Au-delà des économies d'énergie : le micro espion soviétique qui ne consommait pas

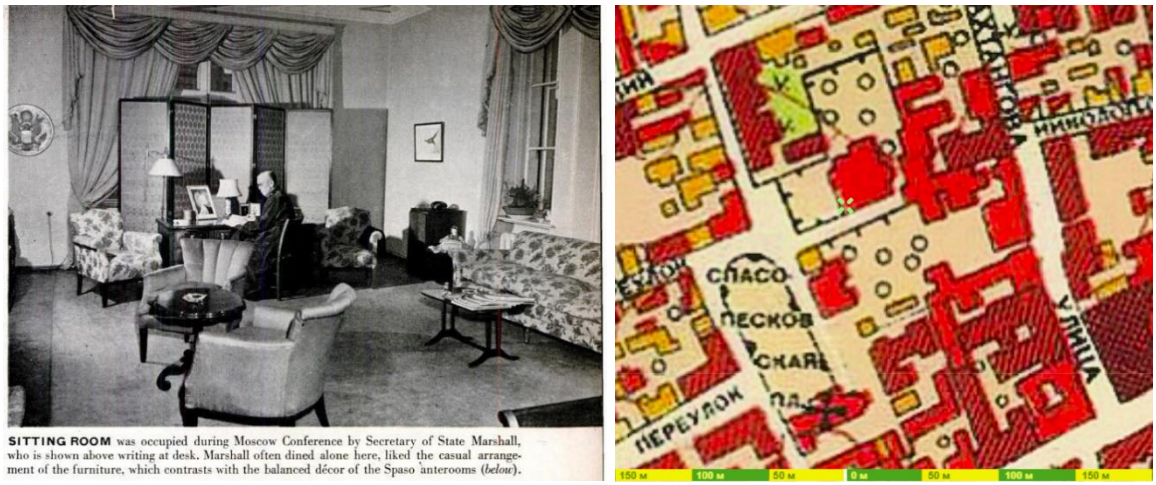
S. Hemour[a,d], N. Barbot[b], F. Collin[c], J.-L. Lachaud[a], S. Destor[a], J. Tomas[a,d]

[a] Laboratoire IMS, CNRS UMR 5218, Bordeaux INP, Université de Bordeaux, France
[b] LCIS, UGA, Grenoble INP, Valence, France
[c] ENSEIRB-MATMECA, Bordeaux, France
[d] Pôle CNFM de Bordeaux (PCB), U. de Bordeaux, Talence, France
Contact email : simon.hemour@u-bordeaux.fr

Cet article présente la mise en place de projets étudiants aux niveaux BUT et Master sur la thématique de la récupération d'informations par un microphone purement passif et uniquement alimenté par un signal radio. Un tel dispositif est inspiré par le micro espion soviétique découvert au sein de l'ambassade des Etats-Unis à Moscou dans les années 50. Il a été reproduit à l'identique ainsi que son écrin en bois sculpté. Il est aussi utilisé pour la vulgarisation scientifique

I. Introduction

Août 1945, URSS. Le troisième Reich est maintenant tombé, et l'ambassadeur américain à Moscou rencontre une délégation de scouts soviétiques dans le cadre du renforcement des liens diplomatiques entre les USA et l'URSS. En signe d'amitié, les enfants lui offrent une magnifique réplique en bois du grand Sceau des États-Unis, sculptée de leurs propres mains. L'ambassadeur américain, ravi par cette impressionnante pièce en bois d'érable, l'accroche dans la *Sitting Room* de sa résidence, *Spaso House* à Moscou (Fig.1).



(a) (b)

Fig.1. (a) Image tirée d'un reportage américain, couvrant le déplacement en mars-avril 1947 du secrétaire d'état George Marshall à Moscou. La sculpture du Grand Sceau est à cette époque encore accrochée au mur (1) de la pièce qui est probablement à l'angle de la façade sud et ouest (2) (b) Carte de Moscou en 1951 (3) indiquant *Spaso House* au centre et les nombreux bâtiments aux alentours dont l'un aura fort probablement servi de poste d'écoute.

