étude fréquentielle

Fréquence en MHZ	0 - 0,19	0,19 - 1,75	1,75 - 2	2 41	41- 46	46 - 86	86 - 108
Airbus	oui	non	oui	non	non	non	non
Eurocopter	oui	non	non	non	non	non	non
autre					bande I tele		Radio, tele bande II

Fréquence en MHZ	108- 174	174-310	310-400	400-450	450-467	467-470	470-496
Airbus	non	non	non	oui	oui	oui	oui
Eurocopter	non	non	non	non	non	non	oui
autre	interbande tele	interbande hyperband bande III	hyper band	hyper band	hyperband et gsm 400	hyper band	gsm 400

Fréquence en MHZ	496-606	606 - 825	825 - 840	840 - 860	860 - 880	880 - 900	900 - 915
Airbus	oui	oui	moyen	moyen	moyen	moyen	moyen
Eurocopter	oui	oui	oui	non	oui	oui	non
autre	bande IV tele	bande V tele				gsm 900 2G	gsm 900 2G

Fréquence en MHZ	915 - 925	925 - 960	960 - 1215	1215 - 1530	1530 - 1660	1660 - 1710	1710 - 1785
Airbus	moyen	moyen	non	oui	non	oui	moyen
Eurocopter	non	non	non	non	non	non	non
autre		gsm 900 2G					gsm 1800 2G

Fréquence en MHZ	1785 - 1800	1800-1805	1805 - 1880	1880-1900	1900-1990	1990 - 2025	2025-2110
Airbus	moyen	moyen	moyen	moyen	moyen	oui	oui
Eurocopter	non	oui	oui	oui	oui	oui	oui
autre			gsm 1800 2G	gsm 1900 2G et 3G	3G	3G	

Fréquence en MHZ	2110-2200	2200 - 2400	2400 - 2483	2483-2500	2500-2690	2690 - 2700	2700 - 2900
Airbus	moyen	moyen	moyen	oui	oui	oui	non
Eurocopter	oui	oui	oui	oui	oui	oui	oui
autre	3G		WIFI et ZIGBEE		2,5G		

Fréquence en MHZ	2900 - 3500	3500 - 4200	4200 - 4400	4400 - 5030	5031 - 5091	5091-5150	5150 - 5350
Airbus	oui	oui	non	oui	non	moyen	moyen
Eurocopter	oui	non	non	non	non	non	non
autre							UMTS 5G

Fréquence en MHZ	5350-5470	5470 - 5500	5500 - 5600	5600 - 5650	5650 - 5725	5725 - 8500	8500 - 9333	9333 - 9345
Airbus	oui	oui	oui	non	oui	oui	oui	non
Eurocopter	non	non	oui	oui	oui	oui	non	non
Autre		UMTS 5G	UMTS 5G	UMTS 5G	UMTS 5G			

9.9. Annexe 9 : étude sécurité

9.9.1. Localisation des points à risques pour la sécurité

Dans cette étude on ne s'intéresse qu'à la sécurité et bien que notre système présente d'autres risques que ce soit au niveau de la fiabilité (conditions environnementales sévères mentionnées plus haut ou tolérance aux fautes) ou de la sureté de fonctionnement (interférences avec le reste de l'avionique embarqué sur l'aéronef) dues au matériel hardware principalement on n'étudiera que l'aspect sécurité qui consiste à prévoir les scenarii d'intrusion volontaires. Les autres aspects sont analysés en profondeur dans une autre étude.

Un intervenant mal intentionné tentera de brouiller ou d'usurper la communication.

On étudiera donc naturellement le sous-système « communication » composé des modules antennes (réception émission) en profondeur pour ce qui concerne la sécurité.

9.9.1.1. Hard

Pour ce qui est du hard, il est suffisamment inaccessible au le public (des études sécurité ont déjà été menée en ce sens) pour avoir à s'en inquiéter. Ceci étant, il est maintenu par le personnel au sol et si un quelconque sabotage au niveau du hard venait à se produire, l'équipe technique serai la seule suspecte. C'est la raison pour laquelle la procédure de maintenance doit être réalisée par plusieurs personnes (démultiplier les effectifs abaisse le pourcentage de chance de corrompre l'intégralité du système de maintenance et ainsi améliore l'intégrité de l'ensemble)

9.9.1.2. Protocole

On se rend bien compte que remplacer les actuelles liaisons filaires par des liaisons sans fils expose les systèmes de capteurs à un risque supplémentaire qui est le risque d'intrusion. En effet un réseau sans fil est interceptable alors qu'un réseau filaire l'est largement moins.

