PRÉPRINT TECHNIQUE

Exploitation cyberélectromagnétique non coopérative de liaisons C2 ExpressLRS d'UAV : reconstruction d'identité, suivi FHSS et substitution contrôlée d'émetteur

Melik Lemariey

Consultant en guerre électronique, France, https ://meliklemariey.com/

Auteur correspondant: melik.e.lemariey@pm.me

ORCID: 0000-0002-1041-0113

Dépôt: `elrs-h44f-executable-evidence`

Résumé—La détection d'une liaison de commande à saut de fréquence ne suffit pas à en reconstruire l'état protocolaire, temporel et radio. Cette étude examine, dans un cadre d'exploitation cyberélectromagnétique, dans quelle mesure l'état physique et logique opérationnel d'une liaison ExpressLRS peut être reconstruit à partir d'observations RF non coopératives, puis utilisé pour le suivi passif et la validation contrôlée de l'état de liaison.

Des implémentations Python indépendantes propres à chaque famille ont été comparées à une référence C++ compilée séparément et dérivée des règles sélectionnées des tags épinglés 1.2.1, 2.5.2, 3.6.4, 4.0.1 et 4.1.0 sur 39 845 888 entrées, sans divergence. La campagne matérielle H44F-A sur ELRS 4.1.0 débute sans oracle de profil radio ou d'identité, sans phrase de liaison, sans UID ni graine fournis et sans table FHSS précompilée. Elle sélectionne passivement un profil unique parmi six profils candidats, le confirme après réinitialisation de la radio, puis reconstruit deux candidats UID2 FHSS-équivalents, `3F|BF`, ainsi que les octets UID3–UID5 `35:59:F0`. À partir des octets UID4 et UID5, elle déduit l'initialiseur CRC de base `0x5DF0`, puis obtient deux graines produisant la même table FHSS de 240 positions.

L'état reconstruit permet le suivi de 960/960 paquets sans erreur CRC ni divergence de canal. Après interruption volontaire de l'émetteur de référence, un émetteur développé séparément est accepté par le récepteur stock. Les 3 698 commandes observées après le retour de la source de référence restent attribuées à la source substitutive ; après l'arrêt de celle-ci, 439 des 440 commandes de récupération sont attribuées à la source de référence. Les 5 671 trames RAW sont reproduites sans erreur CRC, de forme ou de séquence.

La phrase de liaison n'est pas récupérée : sa récupération n'est pas nécessaire à la substitution démontrée sur le banc. H44F-A montre que l'état reconstruit à partir d'observations RF non coopératives permet non seulement le suivi passif et la validation de l'état de liaison, mais aussi une substitution contrôlée de source sur un récepteur stock après interruption de l'émetteur de référence. Ces résultats ne démontrent ni contention initiale contre une source continuellement active, ni capacité de brouillage, ni portée opérationnelle, ni validation en vol, ni applicabilité universelle à ExpressLRS.

Mots-clés—Mobile and wireless security, Network experimentation, Software reverse engineering, Embedded systems security, Cyberwarfare, Command and control

Périmètre du préprint. Les expériences utilisent du matériel détenu par l'expérimentateur, dans un banc RF contrôlé, sans vol ni liaison tierce. Un artefact public de relecture distinct réunit, pour H44F-A et H44F-B, les journaux anonymisés, les empreintes exactes des artefacts sélectionnés, le code hors ligne de reconstruction et de vérification, des comparaisons amont étroites et les scripts de rejeu. Il permet de reproduire hors ligne les deux verdicts sans fournir la chaîne matérielle active. Le dépôt `elrs-h44f-executable-evidence` distribue les scripts originaux sous licence Apache-2.0 et la documentation ainsi que les preuves assainies sous licence CC BY 4.0. Il exclut la phrase de liaison privée, tout firmware prêt à flasher, les outils d'injection directement utilisables et toute procédure opérationnelle de brouillage.

1. Introduction

Les liaisons de commande à étalement de spectre par saut de fréquence associent une porteuse variable à des paquets courts et à de fortes contraintes de latence. Pour un récepteur de COMINT technique ou d'appui électronique, la détection d'énergie n'est qu'une première étape : il faut identifier le PHY, reconstruire ou contraindre l'état protocolaire, acquérir le rythme, se recaler avec une erreur bornée et vérifier la cohérence des paquets décodés. La réussite d'une étape n'implique pas celle de la suivante.

ExpressLRS est un protocole open source de radiocommande à faible latence, mis en œuvre sur plusieurs familles de transcepteurs LoRa. Son ouverture permet une analyse exacte du code et une validation différentielle, mais ne prouve pas qu'une reconstruction théorique soit réalisable pour chaque version, circuit, mode de paquet ou profil temporel. Dans un cadre d'exploitation cyberélectromagnétique, l'étude traite donc comme une chaîne de preuve intégrée la reconstruction des profils PHY depuis les sources épinglées, leur identification passive par observation RF, la reconstruction du protocole et de l'identité, le suivi FHSS, la substitution contrôlée et l'attribution de la source conservée par le récepteur.

La question de recherche est la suivante :

Dans quelle mesure l'état physique et logique d'une liaison de commande ExpressLRS à saut de fréquence peut-il être reconstruit à partir d'observations RF non coopératives, et avec quelle exactitude l'état reconstruit peut-il soutenir un suivi passif et une validation contrôlée de l'état de liaison ?

La campagne expérimentale finale H44F-A apporte une réponse intégrée dans les conditions du banc. Elle reconstruit depuis les sources épinglées les profils radio ExpressLRS compatibles SX126x pour la version et la bande FCC915 étudiées, puis les applique successivement en réception seule sur leur fréquence SYNC. Le détecteur aveugle sélectionne un profil unique à partir de trames SYNC cohérentes, de structure correcte et de CRC valide, sans oracle de profil, d'identité ni phrase de liaison. Après réinitialisation de la radio, son noyau de reconstruction repart d'un SYNC frais et reconstruit l'état logique opérationnel, la classe d'équivalence d'identité, la graine, la table FHSS et l'état de synchronisation. L'état obtenu permet le suivi de 960/960 paquets sans erreur CRC ni divergence de canal, puis une substitution contrôlée de source sur un récepteur stock après interruption volontaire de la source de référence.

Les contributions, volontairement bornées, sont :

1. une reconstruction interversions, épinglée aux sources, des règles sélectionnées régissant les dépendances OTA, CRC, UID, SYNC et FHSS dans les tags étudiés des familles ExpressLRS 1 à 4.1 ;
2. la reconstruction des profils radio ExpressLRS compatibles SX126x pour la version et la bande FCC915 étudiées, puis leur balayage passif jusqu'à la sélection d'un profil unique par détection de SYNC cohérents et CRC valides ;
3. la récupération aveugle des dérivés radio opérationnels d'une identité ELRS 4.1 dérivée de 4096 bits produits par un CSPRNG, sans récupération de la phrase de liaison, dont deux candidats UID2 appartiennent à la même classe d'équivalence FHSS ;
4. le suivi embarqué sur l'ensemble des 240 positions de la table FHSS, avec 960/960 paquets CRC valides sans divergence de canal dans la campagne finale ;
5. la substitution contrôlée et l'attribution vérifiée des sources de référence et substitutive, avec rétention de la source substitutive après retour de la référence, puis récupération de celle-ci après arrêt de la source substitutive.

Des travaux expérimentaux antérieurs menés à partir de 2016 sur une liaison FHSS distincte avaient déjà exploré une démarche apparentée fondée sur la caractérisation du PHY, l'exploitation de champs d'identité observables, la génération locale de séquences candidates et leur élimination progressive par confrontation aux observations. Ces travaux, non publiés à l'époque, ne constituent pas des travaux antérieurs publiquement disponibles concernant ExpressLRS. Leur description détaillée et l'attribution individuelle des contributions sont volontairement différées dans cette version du préprint, dans l'attente de la validation des personnes ayant participé à ces travaux.

Plusieurs propriétés pertinentes d'ExpressLRS ont par ailleurs été discutées publiquement à partir de 2022. Aucune primauté n'est revendiquée sur ces principes généraux. L'apport revendiqué porte sur leur traitement interversions, quantitatif, intégré et reproductible, depuis l'identification passive du profil radio jusqu'à la reconstruction de l'état de liaison, son suivi complet et sa validation contrôlée sur un récepteur stock.

2. État de l'art et frontière des travaux antérieurs

Le cadre général des radiocommunications numériques, de la modélisation des signaux et de la chaîne radiofréquence employé dans cette étude s'appuie sur les deux tomes de l'ouvrage collectif dirigés respectivement par Geneviève Baudoin et Martine Villegas [1, 2]. Ces ouvrages constituent ici des références théoriques générales ; ils ne décrivent ni ExpressLRS, ni une reconstruction non coopérative de son état de liaison. La présente étude part de la classification physique, ou la mène conjointement, puis évalue dans quelle mesure des champs observables et des générateurs déterministes publics permettent de réduire un espace discret d'états de liaison.

Dans le domaine des radiocommandes, g3gg0 a publié une rétro-ingénierie de la liaison distincte TBS Crossfire à 900 MHz, fondée sur des traces SPI, la récupération des paramètres PHY, la découverte de la séquence de saut, l'analyse du CRC, la réception sur une carte Heltec et le suivi temporel en temps réel [3]. Ce travail constitue une contribution méthodologique antérieure pertinente. Il n'est toutefois pas affirmé que TBS Crossfire et ExpressLRS partagent une architecture OTA, une méthode de dérivation d'identité, une initialisation CRC ou une filiation logicielle.

L'analyse publiée par NCC Group en 2022 portait principalement sur ExpressLRS 1.x et 2.x [4]. Elle décrivait la présence de trois octets d'UID dans les trames SYNC, une initialisation CRC dépendant de l'UID, la recherche exhaustive d'un octet de graine, la réduction de 256 candidats littéraux à 128 séquences distinctes ainsi qu'un scénario de configuration d'un émetteur compatible. Le présent travail reproduit certains de ces principes connus lorsque cela est nécessaire et étend le périmètre logiciel et matériel jusqu'à la version 4.1. Il n'emploie pas le terme « détournement » comme un résultat indépendant de la version étudiée et des conditions expérimentales.

Dans la pull request publique #1411, ouverte par `redfiveau` puis fermée sans fusion en 2022, `CapnBry` a discuté l'observation directe de la séquence FHSS, la recherche exhaustive de l'initialisation CRC sur 14 bits, le rejeu d'une trame SYNC statique ainsi que la distinction entre évitement de collision et authentification [5]. `redfiveau` a décrit l'alias d'UID2, puis déclaré avoir écrit et utilisé avec succès un code de détournement lors d'essais. Cette déclaration revendique un travail expérimental antérieur de son auteur ; le code correspondant et les journaux d'essai ne figurent toutefois pas dans le corpus actuellement disponible.