Article publié par EDP Sciences et disponible sur le site https://www.j3ea.org ou https://doi.org/10.1051/j3ea/20241011

(a) (b)

Fig.2. (a) Réplique du Grand Sceau des Etats-Unis d'Amérique (56 cm de diamètre) avec emplacement du micro espion (23cm de long), communément appelé « *The Thing* », « *The Great Seal Bug* » ou « *Endovibrator* » (4). (b) Vue éclatée du micro espion. La membrane métallique n'est pas représentée.

Nous sommes à présent en 1951 puis 1952, Moscou, URSS. Des voix anglaises et américaines sont entendues sur des bandes radio soviétiques par des employés de l'ambassade chargés de leur surveillance. Le Département d'État Américain dépêche des recherches approfondies de l'ambassade et de *Spaso House*, qui aboutira sur la découverte d'un mouchard dissimulé à l'intérieur de la sculpture du Grand Sceau (Fig.1).

Le micro espion, qualifié de très haute technologie selon les rapports d'époque, ne disposait pas de sa propre source d'énergie et n'était pas relié par des fils. Au lieu de cela, le dispositif réfléchissait de manière passive le puissant signal radio provenant de l'extérieur par lequel il était éclairé par un poste du NKGB (**НКГБ :* Народний Комиссарят Государственной Безопасности, en français : Commissariat du peuple à la sécurité gouvernementale, qui prit plus tard le nom de KGB). Ce principe de rétro-modulation conférait au mouchard une durée de vie pratiquement illimitée et permit aux agents Soviétiques d'obtenir des renseignements de premier choix durant la mandature de trois ambassadeurs américains successifs.

Reconstruit par le laboratoire IMS de Bordeaux, suite à la déclassification d'un rapport technique du FBI en 2019 (5), le micro espion rassemble tous les ingrédients d'une « *success story* » pédagogique : l'élégance du principe de fonctionnement (cavité micro-onde à fréquence de résonance variant selon la position de la membrane du micro), le type de signaux retransmis (variation de coefficient de réflexion (S11) de la cavité produisant une modulation d'amplitude), et son application pour l'espionnage suscitent toujours beaucoup d'intérêt et d'engagement de la part des étudiants.

II. Principe de fonctionnement

La cavité micro-onde a été reproduite à l'atelier de mécanique du Laboratoire IMS en suivant les dimensions originales (Fig.1b.) (5). Une fois connectée à une antenne, elle se comporte comme un filtre passe-bande à fréquence de coupure variable, allant de l'état où toute l'énergie est absorbée dans la cavité, jusqu'à l'état où toute l'énergie est réfléchie vers l'antenne. Si la membrane du micro fait varier ces deux états en fonction de l'excitation acoustique, le signal d'éclairage est modulé en réflexion, c'est-à-dire que le coefficient de réflexion, (et donc son delta□RCS, Delta Radar Cross Section (6)) varie en fonction du temps selon le principe de la modulation d'amplitude (figure 4b) (7). Le dispositif est complètement passif, et ne nécessite ni batteries, ni dispositif de capture et rectification

d’énergie radiofréquence comme systématiquement implémenté aujourd’hui dans les capteurs RFID (8).

III. Principe de la mesure à l’analyseur de réseau et à distance

Contrairement au dispositif d’écoute de l’époque qui utilisait séparément une source et un récepteur radiofréquence, nous utilisons avec les étudiants un analyseur de réseau (VNA) dans une configuration spécifique.

Le principe de fonctionnement classique d’un VNA est décrit dans la figure 3a. La source interne génère une onde a1, qui est appliquée au dispositif à tester (DUT, Device Under Test). La discontinuité d’impédance présente entre les 50Ω du VNA et l’impédance du DUT donnera naissance à une onde réfléchie b1, qui peut aussi être vue comme une onde de sortie. Le VNA mesure séparément les ondes a1 et b1 pour chaque fréquence, et calcul le ratio entre les deux pour déterminer la valeur complexe du coefficient de réflexion (paramètre S11). Habituellement, l’analyseur de réseau balaye la fréquence f0 entre deux bornes (fréquences START et STOP) : c’est le « *SWEEP MODE* ».