Les points à risque se trouvent tout au long de la liaison sans fil donc entre chaque nœud et à chaque point d'émission et de réception autrement dit tous les points ou le signal peut être intercepté.

Assurer la sécurité c'est prévoir au maximum les risques d'attaque extérieure. Contrairement à la sûreté de fonctionnement ou la fiabilité, ou l'on connaît les éléments contre lesquels on se protège, pour la sécurité l'attaquant est inconnu. On part donc du principe que l'attaquant connaît très bien le système qu'il va chercher les failles pour l'induire en erreur.

Il faut prendre en compte plusieurs paramètres :

- L'impact de l'attaque (en fonction de la criticité de l'attaque)
- Le coût de l'attaque (de quelques milliers à quelques millions pour du terrorisme)
- Le gain de l'attaquant (de l'impossibilité de décoller ou le non fonctionnement d'une application cabine afin d'attirer le mécontentement des passagers au crash de l'avion)

Plusieurs détracteurs peuvent être envisagés : des terroristes ou simplement des espions industriels

9.9.2. Ebauches de solutions pour parer à la sécurité

9.9.2.1. Aspect soft ware :

Protection des protocoles (clefs wep wpa) crypto procédure redondance (Brouillage intrusion par fausse information intrusion par simple écoute)

Plusieurs types d'attaques sont possibles :

9.9.2.1.1. Le dénie de service : une attaque contre la disponibilité.

Ce problème est typique des protocoles Wireless. En effet il est tout à fait possible de saturer le réseau et ainsi brouiller tous les messages de la bande saturée.

Pour éviter ce type de problème, on peut par exemple choisir une bande de fréquence d'émission très étroite et la faire bouger assez rapidement de façon que les intrus ne puissent pas avoir le temps de la trouver et de la saturer. Cette méthode s'appel le saut de fréquence et est utilisée par les militaire. Cependant, la technologie Bluetooth utilise aussi à moindre mesure le saut de fréquence.

On pourra aussi utiliser la télécommunication avec étalement de spectre : Le signal est transmis sur une bande passante considérablement plus large que l'ensemble des fréquences composant le signal original. Cette technique diminue le risque d'interférences avec d'autres signaux reçus tout en garantissant une certaine confidentialité. L'étalement de spectre utilise généralement une séquence ressemblant à du bruit pour étaler le signal de bande étroite en un signal de relative large-bande. Le récepteur récupère le signal original en corrélant le signal reçu avec une réplique de cette séquence.

A l'origine se trouvaient deux motivations : en premier, résister aux efforts ennemis pour brouiller le signal, puis pour cacher la communication elle-même. De nos jours l'aspect partage d'une même fréquence par plusieurs utilisateurs (accès multiple) est une de ses principales applications. Par ailleurs, l'étalement de spectre facilite les transmissions numériques dans les cas d'interférences par trajets multiples.

⇨ Solution n°1 : Le FHSS (Frequency Hopping Spread Spectrum), ou étalement de spectre par saut.

Définition : C'est une méthode de transmission de signaux qui utilise plusieurs canaux répartis sur une large bande de fréquences selon une séquence pseudo-aléatoire connue de l'émetteur et du récepteur.

Avantage : L'étalement de spectre offre trois avantages par rapport à l'utilisation d'une fréquence unique :

1. il rend le signal transmis très résistant aux interférences,
2. le signal est plus difficile à intercepter,
3. les signaux transmis de cette manière peuvent partager des bandes de fréquence avec d'autres types de transmission, ce qui permet d'utiliser plus efficacement la bande passante ; le partage des fréquences ajoute un minimum de bruit à l'un et à l'autre type de transmission.

Aujourd'hui les réseaux locaux sans fil utilisant cette technologie sont standards ce qui signifie que la séquence de fréquences utilisées est connue de tous (et n'assure donc plus la fonction de sécurisation des échanges) : le FHSS est utilisé dans le standard 802.11 (Wi-Fi) afin de réduire les interférences entre les transmissions des diverses stations d'une cellule.

Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz chacun. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (environ 400 ms) en utilisant une combinaison de canaux connu de toutes les stations, ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée

- ⇨ Solution n°2 : DSSS, ou Direct Sequence Spread Spectrum, (étalement de spectre à séquence directe),

Définition : est une technique d'étalement de spectre utilisée dans les communications par satellite, les réseaux sans fil et plus précisément le Wi-Fi.