Plusieurs modifications de sécurité et leurs coûts ont également été discutés, notamment une mesure de l'occupation de la mémoire flash par `pkendall64`, mais la proposition a finalement été fermée sans fusion. Des commentaires ultérieurs de `CapnBry` et de `redfiveau` ont porté sur les contraintes propres au protocole et au matériel. Ces propos sont attribués à leurs auteurs respectifs et ne sont pas présentés comme une position officielle d'ExpressLRS LLC.

Frontière chronologique et travaux antérieurs. Des travaux expérimentaux antérieurs menés à partir de

2016 sur une liaison FHSS distincte avaient déjà exploré une démarche apparentée fondée sur la caractérisation du PHY, l'exploitation de champs d'identité observables, la génération locale de séquences candidates et leur élimination progressive par confrontation aux observations. Ces travaux, non publiés à l'époque, ne constituent pas des travaux antérieurs publiquement disponibles concernant ExpressLRS et n'établissent ni identité de protocole, ni filiation logicielle, ni architecture OTA commune.

Leur description détaillée et l'attribution individuelle des contributions sont volontairement différées dans cette version du préprint, dans l'attente de la validation des personnes ayant participé à ces travaux. La présente version se limite donc à signaler leur existence et leur continuité méthodologique générale avec la démarche expérimentale actuelle.

Les discussions publiques consacrées à ExpressLRS à partir de 2022 constituent des travaux antérieurs pertinents et sont attribuées à leurs auteurs respectifs. Aucune primauté publique n'est revendiquée sur les principes généraux déjà discutés. L'apport revendiqué porte sur leur traitement interversions, quantitatif, intégré et reproductible, depuis l'identification passive du profil radio jusqu'à la reconstruction de l'état de liaison, son suivi complet et sa validation contrôlée sur un récepteur stock.

3. Système et modèle de menace

Le système comprend une source de référence, un récepteur ExpressLRS stock, des paquets OTA LoRa dont le format dépend de la version, transmis selon un cycle FHSS déterministe, ainsi que des interfaces CRSF [6, 7]. Une phrase de liaison est dérivée en octets d'UID, mais la documentation officielle distingue ce mécanisme d'un mot de passe ou d'une clé de chiffrement et lui attribue un rôle d'évitement des collisions [8]. Une phrase de liaison à forte entropie protège contre le devinement et la recherche de préimage, mais ne constitue pas une authentification cryptographique des trames. Le FHSS ne constitue pas davantage un mécanisme d'authentification. Le CRC vérifie la cohérence d'un paquet avec un état candidat ; ce n'est pas un MAC à clé.

Les actifs protégés sont l'intégrité des commandes, l'authenticité de leur source, la disponibilité de la liaison, l'état de synchronisation FHSS, les états des canaux de commande et de télémétrie, l'état d'acquisition du récepteur et l'identité radio opérationnelle. Les acteurs considérés sont l'opérateur légitime, l'observateur RF non coopératif, l'expérimentateur autorisé équipé d'une radio programmable et le défenseur.

Pour la campagne H44F-A, le modèle suppose connus le protocole ExpressLRS, la version étudiée, la bande FCC915, la compatibilité SX126x et le code source public correspondant. Le format OTA, la largeur du CRC-14, son polynôme `0x2E57` et les règles de dérivation propres à la version sont donc connus. Le profil radio actif n'est toutefois ni fourni par un oracle ni fixé à la compilation. La phrase de liaison et les états propres à la liaison — UID, initialiseur CRC de base, nonce courant, graine, table FHSS et état de synchronisation — ne sont pas fournis. Aucun devinement ni calcul de préimage de la phrase de liaison n'est requis.

La figure 1 sépare le modèle interversions dérivé des sources de la chaîne matérielle intégrée H44F-A. La couverture du code ne transforme pas une version, une bande, une radio ou un profil non testé en preuve RF.

H44F-A reconstruit depuis les sources épinglées les profils radio candidats compatibles avec la configuration étudiée, puis les applique successivement au SX1262 en réception seule sur leur fréquence SYNC respective. Le balayage sélectionne dynamiquement, à l'exécution, l'unique profil produisant une trame SYNC de structure correcte et de CRC valide. Une acquisition indépendante confirme ensuite le même débit radio et les mêmes octets UID4/UID5.

H44F-A est exécutée sans oracle de profil ou d'identité et sans phrase de liaison ; les trois indicateurs correspondants valent zéro. Pendant le balayage, la plateforme Heltec/SX1262 reste strictement en réception et n'effectue aucune émission RF ; seule la source de référence stimulée par CRSF émet. En cas d'absence de profil valide ou d'ambiguïté entre plusieurs profils, la chaîne s'arrête et l'émission RF de la Heltec reste désactivée.

Après confirmation du profil, les états du balayage, du classifieur et de l'identité sont purgés, puis la radio est réinitialisée. Seul le profil sélectionné est transmis au noyau aveugle ; aucun octet d'identité n'est transféré entre les deux étapes internes de la campagne.

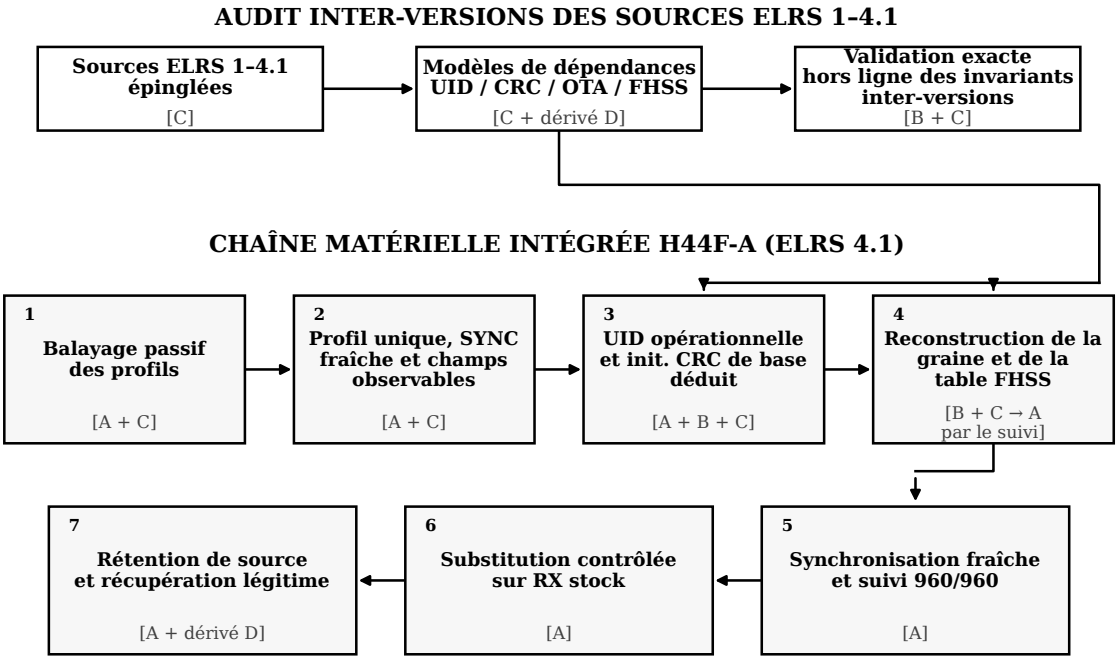
Le noyau de reconstruction de H44F-A débute sans oracle d'identité ni phrase de liaison, sans UID, initialiseur CRC de base, graine ni table FHSS compilés. À partir du profil sélectionné, il acquiert un nouveau SYNC, reconstruit l'identité radio opérationnelle, la graine, la table FHSS et l'état courant de synchronisation, puis valide le suivi passif et la chaîne active contrôlée sur un récepteur stock.

Les phases actives de H44F-A utilisent du matériel détenu et autorisé par l'expérimentateur, dans un environnement RF contrôlé, sans liaison tierce ni vol, et à la puissance pratique minimale. La source de référence est volontairement interrompue avant l'émission substitutive, puis réactivée seulement après acquisition de la source substitutive.

Aucune contention initiale contre une source de référence continuellement active et aucun brouillage ne sont testés. La portée opérationnelle, la validation en vol, l'emploi de l'intelligence artificielle pour l'acquisition ou la classification, les systèmes militaires, l'efficacité opérationnelle, la généralisation à tous les matériels, bandes, profils ou versions, ainsi que la neutralisation générale d'un aéronef restent hors du périmètre expérimental et relèvent, le cas échéant, de travaux futurs.

4. Reconstruction interversions

L'audit épingle les tags 1.2.1, 2.5.2, 3.3.2, 3.6.4, 4.0.1 et 4.1.0 du dépôt officiel [6, 9]. Le tag 4.1.0 correspond localement au commit `a9d4a9c`, dont le hash complet figure dans l'artefact. Le périmètre de l'audit et des diffs conservés est limité aux fichiers impliqués dans les règles OTA, CRC, UID, SYNC, nonce et FHSS, ainsi que dans la définition des profils radio utilisés par H44F-A. Le dépôt amont complet n'est pas redistribué ; l'artefact conserve l'URL, le tag, le commit, le hash de licence, les



Chaque transition est validée séparément ; la couverture logicielle inter-versions ne constitue pas une validation RF universelle.

Figure 1 – Chaîne de preuve interversions et matérielle H44F-A. L'audit des sources épinglées ExpressLRS 1 à 4.1 établit les dépendances UID, OTA, CRC et FHSS utilisées par les reconstructeurs hors ligne. H44F-A reconstruit depuis les sources épinglées les profils radio ExpressLRS 4.1 FCC915 compatibles SX126x, les applique successivement en réception seule et sélectionne dynamiquement, à l'exécution, un profil unique à partir de trames SYNC de structure correcte et de CRC valide. Après confirmation indépendante, purge des états et réinitialisation de la radio, son noyau aveugle reconstruit l'identité opérationnelle, la graine, la table FHSS et l'état de synchronisation. Elle valide ensuite un suivi de 960/960 paquets, une substitution contrôlée sur un récepteur stock, la rétention de la source substitutive après retour de la référence, puis la récupération de cette dernière après arrêt du substitut. Chaque transition est évaluée séparément ; aucune validation RF universelle des versions, bandes, radios ou profils non testés n'est déduite de l'audit logiciel.

notices, des extraits étroits et un script de récupération déterministe.

Invariants transversaux et frontières de version. Le numéro majeur ne partitionne pas à lui seul les algorithmes. Les références épinglées partagent la dérivation UID par MD5 et le profil sub-GHz 50 Hz (BW500, SF8, CR4/7, préambule 10, 20 ms, saut tous les quatre paquets et charge utile de 8 octets). Les fichiers du PRNG ont la même empreinte sur les 37 tags de 2.0.0 à 4.0.1 ; 4.1 conserve le même LCG et le même tirage borné. Les versions 2–4 partagent aussi le mélange FHSS par blocs, mais pas tous ses paramètres.