D'un point de vue matériel, les deux ondes sont partiellement prélevées par des coupleurs, translatés en fréquence (down-converted) puis échantillonnées. Par convention, le récepteur ‘A’ mesure l'image de l'onde b1, et le récepteur ‘R’ mesure l'image de l'onde a1, comme indiqué dans le schéma de la figure 3b où la charge présente habituellement un coefficient de réflexion constant à une fréquence donnée (cas d’un dispositif invariant dans le temps). Dans un tel cas, l’onde réfléchie mesurée par le récepteur A est de fréquence fixe. Dans le mode de balayage nul (ZERO SPAN, ou parfois également appelé mode CW), le balayage en fréquence est désactivé. Le VNA ne trace alors plus l’amplitude en fonction de la fréquence balayée, mais l'amplitude (ou la phase) du signal reçu en fonction du temps (Fig.3b.).

Lorsqu'un dispositif variant dans le temps est mesuré (cas du micro espion), l'onde réfléchie b1 n'est plus de fréquence unique, mais modulée (Fig. 4). Elle contient de nombreuses composantes autour de la fréquence « porteuse » initiale a1, ainsi que ses harmoniques. Si la bande de fréquence occupée par la modulation est inférieure à la largeur de bande du filtre IF (fréquence intermédiaire), les variations temporelles du signal seront capturées par le récepteur A en mode ZERO SPAN. Une simple FFT du signal permet alors de retrouver tout le contenu spectral de la voix et même de déterminer la profondeur de modulation (AM). Il est cependant important de noter que l’acquisition des points dans le domaine temporel induira un possible repliement du spectre utile qu’il convient d’éviter. C’est sur cet aspect et sur le nombre de points mémoire que l’analyseur de réseaux montre une vraie limitation en comparaison avec un récepteur radio hétérodyne dédié.

Dans le cadre de la mesure à distance, le VNA n’est plus directement connecté à la cavité, mais par deux antennes interposées (Fig. 4a). Se pose alors un problème classique de RFID : Le signal émis à f0 est réfléchi non plus par uniquement le transpondeur, mais aussi par tout l’environnement (table, sol, mur, …), alors que le signal rétro modulé par le dispositif variant dans le temps est extrêmement faible. Il convient alors d’implémenter un filtrage passe-haut après la démodulation/translation de fréquence pour réduire l’amplitude de la « porteuse ». Cette dernière opération est réalisée par un programme Python qui récupère les données ZERO SPAN du VNA via des requêtes SCPI, filtre le signal temporel, et l’envoie vers la carte son de l’ordinateur (Fig. 4b).