Avantage :

Le but du DSSS est, d'une part, de rendre les signaux occupant une bande de fréquences réduite, comme un signal de parole, plus résistants aux brouillages rencontrés lors de la transmission; d'autre part de permettre à plusieurs liaisons de partager la même fréquence porteuse (Accès multiple par répartition par code). Pour cela, ils sont combinés avec un signal pseudo-aléatoire de fréquence beaucoup plus élevée. En conséquence, le signal résultant occupe une bande de fréquence plus large, déterminée par la fréquence du signal pseudo-aléatoire. Cette technique s'applique essentiellement à des liaisons numériques; le signal d'étalement est dans ce cas une séquence de code pseudo-aléatoire.

Le fait d'étaler la puissance du signal émis sur une large bande diminue la densité de puissance émise et dans le cadre d'applications militaires, le DSSS peut alors être utilisé dans un tout autre but : dissimuler le signal en augmentant sa ressemblance avec un bruit aléatoire.

En conclusion, le saut de fréquence, l'étalement par séquence directe, l'étalement par pseudo-bruit (en utilisant des séquences de pseudo-bruit), le chirp, et les combinaisons de ces techniques sont des formes d'étalement de spectre.

L'Ultra Wide Band est une technique de modulation qui accomplit le même effet en transmettant des impulsions de très courte durée. Le standard IEEE 802.11 utilise soit le FHSS ou DSSS pour son interface radio.

Elle est par exemple utilisée par les systèmes de positionnement par satellites (GPS, GLONASS), les liaisons cryptées militaires, les communications de la Navette Spatiale avec le sol, et plus récemment dans les liaisons sans fil Wi-Fi.

9.9.2.1.2. Intrusion, écoute :

Cette attaque n'est sur le moment par dérangeante si elle n'est pas couplée avec une autre. Cependant cette attaque est parable par de la cryptographie (message échangée par clef)

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle utilise une clé publique (qui est diffusée) qui permet de coder le message et une clé privée (gardée secrète) qui permet de décoder le message. Ainsi l'expéditeur peut coder le message que seul le destinataire pourra décoder.

Principe

La cryptographie asymétrique, ou cryptographie à clé publique est fondée sur l'existence de fonctions à sens unique — une fois la fonction appliquée à un message, il est extrêmement difficile de retrouver le message original.

En réalité, on utilise en cryptographie asymétrique des fonctions à sens unique et à brèche secrète. Une telle fonction est difficile à inverser, à moins de posséder une information particulière, tenue secrète, nommée clé privée.

À partir d'une telle fonction, voici comment se déroulent les choses : Alice souhaite pouvoir recevoir des messages chiffrés de n'importe qui. Elle génère alors une valeur à partir d'une fonction à sens unique et à brèche secrète à l'aide d'un algorithme de chiffrement asymétrique (liste ici), par exemple RSA.

Alice diffuse à tout le monde la fonction pour coder les messages (notée clé publique) mais garde secrète la fonction de décodage (notée clé privée)

Chiffrement

Un des rôles de la clé publique est de permettre le chiffrement ; c'est donc cette clé qu'utilisera Bob pour envoyer des messages chiffrés à Alice. L'autre clé — l'information secrète — sert à déchiffrer. Ainsi, Alice, et elle seule, peut prendre connaissance des messages de Bob, à condition que la brèche ne soit pas trouvée.

Authentification de l'origine

D'autre part, l'utilisation par Alice de sa clé privée sur le condensat d'un message, permettra à Bob de vérifier que le message provient bien d'Alice : il appliquera la clé publique d'Alice au condensat fourni (condensat chiffré avec la clé privée d'Alice) et retrouve donc le condensat original du message. Il lui suffira de comparer le condensat ainsi obtenu et le condensat réel du message pour savoir si Alice est bien l'expéditeur. C'est donc ainsi que Bob sera rassuré sur l'origine du message reçu : il appartient bien à Alice. C'est sur ce mécanisme notamment que fonctionne la signature numérique.

Analogies 1 : Le coffre-fort

Le chiffrement : Alice a choisi un coffre-fort. Elle l'envoie ouvert à Bob, et en garde la clé. Lorsque Bob veut écrire à Alice, il y dépose son message, ferme le coffre, et le renvoie à Alice. À sa réception, seule Alice peut ouvrir le coffre, puisqu'elle seule en possède la clé, à supposer le coffre inviolable, et que personne ne puisse retrouver la clé.

L'authentification ou la signature : Alice place un message dans le coffre-fort qu'elle ferme avant de l'envoyer à Bob. Si Bob parvient à l'aide de la clé publique d'Alice dont il dispose à ouvrir le coffre-fort c'est que c'est bien celui d'Alice et donc que c'est bien elle qui y a placé le message.