Dans 3.x, l'extraction distingue trois organisations du code FHSS : 3.0.0–3.2.1, 3.3.0–3.3.2 et 3.4.0–3.6.4. Le harnais natif FCC915 classe néanmoins 3.2.1, 3.3.2 et 3.6.4 dans une même famille de comportement pour dix graines réservées. De même, 4.0 et 4.1 sont identiques pour les règles OTA/FHSS sélectionnées, non comme firmwares complets. Les ruptures restent propres à chaque propriété : allocateur de 256 positions en 1.x ; table par blocs de 240 en 2.x ; changements de graine, CRC et SYNC en 3.x ; nouveaux SYNC et état CRC lié au nonce en 4.x. Un invariant commun étend donc la preuve logicielle de cet invariant seulement, jamais la preuve RF d'une version non testée.

Bornage et reconstruction de l'espace des profils. L'espace des profils doit être distingué selon le niveau considéré. Dans ExpressLRS 4.1, les tables amont des familles SX127x, SX128x et LR1121 contiennent au total 36 entrées compilables. Après suppression des entrées correspondant au même profil logique, 24 profils distincts subsistent. Le sous-ensemble 900 MHz formé par l'union des tables SX127x et LR1121 contient neuf profils logiques :

$$\left|\mathcal{P}_{4.1}^{\text{entries}}\right| = 36, \qquad \left|\mathcal{P}_{4.1}^{\text{logical}}\right| = 24, \qquad \left|\mathcal{P}_{4.1}^{900}\right| = 9. \quad (1)$$

Ces neuf profils 900 MHz comprennent les débits logiques suivants :

— `FSK_900_1000HZ_8CH` ;
— `LORA_900_250HZ` ;
— `LORA_900_200HZ_8CH` ;
— `LORA_900_200HZ` ;
— `LORA_900_100HZ_8CH` ;
— `LORA_900_100HZ` ;
— `LORA_900_50HZ` ;
— `LORA_900_25HZ` ;
— `LORA_900_50HZ_DVDA`.

La campagne H44F-A ne balaie pas cet espace global. La source de référence utilise la famille radio SX127x en 900 MHz ; le sous-ensemble pertinent est donc consti-

Table 1 – Dépendances des familles FCC915 épinglées utilisées pour la reconstruction. La concaténation est notée ‖. Pour ELRS 4, l'état CRC des paquets non-SYNC dépend aussi du nonce OTA.

Référence	ID OTA	Init. CRC de base	Graine FHSS	Générateur	L	Canal SYNC
1.2.1	aucune	$u_4 \Vert u_5$	$u_2 \Vert u_3 \Vert u_4 \Vert u_5$	allocation équilibrée	256	0
2.5.2	aucune	$u_4 \Vert u_5$	$u_2 \Vert u_3 \Vert u_4 \Vert u_5$	mélange par blocs	240	20
3.3.2/3.6.4	3	$(u_4 \Vert u_5) \oplus 3$	$u_2 \Vert u_3 \Vert u_4 \Vert (u_5 \oplus 3)$	mélange par blocs	240	21
4.0.1/4.1.0	4	$(u_4 \Vert u_5) \oplus (4 \ll 8)$	$u_2 \Vert u_3 \Vert u_4 \Vert (u_5 \oplus 4)$	mélange par blocs	240	20

tué des six profils logiques définis dans la table amont correspondante :

$$\mathcal{P}_{\text{H44F-A}} = \mathcal{P}_{4.1}^{\text{SX127x,900}}, \qquad |\mathcal{P}_{\text{H44F-A}}| = 6. \tag{2}$$

Les trois profils 900 MHz non inclus dans ce sous-ensemble appartiennent à la table LR1121 :

$$\mathcal{P}_{4.1}^{900} \setminus \mathcal{P}_{\text{H44F-A}} = \left\{ \begin{array}{l} \texttt{FSK\_900\_1000HZ\_8CH}, \\ \texttt{LORA\_900\_250HZ}, \\ \texttt{LORA\_900\_200HZ\_8CH} \end{array} \right\}. \tag{3}$$

Les six profils logiques de H44F-A ne correspondent toutefois qu'à cinq configurations matérielles distinctes en réception sur le SX1262. Les profils `LORA_900_200HZ` et `LORA_900_50HZ_DVDA` partagent le même tuple PHY de réception : facteur d'étalement 6, bande passante de 500 kHz, taux de codage 4/7, préambule de 8 symboles et charge utile de 8 octets.

En notant ϕ l'application qui associe à chaque profil logique sa configuration matérielle de réception SX1262,

$$|\phi(\mathcal{P}_{\text{H44F-A}})| = 5. \tag{4}$$

L'application ϕ n'est donc pas injective : deux profils logiques partagent la même configuration PHY de réception. Leur distinction logique repose ensuite sur le débit énuméré porté par le SYNC et sur les contraintes temporelles associées au profil, et non sur le seul tuple SX1262.

Une borne combinatoire naïve peut être obtenue en considérant indépendamment toutes les valeurs rencontrées dans les champs des six profils :

$$\begin{aligned} N_{\text{naive}} &= 6_{\text{enum}} \times 4_{\text{SF}} \times 1_{\text{BW}} \times 2_{\text{CR}} \times 2_{\text{preamble}} \times 4_{\text{interval}} \\ &\quad \times 2_{\text{hop}} \times 2_{\text{payload}} \times 2_{\text{sends}} \times 5_{\text{ToA}} \times 1_{\text{frequency}} \\ &= 15\,360. \end{aligned} \tag{5}$$

Cette valeur est artificielle et ne constitue pas une borne opérationnelle utile. Le débit énuméré, le facteur d'étalement, le taux de codage, la longueur de préambule, l'intervalle de paquet, l'intervalle de saut, le nombre d'émissions et le temps d'occupation ne sont pas indépendants : ils sont regroupés en tuples cohérents dans le code amont.

En ne conservant que les principales dimensions PHY rencontrées dans les six profils, quatre facteurs d'étalement, une bande passante, deux taux de codage, deux longueurs de préambule et deux longueurs de charge utile produiraient au plus

$$N_{\text{PHY,theoretical}} = 4 \times 1 \times 2 \times 2 \times 2 = 32 \tag{6}$$

combinaisons PHY théoriques.

Si les deux orientations IQ étaient traitées comme une dimension indépendante, cette borne deviendrait

$$N_{\text{PHY+IQ,theoretical}} = 32 \times 2 = 64. \tag{7}$$

L'ajout de deux hypothèses de format CRC, par exemple CRC-8 et CRC-14, produirait une borne relâchée de

$$N_{\text{PHY+IQ+CRC,theoretical}} = 32 \times 2 \times 2 = 128. \tag{8}$$

Cette dernière valeur décrit un espace hypothétique PHY–OTA. Elle ne correspond pas à l'espace réellement testé par H44F-A, car l'orientation IQ, la largeur du CRC, le format OTA et la charge utile sont contraints par la version et par les tuples définis dans les sources.

La borne opérationnelle de H44F-A reste donc

$$\begin{gathered} N_{\text{logical}} = 6, \qquad N_{\text{RX,distinct}} = 5, \\ N_{\text{expected,winners}} = 1. \end{gathered} \tag{9}$$

H44F-A reconstruit depuis les sources épinglées les six profils logiques de la famille SX127x 900 MHz, les traduit en paramètres de réception SX1262 et les applique successivement en réception seule. Le profil actif n'est ni fourni par un oracle ni fixé à la compilation : il est sélectionné dynamiquement à l'exécution à partir des observations RF, puis confirmé par une acquisition indépendante avant passage à son noyau aveugle.

La sélection du profil ne transmet aucun état d'identité. Après confirmation, les états du balayage, du classifieur et de l'identité sont purgés, puis la radio est réinitialisée. Le noyau aveugle acquiert ensuite un nouveau SYNC en utilisant uniquement le profil radio sélectionné.

Dépendances UID, OTA et CRC. Soient $u_i = \text{UID}_i$, $v = \text{OTA\_VERSION\_ID}$, $\Vert$ la concaténation d'octets et n le nonce OTA. La revue du code donne

$$I_{1,2} = (u_4 \ll 8) \mid u_5, \tag{10}$$

$$I_3 = \big((u_4 \ll 8) \mid u_5\big) \oplus v, \quad v = 3, \tag{11}$$

$$I_4 = \big((u_4 \ll 8) \mid u_5\big) \oplus (v \ll 8), \quad v = 4. \tag{12}$$

Pour ExpressLRS 4.x, l'initialisation effective est

$$I_4'(p, n) = I_4 \oplus \begin{cases} 0, & p = \texttt{SYNC}, \\ n, & \text{sinon}. \end{cases} \tag{13}$$

Le chemin standard sélectionné implémente un CRC-14 de polynôme `0x2E57`. Le format OTA, la largeur du CRC et ce polynôme sont connus depuis les sources publiques épinglées ; ils ne sont pas reconstruits par la campagne. Ces équations décrivent un état de détection d'erreurs et de cohérence avec un état candidat. Elles ne décrivent ni une authentification, ni un chiffrement, ni un mécanisme de confidentialité. Le CRC n'est pas un MAC à clé.

Génération et longueur des tables FHSS. Les graines FHSS sont

$$s_{1,2} = (u_2 \ll 24) \mid (u_3 \ll 16) \mid (u_4 \ll 8) \mid u_5, \tag{14}$$
$$s_{3,4} = (u_2 \ll 24) \mid (u_3 \ll 16) \mid (u_4 \ll 8) \mid (u_5 \oplus v). \tag{15}$$

Dans H44F-A, le dernier octet `F4` des graines ELRS 4 est ainsi dérivé, et non directement observé : $\texttt{UID5} \oplus \texttt{OTA\_VERSION\_ID} = \texttt{F0} \oplus \texttt{04} = \texttt{F4}$.

ExpressLRS 1 utilise une allocation équilibrée de longueur 256, avec le canal 0 pour SYNC. Les familles ultérieures utilisent un mélange par blocs :

$$L = F \left\lfloor \frac{256}{F} \right\rfloor, \tag{16}$$

où F est le nombre de fréquences du domaine. Pour FCC915, $F = 40$ et $L = 240$. L'indice SYNC vaut 20 pour ExpressLRS 2 et 4, et 21 pour ExpressLRS 3.

Le Tableau 1 constitue la synthèse compacte de ces dépendances épinglées. ExpressLRS 4.0 et 4.1 sont équivalents pour les règles sélectionnées, mais non pour le firmware complet.

