposed architecture of the interception system.

estimated channel index $\hat{p}$ differs from the effective channel index p. Figure 3 shows the CER versus the signal-to-noise ratio (SNR) defined from (3) as σ_x^2/σ_N^2 with σ_x^2 the variance of the mixed signal defined in (1). This CER is computed for various values of λ and different synchronisation errors. The simulation parameters are $N = 80$, $F_s = 80\,\text{MHz}$, $F_b = 1\,\text{MHz}$, $F_r = 40\text{kHz}$, h=1%. The value of λ is associated to slot durations from 2 μs ($\lambda = 2$) to 200μs ($\lambda = 200$). It shows that the detector is more resistant to the noise for high value of λ, as the noise is averaged.

When it comes to the synchronisation error (defined as $\Delta\tau = (|\tau - \hat{\tau}|)/T_b$), Figure 3 shows that the required fine synchronisation is linked to the slot duration. Indeed, in case of synchronisation mismatch, some of the inputs of the periodogram would be associated to the previous or to the next slot. In the meantime, one can said that a synchronisation error lower than 10% of the slot duration leads to a negligible performance penalty. This metric is fruitful to build a simple yet functional synchronisation stage.

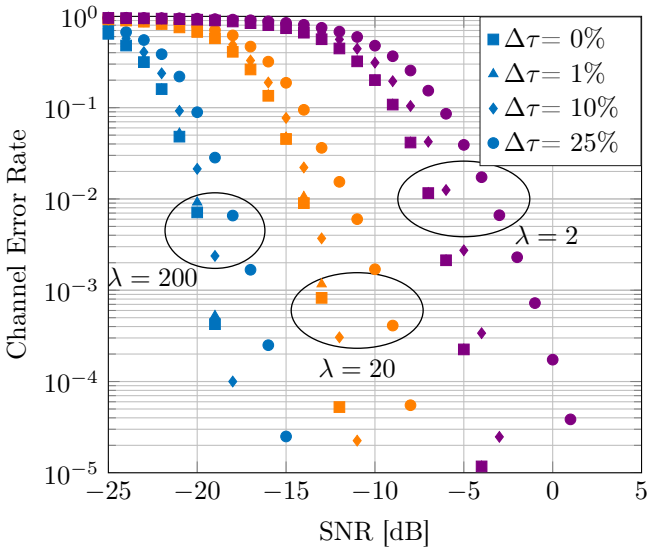

Fig. 3. Channel Error Rate vs SNR for various λ and delay errors Δ_τ.

V. Conclusions & Future Works

This paper focused on the recovering of an audio signal into a frequency hopping legitimate transmission. Side-channel can lead to a unbearable leak of sensitive data, and is difficult to detect especially when carried by an electro-magnetic wave. In this paper, we focused on a TRANSEC legitimate channel that was bearing a sensitive audio stream. As TRANSEC systems are based on frequency hopping with a high number of hops per second over a wide bandwidth, we have proposed a new frequency hopping detection scheme with low complexity and capable to estimate the used channel even with a very small slot duration. We have demonstrated that with such a method the required time synchronisation can be relaxed to 10% of the slot duration. Next steps will be to work on the coarse synchronisation and to propose a real time implementation of the method on a Software Defined Radio.

Acknowledgement

This study is supported by the Pôle d'Excellence Cyber.

References

[1] W. V. Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, no. 4, pp. 269–286, Dec. 1985.

[2] M.Vuagnoux and S. Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," in *USENIX Security Symposium*, Aug. 2009, pp. 1–16.

[3] NSA, *NACSIM 5000: Tempest Fundamentals. National Security Agency*, Partially declassified transcript: http://cryptome.org/nacsim-5000.htm, Feb. 1982.

[4] A. A. Abidi, "The path to the software-defined radio receiver," *IEEE Journal of Solid-State Circuits*, vol. 42, no. 5, pp. 954–966, 2007.

[5] G. Camurati, S. Poeplau, M. Muench, T.Hayes, and A. Francillon, "Screaming channels: When electromagnetic side channels meet radio transceivers," in *Proc. ACM conference on Computer and communications security (CCS)*, Oct. 2018.

[6] T. Wei, S. Wang, A. Zhou, and X. Zhang, "Acoustic Eavesdropping through Wireless Vibrometry," in *Proc. International Conference on Mobile Computing and Networking (MobiCom)*, Sep. 2015.

[7] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, 2011.

[8] L.-L. Yang and L. Hanzo, "Software-defined-radio-assisted adaptive broadband frequency hopping multicarrier DS-CDMA," *IEEE Communications Magazine*, vol. 40, no. 3, pp. 174–183, 2002.

[9] S. Barbarossa and A. Scaglione, "Parameter estimation of spread spectrum frequency-hopping signals using time-frequency distributions," in *IEEE signal processing workshop on signal processing advances in wireless communications*, 1997, pp. 213–216.