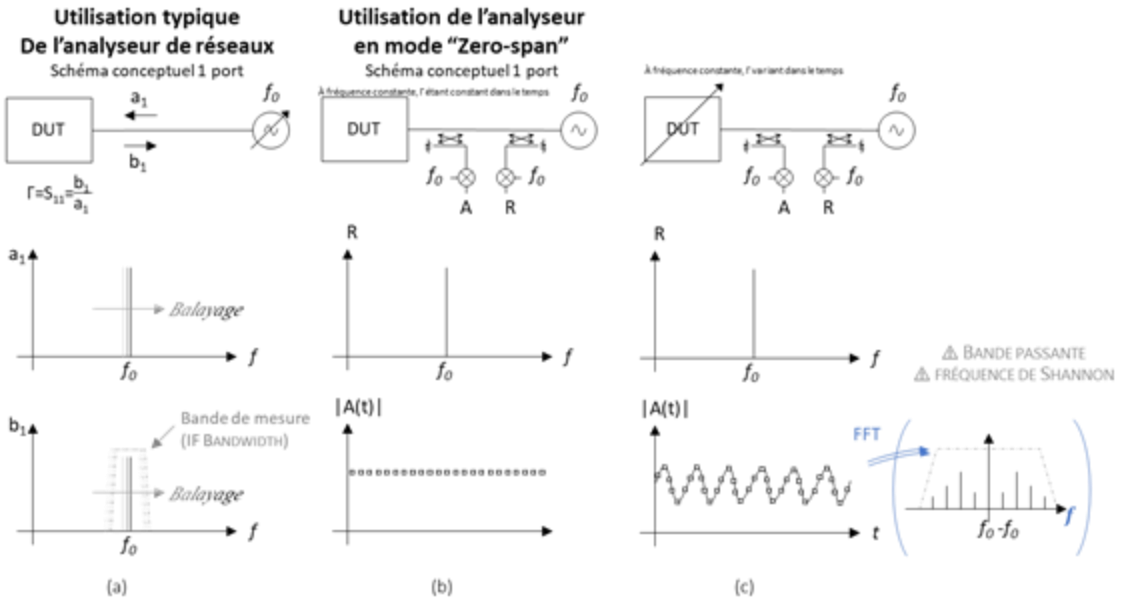


Fig.3. Principe de mesure à l'analyseur de réseaux (9). Ligne du haut : diagramme de la mesure effectuée par l'analyseur. Ligne du milieu : mesure absolue de l'onde incidente. Ligne du bas : mesure absolue de l'onde réfléchie. (a) mesure en mode « SWEEP » d'un dispositif invariant dans le temps, (b) mesure en mode « ZERO SPAN » d'un dispositif invariant dans le temps, (c) mesure en mode « ZERO SPAN » d'un dispositif variant dans le temps.

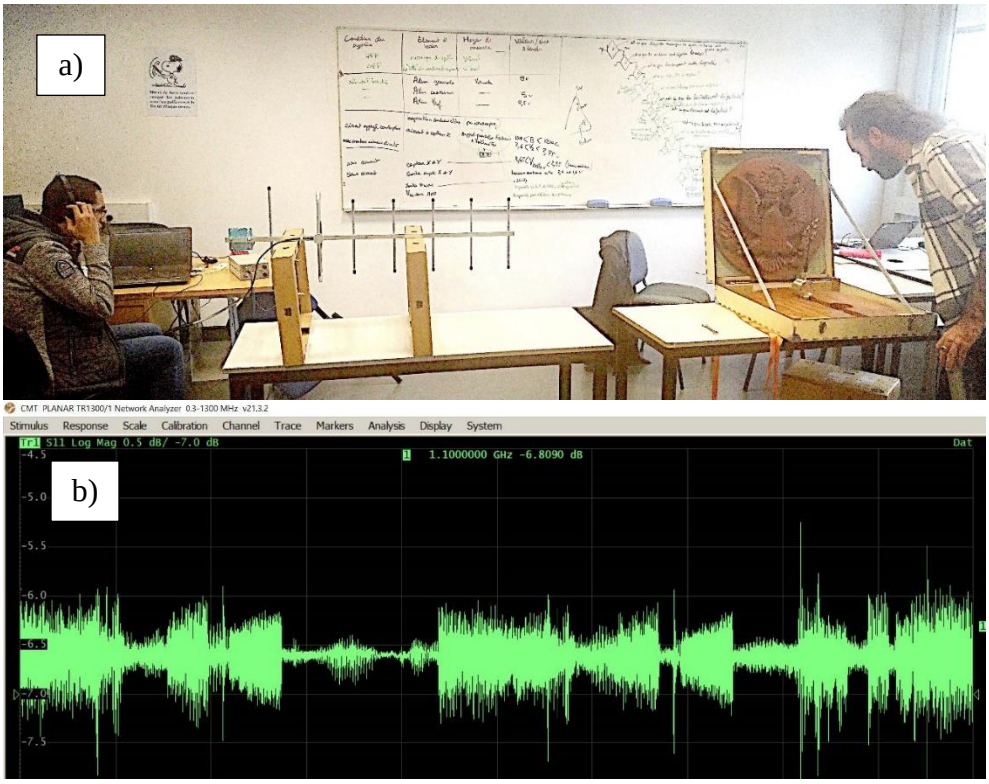


Fig.4. (a) Montage sans-fil composé d'un ordinateur pilotant un analyseur de réseaux, dont le port 1 est connecté à une antenne directionnelle. Face à cette antenne se trouve la cavité résonante et son antenne, qui module la réflexion du signal RF à la mesure du signal audio capté par la membrane de la cavité. (b) Visualisation du signal en mode ZERO SPAN (fonction du VNA pouvant être interprétée comme une démodulation d'amplitude).

IV. Applications pédagogiques

L'objectif est de proposer un défi pédagogique aux étudiants pour qu'ils mesurent (à distance) le signal audio capté par le micro.