4.1 Recherche de phrase de liaison et reconstruction guidée par les observations

Le rôle de MD5 doit être distingué d'une collision ou d'une attaque générique de préimage. Dans l'implémentation testée, MD5 constitue un mécanisme rapide, déterministe et non salé de dérivation d'identité. Les six premiers octets du condensat forment l'UID radio à partir de la définition de compilation

```
-DMY_BINDING_PHRASE="<binding phrase>"
```

Pour une phrase candidate p, on note

$$U(p) = \mathrm{Trunc}_{48}(\mathrm{MD5}(\texttt{-DMY\_BINDING\_PHRASE="}p\texttt{"})) \,. \tag{17}$$

Une phrase humaine, prévisible ou réutilisée peut ainsi être testée hors ligne par dictionnaire : chaque candidat est converti en préimage de compilation, condensé et tronqué, puis comparé aux octets UID reconstruits par observation RF. Si seuls UID2 à UID5 sont reconstruits, la comparaison peut être limitée à ces quatre octets. L'absence de sel permet en outre de réutiliser les mêmes calculs entre équipements configurés avec une phrase identique. Les propriétés pertinentes sont ici le déterminisme, la rapidité, l'absence de sel et la troncature ; une collision MD5 n'est pas nécessaire à cette recherche.

À l'inverse, une phrase uniformément aléatoire de 128 ou 256 bits rend la récupération par dictionnaire impraticable. H44F-A utilise une entrée aléatoire plus longue encore. Une vérification privée postérieure donne l'UID nominale `E9:79:3F:35:59:F0`, tandis que la reconstruction aveugle obtient `UID2=3F|BF`, UID3–5 `35:59:F0`, l'initialiseur CRC de base `0x5DF0`, déduit d'UID4/UID5, et les graines `0x3F3559F4`/ `0xBF3559F4`. La phrase originale n'est pas récupérée. Sa récupération n'est pas nécessaire à la substitution contrôlée démontrée : la campagne reconstruit directement les dérivés opérationnels nécessaires au suivi et à l'acceptation radio.

Classes d'équivalence FHSS. Soit c un candidat d'identité ou, de manière équivalente pour la génération FHSS, un candidat de graine. On note $h_c(j)$ la fréquence prédite par ce candidat à la position j de la table. Les valeurs d'identité littérales sont regroupées en classes d'équivalence FHSS par

$$\begin{aligned} c_a \sim c_b \iff & \big(h_{c_a}(0), \ldots, h_{c_a}(L-1)\big) \\ & = \big(h_{c_b}(0), \ldots, h_{c_b}(L-1)\big). \end{aligned} \tag{18}$$

Cette relation porte sur l'égalité complète des tables radio, et non sur l'égalité littérale des UID. Deux valeurs UID distinctes peuvent donc appartenir à la même classe d'équivalence FHSS et rester indiscernables à partir de l'observation de la seule séquence de saut. L'UID nominale et la classe d'équivalence FHSS sont ainsi deux objets distincts. Une vérification privée postérieure peut identifier l'UID nominale, mais elle est exclue du verdict de reconstruction aveugle.

Le FHSS est ici un mécanisme déterministe de répartition fréquentielle. La connaissance ou la reconstruction de sa table ne constitue pas une authentification de la source.

Dans le chemin de génération testé, le bit de poids fort d'UID2 ne distingue pas la table FHSS : $\texttt{UID2}{=}x$ et $\texttt{UID2}{=}x \oplus \texttt{0x80}$ appartiennent à la même classe effective. Une fois UID4 et UID5 obtenus depuis un SYNC valide, l'espace utile portant sur les sept bits de poids faible d'UID2, notés `UID2[6:0]` ou `UID2 & 0x7F`, et sur UID3 contient donc

$$2^7 \times 2^8 = 32\,768 \tag{19}$$

classes, plutôt que 65 536 couples d'octets nominaux. Un corpus contenant une table de 240 positions par classe représente

$$32\,768 \times 240 = 7\,864\,320 \tag{20}$$

octets bruts de canaux, soit environ 7,5 Mio avant métadonnées et indexation. Cette taille permet une préconstruction déterministe du corpus de tables.

Réduction de l'espace des candidats. Pour une fréquence observée f_k à la position i_k, l'ensemble des candidats compatibles est réduit par

$$\mathcal{C}_{k+1} = \{c \in \mathcal{C}_k \mid h_c(i_k) = f_k\} \,. \tag{21}$$

Chaque observation positive élimine ainsi les candidats dont la fréquence prédite diverge de la fréquence observée.

L'implémentation hors ligne construit l'index inversé

$$(i_k, f_k) \longmapsto \{c \mid h_c(i_k) = f_k\}. \tag{22}$$

Chaque ensemble de candidats est représenté par un vecteur de bits stocké dans un entier Python de longueur arbitraire ; l'élagage se réduit alors à des opérations `AND` successives. Seules les observations positives sont utilisées comme contraintes dures. Une absence de paquet peut résulter d'une erreur temporelle, d'une perte de canal, d'un créneau de télémétrie ou d'un état du récepteur sans rapport avec le candidat ; elle n'est donc pas interprétée comme une preuve d'invalidité.

Si le décalage cyclique τ n'est pas fixé, un score d'alignement peut être défini par

$$S(c, \tau) = \sum_{k=1}^{N} \mathbf{1}\big[h_c\big((i_k + \tau) \bmod L\big) = f_k\big]\,. \tag{23}$$

L'indice de table est ainsi évalué modulo sa longueur cyclique L. H10, H12 et H44F-A utilisent toutefois une intersection exacte des contraintes, puis une validation sur des observations indépendantes, plutôt qu'un verdict fondé sur un seuil appliqué à S.

5. Méthode expérimentale

Les preuves sont classées A (mesure matérielle), B (résultat hors ligne exact), C (source amont épinglée), D (analyse dérivée documentée), E (interprétation) ou F (non démontré). Les éléments de classes E et F ne sont jamais présentés comme des résultats expérimentaux. Chaque valeur quantitative renvoie à un fichier primaire, un localisateur, un vérificateur et une empreinte SHA-256. Les figures sont régénérées depuis des copies de travail en lecture seule. Le code original, les éléments amont, leurs ancres et les comparaisons sémantiques étroites sont séparés et ne sont pas relicenciés.

Les essais ExpressLRS 3 utilisent une carte Heltec WiFi LoRa 32 V3 équipée d'un SX1262 comme récepteur et, uniquement pendant les phases actives protégées, comme émetteur de laboratoire [10]. Les essais ExpressLRS 4.1 utilisent un module EMAX NANO 900TX comme source de référence, un récepteur stock non modifié, une carte Heltec/SX1262 comme source programmable et un moniteur CRSF indépendant. Dans les journaux et données RAW, les étiquettes *Aeris* et *Heltec* désignent respectivement la source de référence et la source substitutive.

H37C, antérieur aux campagnes finales, caractérise en lecture seule le module, la version logicielle 4.1.0 et son interface CRSF normale à 400000 bauds. Il n'initialise pas le SX1262, n'émet pas en RF et ne fournit ni profil OTA, ni identité, ni table FHSS à la chaîne finale.

Sélection du périmètre matériel interversions. L'inventaire de firmwares disponibles pour le banc comprend 4.0.0, 4.0.1 et 4.1.0, un sous-ensemble 3.x s'étendant de 3.0.0 à 3.6.4, ainsi que 2.5.0, 2.5.1 et 2.5.2. Il ne comprend ni image 1.x, ni image 2.0–2.4. La présence d'une image ne suffit toutefois pas à constituer une preuve matérielle : il faut également une paire TX/RX compatible et restaurable, une cible de compilation épinglée, un chemin radio observable par l'instrumentation et un protocole de vérification propre à la famille.

Des configurations 3 et 4 ont été retenues pour les campagnes RF parce que ces conditions étaient établies sur le banc : la chaîne ELRS 3 disposait des cibles SX127x/SX1262 déjà caractérisées dans H8B et H15/H16, tandis que la chaîne ELRS 4.1 disposait d'une paire stock, du sélecteur passif et de la chaîne intégrée H44F-A. Le niveau de preuve diffère : les campagnes 3.x séparent la reconstruction FHSS (H8B/H10/H12) de la substitution contrôlée (H15), tandis que 4.1 les réunit avec la sélection aveugle du profil dans une chaîne intégrée.

Ce choix ne suppose pas quatre algorithmes disjoints. L'audit de la Section 4 montre au contraire des invariants transversaux : UID et PHY 50 Hz communs, PRNG identique de 2.0.0 à 4.0.1, mélange par blocs commun aux versions 2–4 et même comportement FHSS aux trois jalons 3.x. Graine, CRC, SYNC, nonce et format OTA restent traités séparément.

Les images 2.5.x disponibles n'ont pas, dans cette étude, fait l'objet du préflight matériel complet nécessaire à une campagne aveugle comparable. Les règles sélectionnées de 4.0 et 4.1 étant identiques dans le diff épinglé, la campagne matérielle complète a été exécutée sur 4.1 ; cette équivalence de source ne transforme pas 4.0 en validation RF. Le choix des configurations 3.x et 4.1 constitue donc un échantillonnage raisonné de deux chemins matériels instrumentables. Les invariants partagés élargissent la portée de l'audit logiciel, mais pas celle de la preuve RF.

Chronologie de développement et campagne finale. Le noyau de reconstruction à profil fixé a d'abord été validé dans les runs intermédiaires H43, puis le sélecteur passif a été développé séparément sous l'alias H44. Ces identifiants décrivent la chronologie de développement et restent attachés à leurs artefacts historiques. La campagne finale H44F-A réunit ensuite les deux étapes dans un firmware, un protocole série, un journal et un verdict uniques. Son ordre d'exécution est sélection du profil, purge et réinitialisation, puis reconstruction aveugle depuis un SYNC frais. Les compteurs des campagnes intermédiaires ne sont pas agrégés à ceux de H44F-A.

H44F-B est exécutée ultérieurement comme validation matérielle passive complémentaire et indépendante. Elle reprend la sélection aveugle du profil et la reconstruction UID2/UID3, mais borne le sondage à cinq observations et le suivi réservé à cinq sauts. Elle reste RX-only et n'exécute ni substitution, ni rétention, ni récupération de source. Son journal et son verdict ne sont pas agrégés à ceux de H44F-A.

Sélection dynamique du profil radio. La première étape de H44F-A remplace le profil radio précédemment fixé à la compilation par une sélection dynamique à l'exécution. Les six profils logiques ExpressLRS 4.1

SX127x/900 MHz sont reconstruits depuis les sources épinglées, traduits en paramètres de réception SX1262, puis appliqués successivement en réception seule sur leur fréquence SYNC respective.

Pour chaque profil candidat ρ_j, H44F-A journalise notamment le débit radio, le facteur d'étalement, la bande passante, le taux de codage, le préambule, la longueur de charge utile, l'intervalle de paquet, l'intervalle de saut, le temps d'occupation, le nombre de réceptions terminées, les candidats SYNC et les SYNC valides. Un profil passe la première étape lorsqu'il produit une trame SYNC de structure correcte et de CRC valide.