Analogies 2 : La boîte à deux serrures

Une autre analogie envisageable serait d'imaginer une boîte avec deux serrures différentes. Lorsque l'on ferme la boîte d'un côté, seule la clé correspondant à l'autre serrure permet l'ouverture de la boîte et vice-versa. Une des clés est privée et conservée secrète, l'autre est dite publique et un exemplaire peut-être obtenu par quiconque souhaite utiliser la boîte.

Pour chiffrer un message Bob prend la boîte, y place son message, et la ferme à l'aide de la clé publique. Seul le détenteur de la clé privée permettant d'accéder à l'autre serrure, Alice en l'occurrence, sera en mesure de rouvrir la boîte.

Pour signer un message, Alice le place dans la boîte et ferme celle-ci à l'aide de sa clé privée. Ainsi n'importe qui ayant récupéré la clé publique pourra ouvrir la boîte. Mais comme la boîte a été fermée par la clé privée, cette personne sera assurée que c'est bien Alice, seule détentrice de cette clé, qui aura placé le message dans la boîte et fermé ladite boîte.

Applications

Transmission sécurisée de la clé symétrique

La cryptographie asymétrique répond à un besoin majeur de la cryptographie symétrique : le partage sécurisé d'une clé entre deux correspondants, afin de prévenir l'interception de cette clé par une personne tierce non autorisée, et donc la lecture des données chiffrées sans autorisation.

Les mécanismes de chiffrement symétrique étant moins coûteux en temps de calcul, ceux-ci sont préférés aux mécanismes de chiffrement asymétrique. Cependant toute utilisation de clé de chiffrement symétrique nécessite que les deux correspondants se partagent cette clé, c'est-à-dire la connaissent avant l'échange. Ceci peut être un problème si la communication de cette clé s'effectue par l'intermédiaire d'un medium non sécurisé, « en clair ». Afin de pallier cet inconvénient, on utilise un mécanisme de chiffrement asymétrique pour la seule phase d'échange de la clé symétrique, et l'on utilise cette dernière pour tout le reste de l'échange.

Mécanismes d'authentification

Un inconvénient majeur de l'utilisation des mécanismes de chiffrement asymétriques est le fait que la clé publique est distribuée à toutes les personnes : Bob, Carole, … souhaitant échanger des données de façon confidentielle. De ce fait, lorsque la personne possédant la clé privée, Alice, déchiffre les données chiffrées, elle n'a aucun moyen de vérifier avec certitude la provenance de ces données (Bob, ou Carole …) : on parle de problèmes d'authentification. Afin de résoudre ce problème, on utilise des mécanismes d'authentification permettant de

garantir la provenance des informations chiffrées. Ces mécanismes sont eux aussi fondés sur le chiffrement asymétrique.

Principe d'authentification par chiffrement asymétrique :

Objectif : Bob souhaite envoyer des données chiffrées à Alice en lui garantissant qu'il en est l'expéditeur.

1. Bob crée une paire de clés asymétriques : il conserve la clé privée et envoie la clé publique à Alice

2. Alice crée une paire de clés asymétriques : clé privée (qu'elle conserve), clé publique (qu'elle diffuse librement, notamment à Bob)

3. Bob effectue un condensat de son message « en clair » puis chiffre ce condensat avec sa propre clé privée

4. Bob chiffre son message avec la clé publique d'Alice.

5. Bob envoie le message chiffré accompagné du condensat chiffré.

6. Alice reçoit le message chiffré de Bob, accompagné du condensat.

7. Alice déchiffre le message avec sa propre clé privée. À ce stade le message est lisible mais elle ne peut pas être sûre que Bob en est l'expéditeur.

8. Alice déchiffre le condensat avec la clé publique de Bob.

9. Alice utilise la même fonction de hachage sur le texte en clair et compare avec le condensat déchiffré de Bob. Si les deux condensats correspondent, alors Alice peut avoir la certitude que Bob est l'expéditeur. Dans le cas contraire, on peut présumer qu'une personne malveillante a tenté d'envoyer un message à Alice en se faisant passer pour Bob !

Cette méthode d'authentification utilise la spécificité des paires de clés asymétriques : si l'on chiffre un message en utilisant la clé publique, alors on peut déchiffrer le message en utilisant la clé privée ; l'inverse est aussi possible : si l'on chiffre en utilisant la clé privée alors on peut déchiffrer en utilisant la clé publique.

Certificats

La cryptographie asymétrique est également utilisée avec les certificats numériques, celui-ci contenant la clé publique de l'entité associée au certificat. La clé privée est quant à elle stockée au niveau de cette dernière entité. Une application des certificats est par exemple la mise en œuvre d'une infrastructure à clés publiques (PKI) pour gérer l'authentification et la signature numérique d'une entité, par exemple un serveur web (Apache avec le module SSL par exemple), ou simplement un client souhaitant signer et chiffrer des informations à l'aide de son certificat de la façon décrite dans les sections précédentes.