Cet objectif est adapté au niveau d'enseignement :

- Niveau BUT GEII, il s'agit de mesurer le signal modulé en amplitude à l'aide d'un analyseur de réseaux en mesure du paramètre S11 en mode *ZERO SPAN*, puis d'extraire de la profondeur de modulation.
- Niveau Master ISC/SE, il s'agit alors de caractériser le dispositif comme s'il s'agissait d'un mélangeur où l'oscillateur local serait l'onde à f0, le signal de bande intermédiaire serait l'onde acoustique et le signal radiofréquence serait b1. Il convient alors de découpler sur le VNA la fréquence d'excitation et la fréquence d'analyse à l'aide du mode « *Frequency Offset* » (8).
- BAC+3 à BAC+5 (voire en formation doctorale) : Sous forme de projet cours, il est également proposé aux étudiants de reproduire une version *Do It Yourself* à moindre coût du dispositif soviétique. Cette réalisation nécessite une rétro-ingénierie, et notamment de comprendre quels sont les aspects critiques au fonctionnement du dispositif. Le paramètre clef étant le facteur de qualité du résonateur micro-onde, et donc les pertes des matériaux utilisés. On peut voir en Figure 5, cette version réalisée à partir d'une canette alimentaire.

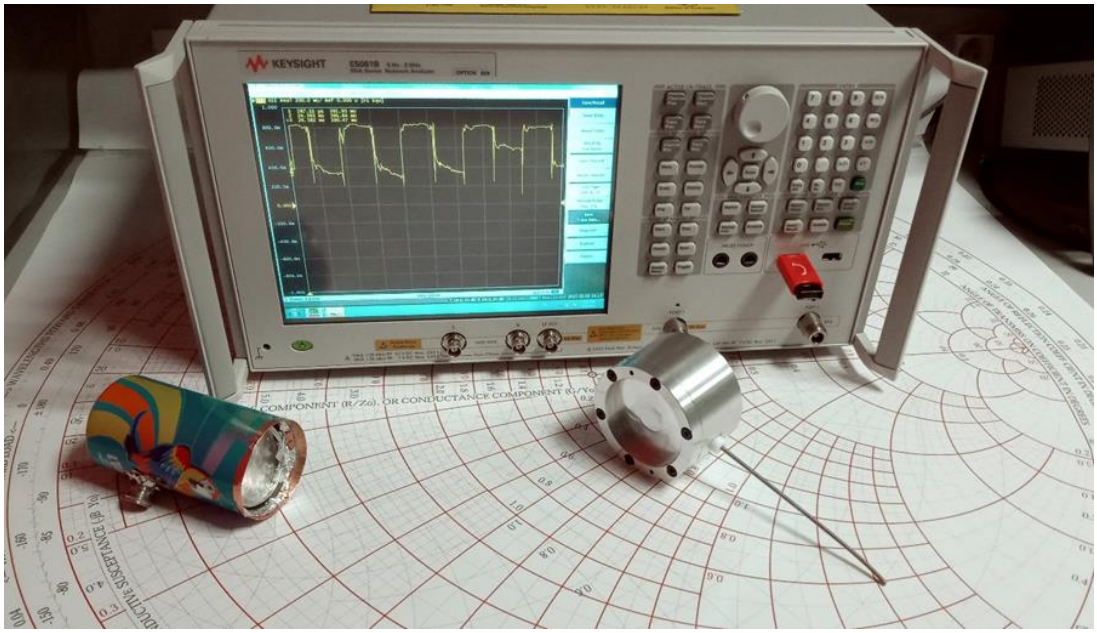


Fig.5. Mesure du S11 en mode *ZERO SPAN* à l'analyseur de réseau du dispositif construit par des étudiants à partir d'une cannette et de papier aluminium de cuisine : pendant la mesure, la membrane est tour-à-tour plaquée ou déconnecté à la tige de métal constituant la cavité coaxiale.

V. Conclusion et perspectives

Outre les travaux pratiques proposés, ce sujet a aussi été couvert par deux projets tuteurés et deux stages pour accompagner la reproduction des dispositifs et des stratégies de mesures. L'objectif est dans tous les cas de profiter de l'aura du micro espion comme levier de motivation pour amener les étudiants vers de nouveaux horizons !