Le balayage doit produire exactement un gagnant. Une absence de profil valide ou plusieurs gagnants entraîne l'arrêt de la chaîne, sans autoriser l'émission RF de la plateforme Heltec. Le profil retenu est ensuite soumis à une acquisition indépendante confirmant le même débit radio et les mêmes octets UID4/UID5.

Après confirmation, les états du balayage, du classifieur et de l'identité sont purgés, puis la radio est réinitialisée. Aucun octet d'identité n'est transmis au noyau aveugle. Seul le profil radio sélectionné dynamiquement est conservé.

La première partie de la chaîne préenregistrée est ainsi

$$\begin{array}{c}\text{profils issus des sources} \rightarrow \text{balayage RX-only}\\ \downarrow\\ \text{profil unique} \rightarrow \text{confirmation indépendante}\\ \downarrow\\ \text{purge des états et réinitialisation}\\ \downarrow\\ \text{transmission du seul profil au noyau aveugle.}\end{array}$$

H44F-A est exécutée sans oracle de profil ou d'identité et sans phrase de liaison. Pendant le balayage, la Heltec/SX1262 reste en réception seule et n'émet pas ; la source de référence émet les SYNC observés. Les critères de garde incluent l'absence d'appel à la mise en émission de la Heltec, la purge des états, l'absence de transfert d'identité et l'acquisition d'un nouveau SYNC par le noyau après réinitialisation.

Reconstruction aveugle et suivi FHSS. À partir du profil sélectionné, le noyau aveugle de H44F-A débute sans UID, initialisation CRC, graine ou table FHSS compilés, et sans phrase de liaison ni oracle d'identité. La chaîne intégrée préenregistrée est

$$\begin{array}{c}\text{SYNC aveugle} \rightarrow (u_4, u_5, I_4) \rightarrow \text{sondage}\\ \downarrow\\ (u_2, u_3) \rightarrow \text{table FHSS} \rightarrow \text{SYNC frais}\\ \downarrow\\ \text{suivi 960/960 ; erreurs CRC/canal : 0}\\ \text{transition RX–TX}\rightarrow\text{substitution}\\ \downarrow\\ \text{retour de la référence} \rightarrow \text{rétention du substitut}\\ \downarrow\\ \text{arrêt du substitut} \rightarrow \text{récupération de la référence.}\end{array}$$

UID4/UID5 sont lus dans chaque SYNC candidat ; la règle publique propre à la version en déduit un initialiseur CRC de base, puis le CRC recalculé valide ou rejette le candidat. Cet initialiseur n'est donc pas une mesure indépendante. Les observations positives associant un indice de table à un canal fréquentiel contraignent ensuite UID2/UID3. Deux candidats différant uniquement par le bit 7 d'UID2 sont conservés lorsque leurs tables de 240 positions sont strictement identiques. Ils constituent alors une même classe d'équivalence FHSS, sans déterminer à eux seuls l'UID nominale.

Le suivi exige un tour complet de la table, au moins 500 paquets valides, aucune erreur CRC, aucune divergence entre le canal prédit et le canal observé, et aucun recours à un oracle d'identité. La campagne finale utilise 960 créneaux, correspondant à 240 sauts et à la couverture des 240 positions de la table.

Après le suivi, un nouveau SYNC est acquis avant la transition RX–TX. La source de référence est ensuite interrompue volontairement avant le début de l'émission substitutive. Elle est réactivée uniquement après l'acquisition de la source substitutive par le récepteur stock. La phase finale vérifie successivement la substitution, la rétention de la source substitutive après retour de la référence, puis la récupération de cette dernière après arrêt de la source substitutive.

Attribution des sources. Les sources de référence et substitutive produisent des signatures CRSF multivoies distinctes et préenregistrées. Le parseur hors ligne vérifie chaque trame RC de 26 octets, son CRC-8 CRSF de polynôme `0xD5`, sa forme, la continuité de séquence et ses 16 canaux avant de l'attribuer à la source de référence, à la source substitutive ou à la classe `unknown`.

Ce CRC-8 porte sur la couche série CRSF ; il est distinct du CRC-14 `0x2E57` des paquets radio OTA et n'authentifie pas leur source.

L'attribution des sources est indépendante de la démodulation RF utilisée pour la reconstruction. Elle sert à vérifier quelle source commande effectivement le récepteur pendant les phases de référence seule, de substitution, de présence simultanée et de récupération.

La phrase de liaison reste séparée du protocole aveugle. Elle n'est jamais fournie au firmware, au reconstructeur ou au vérificateur principal. Elle ne sert qu'à une vérification privée postérieure de l'UID nominale, explicitement exclue du verdict aveugle.

Métriques. Le taux conditionnel de suivi et le résidu d'ordonnancement sont définis par

$$P_{\text{track}} = \frac{N_{\text{matched}}}{N_{\text{observed}}}, \qquad r_k = t_k - (t_0 + kT_s). \tag{24}$$

Le résidu maximal rapporté est

$$r_{\max} = \max_k |r_k|. \tag{25}$$

P_{track} est conditionné aux créneaux effectivement observés pendant la fenêtre de suivi. Il ne constitue ni une estimation universelle du taux de livraison de la liaison, ni une mesure de portée, ni une preuve de domination RF.

Le verdict matériel est complété par une vérification hors ligne des journaux et captures RAW. Celle-ci contrôle les contrats aveugles, l'unicité du balayage, la confirmation du profil, la purge des états, la reconstruction, le suivi, les événements opérateur, la capture complète, l'absence de divulgation de la phrase de liaison et l'état sûr final. Le run n'est déclaré PASS que si les verdicts embarqué et hors ligne concordent et qu'aucun contrôle obligatoire n'échoue.

6. Résultats

Les validations hors ligne comparent les implémentations Python indépendantes à des références C++ compilées séparément et dérivées des sources sur 39 845 888 entrées et 32 768 classes `UID2[6:0]`/UID3 par référence, sans divergence. Le validateur multiversion initial couvre 31 981 568 entrées ; son contrôle négatif réussit et ses 64/64 allers-retours déterministes sont exacts. Une validation complémentaire propre au tag ExpressLRS 4.1.0 compare ensuite 7 864 320 positions directement au code amont épinglé au commit `a9d4a9cb5b5687c4c9d7e9e7fbdf44ad93651da6`, également sans divergence. ExpressLRS 1 représente 8 388 608 entrées de longueur 256 ; ExpressLRS 2, 3, 4.0 et 4.1 représentent chacun 7 864 320 entrées de longueur 240. Les matrices 4.0 et 4.1 sont identiques pour les règles sélectionnées, mais leurs comparaisons aux deux références amont épinglées ont été exécutées et sont comptées séparément. Ces résultats portent sur les modèles logiciels sélectionnés ; ils ne constituent pas des validations RF des familles complètes de firmwares.

Les campagnes antérieures établissent séparément les étapes élémentaires. H8B enregistre 44 877 correspondances CRC valides sur 44 902 créneaux, sans divergence de canal, sur les 240 positions de la table et 46 cycles. H10 et H12 réduisent indépendamment 128 classes radio à une seule et valident respectivement 30/30 puis 48/48 positions réservées. La Figure 2 replace ces réductions parmi les validations complémentaires H8B, H15, H28 et H44F-A, sans agréger leurs métriques de nature différente.

H15 réalise six cycles contrôlés ExpressLRS 3 et 5 574/5 574 événements `TxDone`. Sa séquence de 16 états fait varier CH1–CH4, avec le throttle au minimum et les canaux AUX sûrs maintenus bas ; elle ne démontre donc pas le contrôle arbitraire de tout l'espace AUX.

H28 réalise cinq runs ExpressLRS 4.1 à identité connue, soit 4 800 fenêtres de suivi et les 240 indices de table par run, avec un résidu maximal de 409 μs. À l'inverse, H29F ne valide aucun candidat aveugle, H38F observe 148 événements `RxDone` sans SYNC valide, et H39 échoue avant capture. Ces résultats négatifs restent valides pour leurs chemins expérimentaux respectifs ; H44F-A utilise une chaîne intégrée distincte et ne les requalifie pas rétroactivement.

6.1 H42B_R2 : caractérisation préparatoire de l'attribution et de la rétention

H42B_R2 constitue une campagne préparatoire de caractérisation des sources ; elle ne réalise pas la reconstruction aveugle intégrée de H44F-A. Son parseur reproduit 4 875/4 875 trames RC RAW sans erreur CRC, de forme ou de séquence, et sans source inconnue.

Dans `BOTH_ON_1`, la source de référence est établie en premier : 1 253/1 253 trames sont attribuées à Aeris et aucune à Heltec. Après interruption de la référence, les 1 334/1 334 trames de `AERIS_OFF_1` sont attribuées à Heltec. Environ 5,98 s séparent la dernière trame Aeris de la première trame Heltec.

Après retour de la référence, les 1 287/1 287 trames de `BOTH_ON_2` restent attribuées à Heltec, sans alternance, fusion ou source inconnue. Enfin, les 1 001/1 001 trames de `AERIS_OFF_2` restent attribuées à Heltec. H42B_R2 établit ainsi l'attribution multivoie et la continuité au profit de la source déjà acquise ; elle ne démontre pas la préemption initiale d'une source continuellement active.

6.2 H44F-A : campagne aveugle intégrée

H44F-A réunit dans un même firmware et un journal unique la sélection passive du profil, la reconstruction aveugle de l'identité opérationnelle, le suivi FHSS et la validation active contrôlée. La campagne est identifiée par l'UUID public `5e47158c-14cb-4395-a803-47ea468e8e8a` ; aucun horodatage absolu n'est utilisé comme alias dans l'article.

La stimulation CRSF filaire du module de référence envoie 9 459 trames sans erreur d'écriture. Pendant le balayage, le SX1262 Heltec reste en réception seule : `heltec_rf_tx=0` et aucun appel à la mise en émission n'est effectué. Les six profils logiques ExpressLRS 4.1 SX127x/900 MHz reconstruits depuis les sources épinglées sont testés. Un seul produit un SYNC satisfaisant simultanément les contrôles de structure, de débit énuméré et de CRC : `LORA_900_50HZ`. Il utilise SF8, 500 kHz, un taux de codage 4/7, un préambule de 10 symboles, une charge utile de 8 octets, un intervalle de 20 000 μs et un saut toutes les quatre trames.