Une clé privée inviolable ?

Un chiffrement symétrique au moyen d'une clé de 128 bit propose 2128 (un nombre à trente-huit chiffres) façons de chiffrer un message. Un pirate qui essaierait de déchiffrer le message par la force brute devrait les essayer une par une.

Pour les systèmes à clé publique, il en va autrement. Tout d'abord les clés sont plus longues (par exemple 1 024 bit minimum pour RSA) ; ceci est dû au fait qu'elles possèdent une structure mathématique très particulière (on ne peut pas choisir une suite de bits aléatoire comme clé secrète, car, dans le cas du RSA, seuls les nombres premiers sont utilisés). Ensuite, il y a clairement mieux à faire qu'une recherche exhaustive sur, par exemple, 1 024 bit, à savoir exploiter la structure mathématique de la clé (pour RSA, cela mène à la factorisation).

Il faut noter le développement actuel de la cryptographie utilisant les courbes elliptiques, qui permettent (au prix d'une théorie et d'implémentations plus complexes) l'utilisation de clés nettement plus petites que celles des algorithmes classiques (une taille de 160 bit étant considérée comme très sûre actuellement), pour un niveau de sécurité équivalent.

Rf fingerprint :

Le processus d'identification d'émetteurs radio qui consiste a examiné leurs caractéristiques uniques en début de transmission est appelé la prise des empreintes digitales Rf. La sécurité de réseaux sans fil peut être améliorée en poussant l'utilisateur à prouver son identité. Si l'empreinte digitale d'un dispositif de réseau est non identifiée il pourra être considéré comme une menace. Pour SAHARA il faudra que chaque nœud du réseau puisse être identifié au moyen de son empreinte digitale Rf. Un système d'identification complet sera à envisager, y compris l'acquisition de données, la détection passagère et l'extraction d'empreinte digitale de Rf. Des études ont démontré que la technique des empreintes digitales Rf peut être utilisée comme un outil supplémentaire pour améliorer la sécurité de réseaux sans fil.

Dans la cryptographie à clef publique, une empreinte digitale de clef publique est une courte séquence d'octets utilisés afin d'authentifier une clé publique plus longue. Les empreintes digitales sont créées en appliquant une fonction de hachage cryptographique à une clé publique. Puisque les empreintes digitales sont plus courtes que les clés auxquelles elles se réfèrent, elles peuvent être utilisées pour simplifier certaines tâches de gestion de clefs.

Une technique en cours d'évaluation a été conçue et mis en œuvre pour identifier la carte d'interface de réseau source (en anglais NIC network interface card) d'un IEEE 802.11 cadré par l'analyse de fréquence radio passive. Cette technique, appelée PARADIS, démultiplie les imperfections infimes de matériel émetteur qui sont acquises à la fabrication et sont présentes même dans les NICS autrement identique. Ces imperfections sont spécifiques à chaque émetteur et se manifestent comme les artefacts des signaux émis. PARADIS, mesure les artefacts se différenciant du sans fil individuels dans le domaine de modulation, et applique des outils de classification machine-learning appropriés pour atteindre un degrés d'exactitude d'identification NIC significativement plus hauts que les techniques antérieurs les mieux connus. L'efficacité de PARADIS a été démontrée expérimentalement la différenciation entre

plus de 130 NICS 802.11 identiques avec une exactitude de plus de 99 %. Les résultats montrent aussi que l'exactitude de PARADIS est résistante contre au bruit ambiant et aux fluctuations du canal sans fil.

9.9.2.1.3. Intrusion et diffusion de fausses informations :

Le meilleur moyen pour remédier à ce problème reste la redondance du signal mais la cryptographie asymétrique (chiffrement) y contribue aussi fortement surtout si les procédures de génération des clefs sont correctement suivies (personne n'y a accès et les clefs sont régulièrement changées comme cela est prévu pour les systèmes critiques)

9.9.2.2. Aspect hard ware :

En ce qui concerne l'aspect hard ware le détracteur ne peut agir à distance il faut qu'il ait un contact direct avec le matériel et comme pour tous systèmes électroniques accessibles, la méthode de protection principale reste la procédure de maintenance. Augmenter le nombre de vérification (et de vérificateur) permet de protéger le système.

Des capteurs peuvent aussi alarmer l'unité de contrôle en cas de panne du système et dans des cas extrême ou le matériel ne doit absolument pas se retrouver entre les mains d'un détracteur, poser un système d'autodestruction si le système est retiré de sa position initiale