Partageons enfin une expérimentation qui est en train de se dérouler cette année : au sein de deux IUT Bordelais, une équipe d'étudiants du département « métiers du livre et patrimoine » a été jumelée avec une équipe d'étudiants du département GEII « Génie Électrique et Informatique Industrielle », avec pour ambition de construire une exposition sur les technologies sans fil du début de la guerre froide. Dans ce projet, les étudiants littéraires construisent la scénographie et la mise en valeur des fonds historiques et littéraires. Ils tiennent aussi le rôle de client pour les étudiants électroniciens qui doivent fournir des démonstrations fonctionnelles. Ce jeu de rôle de client-fournisseur ne donne pas de rôle à l'enseignant (si ce n'est celui de conseil) mais responsabilisent les étudiants en les plaçant face à leurs l'engagements de livrables, sans le filet du « travail dans le vide » souvent ressenti en milieu scolaire. Une fois développé, l'exposition sera amenée à se déplacer de bibliothèque en bibliothèque à travers le territoire local pour servir de vecteur à la diffusion de la culture scientifique et électronique au sein de la société.

Remerciements

Les auteurs souhaitent remercier HB sculpture, Castelnou pour la reproduction du grand Sceau des Etats Unis en bois, ainsi que les conservateurs du Cryptomuseum pour les passionnants échanges historiques. Les auteurs tiennent aussi à souligner l'implication des étudiants de Licence Professionnelle CAFiEM de l'IUT GEII de Bordeaux sur ce projet : L. MIARA et P. GRASSET (2020-2021), R. CLIMENT et M. BAKARI (2021-2022), D. TABARY et M. LAVAUD (2023-2024), et la reproduction mesures en utilisant une antenne Yagi par R. Dauny (2023). Les travaux ont bénéficié du soutien du Ministère de l'Enseignement Supérieur et de la recherche à travers "France 2030", du GIP-CNFM (10) et de son projet "ANR-23-CMAS-0024 INFORISM" (11).

Références

1. Reportage de 1947 *https://malyan.livejournal.com/24022.html* (*dernière consultation* nov. 2023).
2. Informations sur la répartition des pièces dans Spaso House : https://nsarchive.gwu.edu/document/28876-document-5-report-trip-ussr-1959-and-radiation-discovered-spaso-house-moscow-ussr (*dernière consultation* nov. 2023).
3. *https://www.cryptomuseum.com/covert/bugs/thing/index.htm* (*dernière consultation* nov. 2023).
4. Carte de Moscou datant de 1951 http://www.etomesto.com/map-moscow_1951/ (*dernière consultation* nov. 2023. Voir à la Latitude 55.750763 and Longitude 37.588305).
5. *https://www.cryptomuseum.com/covert/bugs/thing/files/GREAT_SEAL_BUG.pdf* (*dernière consultation* nov. 2023).
6. N. Barbot, O. Rance and E. Perret, Differential RCS of Modulated Tag, *IEEE Transactions on Antennas and Propagation*, **69**, 9, 6128-6133, doi: 10.1109/TAP.2021.3060943 (2021).
7. H. Ribeiro, S. Hemour and N. B. Carvalho, Fully Passive Modulation Technique for SWIPT Scenarios, *2023 IEEE/MTT-S International Microwave Symposium - IMS 2023*, San Diego, CA, USA, 999-1002, doi: 10.1109/IMS37964.2023.10188111 (2023).
8. K. Niotaki *et al*., RF Energy Harvesting and Wireless Power Transfer for Energy Autonomous Wireless Devices and RFIDs, *IEEE Journal of Microwaves*, **3** (2**)**, 763-782, doi: 10.1109/JMW.2023.3255581 (2023).
9. S. Hemour and N. Barbot, Backscattering modulation 101: VNA measurements, *2023 IEEE 13th International Conference on RFID Technology and Applications (RFID-TA)*, Aveiro, Portugal, 169-172, doi: 10.1109/RFID-TA58140.2023.10290457 (2023).
10. GIP-CNFM : Groupement d'Intérêt Public - Coordination Nationale pour la formation en Microélectronique et en nanotechnologies. *Website : http://wwww.cnfm.fr*.
11. INFORISM, INgénierie de FORmations Innovantes et Stratégiques en Microélectronique, projet ANR-23-CMAS-0024-INFORISM au titre du programme France 2030. Ce projet à 5 ans a démarré au cours de l'année académique 2023-2024.