Une acquisition après réinitialisation complète confirme indépendamment le même débit et les mêmes octets UID4/UID5. Les états du balayage, du classifieur et de l'identité sont alors purgés ; le stimulus est arrêté, GPIO47 est remis en entrée et aucun octet d'identité n'est transmis au noyau aveugle. Les quatre portes de sélection valent

$$\begin{aligned} &\texttt{profile\_sweep\_pass} = 1, && \texttt{profile\_lock\_pass} = 1, \\ &\texttt{profile\_confirm\_pass} = 1, && \texttt{handoff\_pass} = 1. \end{aligned} \tag{26}$$

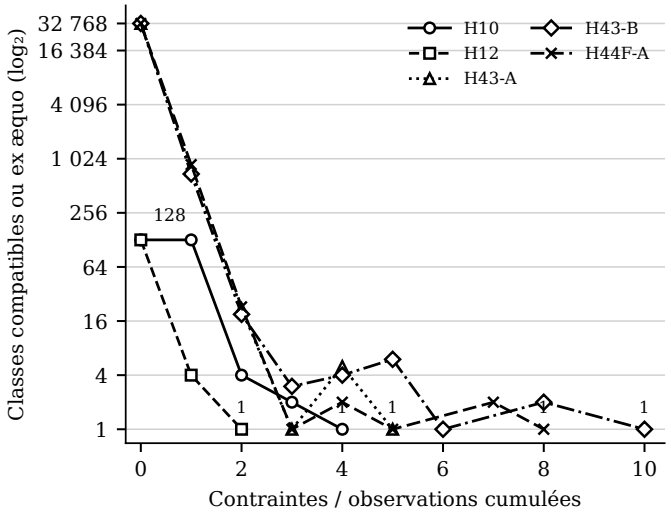
Le noyau repart d'un SYNC frais, sans UID, initialiseur CRC de base, graine ou table FHSS compilés, sans phrase de liaison et sans oracle d'identité. Le sondage de 3 000 créneaux journalise 64 observations positives. La reconstruction obtient UID2 `3F|BF`, UID3–5 `35:59:F0`, l'initialiseur CRC de base `0x5DF0`, déduit d'UID4/UID5, et les graines `0x3F3559F4`/ `0xBF3559F4`, dont les tables de 240 positions sont identiques. Le suffixe `F4` des graines résulte de $\texttt{F0} \oplus \texttt{04}$. Tous les critères embarqués sont satisfaits :

$$\begin{aligned} &\texttt{blind\_sync\_pass} = 1, && \texttt{probe\_pass} = 1, \\ &\texttt{reconstruction\_pass} = 1, && \texttt{fhss\_follow\_pass} = 1, \\ &\texttt{takeover\_pass} = 1, && \texttt{incumbent\_lock\_pass} = 1, \\ &\texttt{aeris\_recovery\_pass} = 1, && \texttt{raw\_pass} = 1, \\ & && \texttt{final\_safe} = 1. \end{aligned} \tag{27}$$

Table 2 – Validation des tags et configurations testés, bornée par les preuves. La validation hôte/source porte sur les règles de reconstruction sélectionnées, non sur une famille complète de firmwares. La ligne matérielle ELRS 3 donne les versions effectives du banc H8B. « Substitution » désigne l'acceptation contrôlée d'une source par un RX stock, non un contrôle AUX arbitraire ni la préemption initiale d'une source continuellement active.

Tag/configuration testé	Validation hors ligne/source	RF passive	Suivi temps réel	Substitution
1.2.1	HÔTE VALIDÉ	NON TESTÉ	NON TESTÉ	NON TESTÉ
2.5.2	HÔTE VALIDÉ	NON TESTÉ	NON TESTÉ	NON TESTÉ
3.3.0 TX / 3.3.2 RX	SOURCE VALIDÉE	DÉMONTRÉ	DÉMONTRÉ	DÉMONTRÉ
3.6.4	HÔTE VALIDÉ	NON TESTÉ	NON TESTÉ	NON TESTÉ
4.0.1	HÔTE VALIDÉ	NON TESTÉ	NON TESTÉ	NON TESTÉ
4.1.0	HÔTE/AMONT VALIDÉ	DÉMONTRÉ	DÉMONTRÉ	DÉMONTRÉ

(a) Réduction et convergence



(b) Validations complémentaires

Campagne	Mesure	Couverture / erreurs
H8B	44 877 / 44 902	240 pos. ; div. 0
H10	30/30 réservées	30 can. ; div. 0
H12	48/48 réservées	27 can. ; div. 0
H15	5 574/5 574 TxDone	6 cycles
H28	4 800 fenêtres	5 runs ; 240 ind./run
H44F-A	960/960 paquets	240/240 pos. ; erreurs 0

Figure 2 – Réduction des classes FHSS et validations expérimentales complémentaires. À gauche, H10 et H12 appliquent une intersection exacte à 128 classes. H43-A, H43-B et H44F-A partent de 32 768 classes canoniques `UID2[6:0]`/UID3 ; leurs courbes indiquent le nombre de classes ex æquo au meilleur score cumulatif jusqu'à stabilisation d'une classe unique. Une remontée temporaire traduit donc un nouvel ex æquo, et non la réintroduction d'une classe éliminée par une intersection exacte. À droite, les métriques restent exprimées dans leurs unités propres pour H8B, H10, H12, H15, H28 et H44F-A ; elles ne sont pas agrégées. Les comptes désignent des classes de tables radio, et non des UID littérales.

Le suivi couvre 960 créneaux, 240 sauts et les 240 positions de la table. Il produit 960 événements `RxDone` et 960 paquets valides, sans erreur CRC ni divergence de canal ; le résidu maximal vaut 2 327 μs. Après acquisition d'un nouveau SYNC et interruption physique de la référence, la phase TX bornée couvre 6 000 créneaux : 5 625 émissions aboutissent à 5 625 événements `TxDone`, avec 375 créneaux de télémétrie, aucun timeout, aucun échec de recalage et des erreurs radio finales nulles.

Le parseur attribue 1 533/1 533 commandes à Heltec pendant la prise de relais et 3 698/3 698 à cette même source après le retour d'Aeris, sans trame Aeris ni source inconnue dans ces deux phases. Après l'arrêt de Heltec, la récupération contient 439 trames Aeris et une dernière trame Heltec, sans source inconnue et avec une transition unique. Environ 5,584 s séparent la dernière trame Heltec de la première trame Aeris.

Le verdict du noyau, le verdict global et leurs vérifications hors ligne valent tous `PASS`. La capture contient 5 671 lignes RAW, sans erreur CRC, de forme ou de séquence et sans débordement. L'arrêt final désactive l'émission RF et replace GPIO47 et GPIO42 en entrée. L'empreinte SHA-256 du journal public assaini et vérifié est `e8e4a73a0d802861cec98e5ef0a34aaf2366cd9e5624b872626d3cb764fc4aff` . Le paquet combiné fournit en outre une copie de rejeu normalisée, obtenue par suppression du seul bruit binaire de démarrage ; son empreinte est `bf9f6e041be81515d1c5c9a996f68fc804ff9fa129a5324f5dc11ab3c23f818e`. Le manifeste conserve les deux empreintes et explicite cette dérivation.

H44F-A constitue ainsi la validation intégrée de la chaîne complète :

sélection dynamique du profil
↓
reconstruction aveugle → suivi FHSS 960/960
↓
substitution contrôlée
↓
rétention après retour de la référence
↓
récupération après arrêt du substitut.

Les campagnes intermédiaires de développement restent conservées dans l'artefact historique, avec leurs verdicts propres. Elles ont validé séparément le noyau aveugle à profil fixé puis le sélecteur passif. Elles ne sont pas agrégées aux compteurs de H44F-A et ne portent pas le verdict de la campagne finale.

6.3 H44F-B : validation passive FAST sur cinq sauts

H44F-B constitue une répétition matérielle passive distincte, identifiée par l'UUID public `583431a1-9948-4173-9b9b-14954169cb33`. Elle sélectionne et confirme à froid le même profil `LORA_900_50HZ`, purge l'état d'identité, puis acquiert un nouveau SYNC CRC-valide. Le sondage s'arrête dès cinq observations positives situées sur cinq indices FHSS distincts.

La recherche exhaustive des 32 768 classes canoniques `UID2[6:0]`/UID3 laisse une classe unique : UID2 `3F|BF`, UID3 `35`, avec UID4/UID5 `59:F0` et les graines `0x3F3559F4`/`0xBF3559F4`. Quatre observations correspondent exactement à la table et une utilise la tolérance bornée d'un canal adjacent. Une acquisition fraîche valide ensuite la table sans tolérance sur cinq sauts et 20/20 paquets CRC-valides, avec zéro divergence de canal et un résidu maximal de 2 006 μs.

Le verdict embarqué et le rejeu hors ligne valent `PASS`. L'empreinte du journal de rejeu anonymisé est `fefe06180f79758c58160a60110ebeab99e778eea659a21b36feca105e9fc83b`. Le SX1262 Heltec reste en réception seule pendant toute la campagne et l'arrêt final remet GPIO47 en entrée. H44F-B confirme donc matériellement la reconstruction passive rapide dans cette session ; elle ne démontre ni substitution, ni rétention, ni récupération de source et ne remplace pas H44F-A.

7. Conséquences de sécurité et contre-mesures

7.1 Positionnement du protocole et portée de l'analyse

ExpressLRS est un protocole open source conçu en priorité comme une liaison de radiocommande performante pour les usages FPV : faible latence, portée, robustesse radio, efficacité spectrale et compatibilité avec des matériels contraints [6, 8]. Dans ce périmètre, son architecture est cohérente et particulièrement efficace.

ExpressLRS n'est toutefois ni présenté ni évalué par le projet comme un système de commandement et de contrôle sécurisé, durci contre un adversaire actif, ou comme une liaison militaire certifiée. La présente étude ne montre donc pas que le protocole échoue à remplir sa fonction première. Elle examine ce qui se produit lorsqu'une liaison civile orientée vers la performance est placée dans un modèle de menace cyberélectromagnétique plus exigeant que celui de son usage nominal.

L'emploi éventuel d'ExpressLRS dans un environnement contesté, de sécurité critique ou militaire modifie le modèle de menace sans modifier rétroactivement les objectifs de conception du protocole. Les résultats présentés doivent ainsi être compris comme une analyse de l'écart entre ces deux contextes, et non comme une attaque contre le projet, ses développeurs ou la qualité de son ingénierie.

7.2 Phrase de liaison, entropie et authentification

Une phrase de liaison forte reste nécessaire. Elle devrait être générée par un CSPRNG, être unique pour chaque liaison et ne contenir aucun nom, date, motif prévisible ou valeur réutilisée entre équipements ou flottes. Une min-entropie d'au moins 128 bits constitue une base raisonnable ; une valeur aléatoire de 256 bits reste également pratique [11, 12, 13].

Une telle valeur protège principalement contre le devinement direct, les dictionnaires et la réutilisation de secrets prévisibles. Elle reste utile pour la configuration, la coordination et l'identification radio. H44F-A ne récupère cependant pas la phrase de liaison : la campagne reconstruit directement les dérivés opérationnels nécessaires à l'état radio testé.

La distinction est essentielle :

> *Le FHSS n'est pas une authentification ; le CRC n'est pas un MAC ; une phrase de liaison forte protège contre le devinement de la phrase, mais n'authentifie pas nécessairement tous les états radio opérationnels qui en dérivent.*

L'UID nominale et la classe d'équivalence FHSS effective sont également deux objets distincts. Plusieurs valeurs littérales peuvent conduire à une même table FHSS et rester indiscernables par l'observation de la seule séquence de saut. Une forte entropie d'entrée ne remplace donc ni l'authentification cryptographique de la source, ni l'intégrité des commandes, ni une notion authentifiée de fraîcheur.

Le problème observé ne se réduit pas à l'emploi de MD5 pour la dérivation de configuration. Remplacer uniquement la fonction de hachage, sans modifier la structure d'authentification des trames et des états de synchronisation, ne suffirait pas à empêcher la reconstruction des dérivés opérationnels ou l'acceptation d'une source radio compatible.

7.3 Configuration et évolution du protocole

Dans les déploiements actuels, l'utilisateur devrait générer et conserver de manière sûre une valeur aléatoire unique pour chaque liaison. La réutilisation d'une même phrase entre plusieurs équipements ou une flotte entière augmente la portée d'une compromission et facilite la corrélation des identités.

Un sel peut empêcher la réutilisation globale de certains précalculs, mais il ne transforme pas une phrase faible en secret fort. Il n'authentifie pas davantage les commandes, les trames SYNC ou les transitions d'état.

Pour un profil de sécurité plus exigeant, une identité radio publique devrait être séparée d'un secret d'authentification indépendant. Une KDF moderne, contextualisée et dotée d'une séparation de domaines pourrait dériver des clés distinctes pour l'authentification, la synchronisation et, si nécessaire, la confidentialité.

Les commandes, les états critiques et les transitions SYNC devraient porter une preuve d'intégrité authentifiée, associée à un compteur ou à un nonce également authentifié. Le protocole devrait alors définir explicitement :

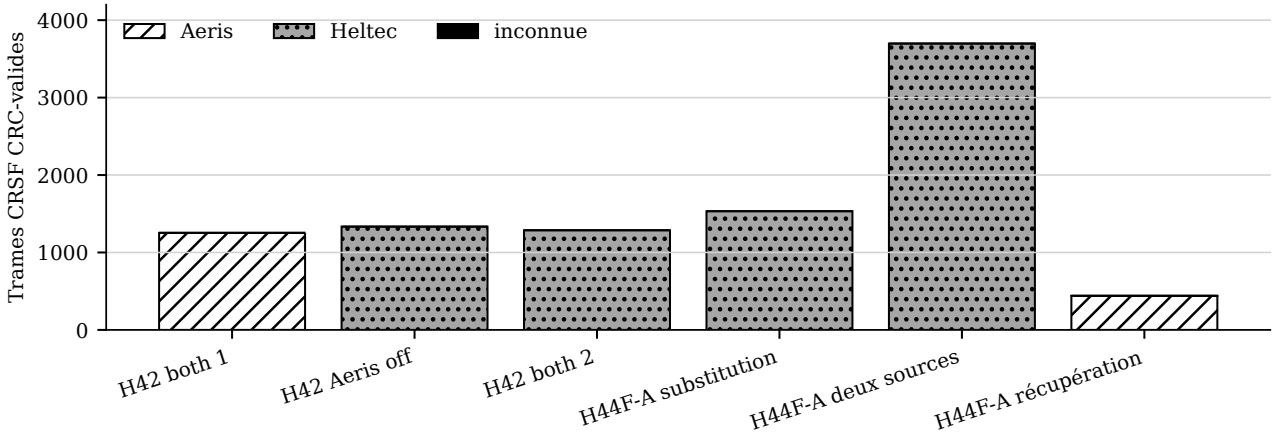


Figure 3 – Attribution des sources régénérée depuis les captures RAW H42B_R2 et H44F-A. L'émission H44F-A débute après interruption volontaire de la référence ; la phase « both on » mesure la rétention de la source substitutive, et non une contention initiale contre une source continuellement active. La phase terminale `AERIS_OFF_2` de H42B_R2 n'est pas représentée.

Table 3 – Synthèse compacte des résultats. Les preuves primaires et leur interprétation dérivée sont séparées ; les niveaux sont définis dans la Section 5.

Campagne	Tag/profil	Résultat et frontière	Preuves primaires	Interprétation dérivée
Hors ligne	1.2.1/2.5.2/3.6.4/ 4.0.1/4.1.0	Comparaisons Python/C++ indépendantes : 39 845 888 entrées, 0 divergence	B, C	–
H8B/H10/H12	3.3.0 TX/3.3.2 RX	44 877 correspondances paquets/canaux ; une classe FHSS réservée	A, B, C	D
H15	3.3.x	6/6 cycles ; throttle minimal et AUX sûrs inchangés	A	–
H42B_R2	4.1.0	4 875 trames attribuées propres ; rétention de source acquise	A, B	D
H44F-A	4.1.0 / profil 50 Hz sélectionné	Profil aveugle unique ; reconstruction ; suivi 960/960 ; substitution, rétention et récupération sur RX stock ; 5 671 trames RAW intègres	A, B, C	D
H44F-B	4.1.0 / profil 50 Hz sélectionné	Validation RX-only distincte ; classe unique après cinq observations ; suivi réservé de cinq sauts et 20/20 paquets valides, sans divergence	A, B, C	D

— la protection anti-rejeu ;
— la persistance des compteurs après redémarrage ;
— la reprise après pertes de paquets ;
— le renouvellement sûr des clés ;
— le comportement lors d'une désynchronisation ;
— l'absence de remise à zéro de la confiance par une resynchronisation non authentifiée.

Le résultat expérimental met d'abord en évidence un besoin d'authentification de l'intégrité et de la fraîcheur ; il ne démontre pas un besoin de confidentialité. Un MAC, par exemple CMAC ou HMAC, associé à un compteur ou à un nonce authentifié constitue donc une réponse conceptuelle minimale [14, 15]. Un mode AEAD évalué, tel que ChaCha20-Poly1305, ne devient pertinent que si la confidentialité des commandes ou de la télémétrie est également recherchée [16].

Les trames SYNC, les compteurs et les transitions de resynchronisation doivent eux-mêmes être authentifiés ; chiffrer les seules commandes ne suffirait pas. Compte tenu de la charge utile de huit octets du profil étudié, ces mécanismes ne peuvent pas être ajoutés comme une simple option. Ils nécessiteraient un format OTA distinct et une évaluation expérimentale de la longueur du tag et du nonce, du débit, de la latence, du temps d'antenne, de la mémoire, de la consommation, de la reprise après pertes et de la rétrocompatibilité.

Ces propositions correspondent à un éventuel profil *Secure C2* distinct du profil FPV nominal. Elles ne doivent pas imposer au protocole civil d'origine des objectifs qu'il n'a pas revendiqués, mais fournir une base pour une variante destinée à des environnements adversariaux.

7.4 Détection et défense en profondeur

En l'absence d'authentification cryptographique complète, une défense complémentaire peut surveiller :
— les discontinuités de SYNC ou de nonce ;
— les retours inattendus à un état de synchronisation antérieur ;
— les identités logiques dupliquées associées à des empreintes RF différentes ;
— les variations rapides de puissance, de fréquence ou de provenance ;
— les changements de source observés sur l'interface de commande ;

— les récupérations ou réacquisitions de source inattendues.

Ces indices peuvent aider à détecter une anomalie, mais ils ne constituent pas des preuves cryptographiques. Les variations de propagation, les pertes de paquets, les redémarrages légitimes et les changements de puissance peuvent produire des faux positifs. La détection doit donc être considérée comme une mesure de défense en profondeur, et non comme un substitut à l'authentification des commandes et des états de synchronisation.

Limites, éthique et divulgation

Statut de divulgation. Certaines propriétés générales pertinentes avaient déjà fait l'objet de discussions publiques avant la présente étude. Aucun processus privé de divulgation coordonnée avec les mainteneurs du projet n'a précédé la préparation du manuscrit. Des parties prenantes concernées ont néanmoins été informées des risques identifiés avant publication. Cette mention décrit uniquement la chronologie de diffusion et ne suppose ni validation ni approbation des résultats par les mainteneurs.

Anonymisation et publication des artefacts. Le corps de l'article identifie les campagnes par des alias stables, notamment `H42B_R2`, `H44F-A` et `H44F-B`, plutôt que par leurs horodatages absolus. Le manifeste public associe chaque alias à un UUID public, au verdict correspondant, à la liste de ses fichiers et aux empreintes SHA-256 des copies publiées. L'UUID sert uniquement d'identifiant ; l'intégrité est assurée par les empreintes cryptographiques.

Les copies publiques des journaux remplacent les dates absolues par des temps relatifs ou des numéros de créneau, les chemins locaux par des chemins relatifs et les noms de machine ou de session par des identifiants génériques. La correspondance avec les horodatages originaux et les journaux bruts reste conservée dans un manifeste privé. Comme l'anonymisation modifie les fichiers, les empreintes publiques portent sur les copies assainies et non sur les originaux privés.

L'artefact public spécialisé H44F-A/H44F-B fournit les deux journaux de rejeu assainis, leurs UUID et empreintes SHA-256, les captures et tables dérivées, ainsi que les reconstructeurs, parseurs et vérificateurs hors ligne. Il donne les ancres exactes du commit amont et une comparaison sémantique étroite des six profils, sans recopier les sources ExpressLRS. Le paquet général du manuscrit conserve séparément les campagnes historiques et les scripts de régénération des figures. L'artefact spécialisé ne publie pas la phrase de liaison, les outils d'injection directement utilisables, les firmwares prêts à flasher ni des procédures opérationnelles de brouillage ou de neutralisation.

Ce choix permet la vérification des affirmations passives, logiques et expérimentales à partir des journaux, mais limite la reproduction publique directe de la phase active. Cette restriction fait partie des limites de reproductibilité déclarées du paquet public.

La disponibilité locale d'un firmware ne doit pas être confondue avec une validation matérielle de sa famille. Les images 2.5.x et 4.0.x inventoriées n'ont pas reçu le même préflight, la même campagne aveugle et la même vérification RF que les configurations 3.x et 4.1 testées. Les résultats matériels restent donc attachés aux tags, cibles et couples TX/RX explicitement rapportés ; ils ne s'étendent ni aux versions intermédiaires ni à toutes les images disponibles.

Réciproquement, les croisements de code ne doivent pas être ignorés : une empreinte identique du PRNG ou un comportement FHSS identique étend la validation logicielle de cette propriété précise aux tags audités. Cette extension composant par composant ne constitue pas une équivalence globale du firmware et ne remplace pas une campagne RF propre à chaque configuration.

Travaux futurs. Les travaux futurs portent uniquement sur des propriétés non démontrées dans la présente étude : l'extension du sélecteur aux autres profils 900 MHz et aux autres familles radio, l'implémentation des chemins GFSK, la mesure des seuils d'acquisition et de récupération sous atténuation contrôlée, ainsi que la caractérisation instrumentale des marges temporelles et RF.

D'autres travaux pourront étudier la détection défensive des changements de source, l'amélioration de l'acquisition PHY, le suivi, la fusion de capteurs et la calibration des scores de confiance. L'assistance par intelligence artificielle à la classification ou à l'acquisition, le brouillage contrôlé et toute forme de neutralisation restent des directions prospectives. Ils ne sont ni implémentés, ni évalués, ni revendiqués comme résultats de cet article.

8. Conclusion

Dans le périmètre expérimental, la réponse à la question de recherche est affirmative : l'état physique et logique opérationnel d'une liaison ExpressLRS peut être reconstruit à un degré suffisant pour permettre son suivi passif puis une substitution contrôlée de la source après interruption de la référence.

La campagne intégrée H44F-A établit d'abord, sans oracle de profil et en réception seule, la sélection dynamique du profil radio actif parmi les six profils ExpressLRS 4.1 SX127x/900 MHz reconstruits depuis les sources épinglées. Après confirmation indépendante, purge des états et réinitialisation de la radio, son noyau aveugle repart d'un nouveau SYNC, sans phrase de liaison, UID, initialiseur CRC de base, graine ni table FHSS fournis.

Les observations RF non coopératives permettent alors de reconstruire le profil PHY et temporel, l'initialiseur CRC de base déduit d'UID4/UID5, une classe d'équivalence FHSS de l'UID, la graine, la table FHSS et l'état courant de synchronisation. La reconstruction s'appuie sur 64 observations fréquentielles positives recueillies pendant un sondage de 3 000 créneaux.

Le suivi passif valide ensuite 960/960 paquets RF, soit 240 sauts et la couverture complète des 240 positions de la table FHSS, sans échec CRC ni divergence de canal. Ce nombre décrit la fenêtre dédiée à la validation du suivi ; il ne résume pas à lui seul l'ensemble de la campagne.

Après interruption volontaire de la source de référence, un émetteur développé séparément réalise 5 625/5 625 émissions RF, sans timeout ni échec de recalage, et établit une liaison acceptée par un récepteur stock non modifié. Le parseur hors ligne analyse ensuite 5 671 trames RC sans erreur CRC, de forme ou de séquence : 1 533 sont attribuées à la source substitutive pendant la prise de relais, 3 698 restent attribuées à cette source après le retour de la référence, puis la phase de récupération contient 439 trames de la référence et une dernière trame du substitut, avec une transition unique entre les deux sources.

Le récepteur stock conserve donc la source substitutive tant qu'elle reste active, y compris après réactivation de la référence, puis récupère cette dernière après l'arrêt du substitut. Le résultat dépasse ainsi la seule question de la reconstruction et du suivi : il démontre une substitution de source contrôlée après interruption de la référence, puis caractérise expérimentalement la rétention et la récupération de source.

Sélection dynamique du profil radio	OUI
Reconstruction de l'état physique	OUI
Reconstruction logique opérationnelle	OUI
Sondage fréquentiel (3 000 créneaux ; 64 observations positives)	OUI
Suivi FHSS (960/960 ; 240/240 positions)	OUI
Erreurs CRC ou divergences de canal pendant le suivi	0
Émissions RF de substitution (5 625/5 625)	OUI
Validation sur récepteur stock	OUI
Rétention de la source déjà acquise après réapparition de l'autre source	OUI
Récupération de la référence après arrêt du substitut	OUI
Trames RC analysées (5 671 ; erreurs : 0)	OUI
Récupération de la phrase de liaison originale	NON, et non requise
Prise de relais sans interruption préalable de la source déjà acquise	NON TESTÉE

Ces conclusions sont expérimentales et bornées au protocole, à la version, à la bande, aux profils et aux matériels testés. Le récepteur favorise empiriquement la continuité de la source déjà acquise, sans revenir automatiquement à la source antérieure lorsqu'elle réapparaît. La campagne ne teste toutefois pas une prise de relais sans interruption préalable de la source déjà acquise.

Les résultats ne démontrent ni la récupération de la phrase de liaison, ni un cassage de chiffrement, ni une capacité universelle applicable à toutes les versions, bandes, radios ou conditions de propagation.

Ils ne constituent pas davantage une revendication de portée opérationnelle, de brouillage ou de neutralisation générale. Ils caractérisent l'écart entre une liaison civile conçue pour la performance FPV et les propriétés attendues d'un système de commandement et de contrôle sécurisé en environnement adversarial.

Contribution de l'auteur et attribution des travaux antérieurs

Melik Lemariey : conceptualisation de l'étude ExpressLRS actuelle ; méthodologie ; logiciels ; firmwares ; validation ; analyse formelle ; investigation ; curation des données ; visualisation ; rédaction initiale ; révision et approbation du présent préprint.

Les campagnes ExpressLRS rapportées dans ce manuscrit ont été conçues, réalisées et analysées par Melik Lemariey.

Une partie du raisonnement méthodologique s'inscrit dans la continuité de travaux expérimentaux antérieurs menés en collaboration à partir de 2016 sur une liaison radio distincte. Leur description détaillée et l'attribution individuelle des contributions sont différées dans cette version, dans l'attente de leur validation par les participants concernés.

Conflits d'intérêts

L'auteur déclare ne connaître aucun conflit d'intérêts susceptible d'avoir influencé la conduite, l'analyse ou la présentation de cette étude.

Disponibilité des données et du code

Le dépôt public associé est `https://github.com/Melik159/elrs-h44f-executable-evidence`.

L'artefact public spécialisé contient les journaux anonymisés de H44F-A et H44F-B, les captures et données extraites, les tables FHSS reconstruites, les rapports de vérification, les manifestes de traçabilité et les empreintes SHA-256 des copies publiées. Les identifiants temporels absolus, chemins locaux et noms de machine sont remplacés par des alias stables, des UUID publics et des temps relatifs. Les preuves historiques H42B_R2 et les scripts de génération des figures restent distribués séparément dans le paquet général du manuscrit.

L'artefact spécialisé contient également le code hors ligne de reconstruction et de validation, les localisateurs et ancres des sources amont épinglées, une comparaison sémantique étroite des profils et un protocole de rejeu déterministe. Les scripts originaux sont distribués sous Apache-2.0 ; la documentation et les preuves assainies le sont sous CC BY 4.0. Les éléments amont restent séparés, conservent leur propre licence et ne sont pas relicenciés.

La phrase de liaison privée, la correspondance entre les identifiants publics et les journaux originaux, le firmware actif prêt à l'emploi ainsi que les outils d'émission ou d'injection directement opérationnels ne sont pas distribués. Cette restriction limite la reproduction publique directe des phases actives, mais n'empêche pas la vérification hors ligne des résultats rapportés à partir des artefacts assainis.

Déclaration d'usage de l'intelligence artificielle

Des outils d'intelligence artificielle générative ont assisté l'inventaire des artefacts, la génération et la révision de scripts, la préparation du document LaTeX, les contrôles de cohérence et certaines étapes de rédaction.

Ces outils n'ont produit aucune mesure expérimentale et n'ont pas été utilisés comme source de preuve. Les

résultats proviennent exclusivement des captures, journaux, programmes et vérificateurs sélectionnés. Melik Lemariey a contrôlé les sorties utilisées, vérifié les affirmations et demeure seul responsable du contenu et de l'approbation du manuscrit.

Notification des parties prenantes

Des parties prenantes concernées ont été informées des risques identifiés avant la publication de cette étude.

Références

[1] Geneviève Baudoin, Martine Villegas, Jean-François Bercher, Corinne Berland, Jean-Marc Brossier, Daniel Courivaud, Nicolas Gresset, Pascale Jardin, Gaëlle Lissorgues, Christian Ripoll, and Olivier Venard. *Radiocommunications numériques. Tome 1 : Principes, modélisation et simulation.* Technique et ingénierie. Dunod, Paris, 2013. 2e édition.

[2] Martine Villegas, Corinne Berland, Daniel Courivaud, Gaëlle Lissorgues, Christian Ripoll, and Odile Picon. *Radiocommunications numériques. Tome 2 : Conception de circuits intégrés RF et micro-ondes.* Technique et ingénierie. Dunod, Paris, 2007. 2e édition.

[3] g3gg0. Analysis of TBS Crossfire, Reverse Engineering the Air Link. Online technical report, August 2021. Separate 900-MHz RC link ; accessed 30 July 2026.

[4] Richard Appleby. Technical advisory—ExpressLRS vulnerabilities allow for hijack of control link. NCC Group Research, June 2022. Online advisory, published 30 June 2022 ; accessed 30 July 2026.

[5] redfiveau and ExpressLRS contributors. Security Improvements, ExpressLRS Pull Request 1411. GitHub, 2022. Closed unmerged ; accessed 30 July 2026.

[6] ExpressLRS Project. ExpressLRS Source Repository. GitHub, 2026. Pinned revisions are listed in the artifact ; accessed 30 July 2026.

[7] TBS Avionics Co. Ltd. CRSF Protocol Specification. GitHub, 2026. Pinned revision recorded in the artifact ; accessed 30 July 2026.

[8] ExpressLRS Project. Binding ExpressLRS. Official documentation, 2026. Accessed 30 July 2026.

[9] ExpressLRS Project. ExpressLRS version 4.1.0 source tree. GitHub source release, 2026. Tag 4.1.0, commit a9d4a9cb5b5687c4c9d7e9e7fbdf44ad93651da6 ; accessed 31 July 2026.

[10] Semtech Corporation. *SX1261/SX1262 Long Range, Low Power, Sub-GHz RF Transceivers.* Semtech Corporation, 2025. Data sheet ; accessed 31 July 2026.

[11] Donald E. Eastlake, 3rd, Jeffrey I. Schiller, and Steve Crocker. Randomness requirements for security. RFC 4086, RFC Editor, June 2005.

[12] Elaine Barker and John Kelsey. Recommendation for random number generation using deterministic random bit generators. NIST Special Publication 800-90A Revision 1, National Institute of Standards and Technology, 2015.

[13] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. *Cryptography Engineering : Design Principles and Practical Applications.* Wiley, 2010.

[14] Morris J. Dworkin. Recommendation for block cipher modes of operation : The CMAC mode for authentication. NIST Special Publication 800-38B, National Institute of Standards and Technology, 2016.

[15] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC : Keyed-hashing for message authentication. RFC 2104, RFC Editor, 1997.

[16] Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF protocols. RFC 8439, RFC Editor, 2018.