

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE



UNIVERSITE DE M'SILA
Faculté de Mathématiques et Informatique
Département d'Informatique



MEMOIRE

Présenté pour l'obtention du diplôme de :

MASTER

Spécialité : **Informatique**

Option : **Réseaux**

Par : **MR. TAIBI Azeddine**

Thème

**Protocoles délimiteurs de distance des systèmes RFID:
étude comparative**

Soutenu publiquement le : ---- / 06 / 2014 devant le jury composé de :

Mr.Président
Mr. Chikouche Noureddine..... Rapporteur
Mr.Examineur

À ma famille ...

REMERCIEMENTS

Je remercie en premier lieu notre Dieu qui m'a facilité la tâche, et m'a donné force et volonté pour bien achever ce travail.

Je tiens à remercier tout d'abord mon encadreur Mr. CHIKOUCHE Noureddine de m'avoir proposé un tel intéressant sujet .

Les membres de jury qui m'ont fait un grand honneur en acceptant la valorisation de ce modeste travail.

J'adresse toute ma gratitude aux membres de ma famille, mes parents, mes sœurs, mon frère .

Je n'omettrai pas de remercier mes collègues de la promotion chacun par son nom.

Que toute personne m'a aidé trouve ici mes vifs remerciements.

Azeddine

TABLE DES Matière

CHAPITRE I.....	1
La Technologie RFID.....	1
I.1 Présentation de la technologie RFID.....	3
I.1.1 Introduction :	3
I.1.2 Définition	3
I.1.3 Historique.....	3
I.2 Composition d'un système RFID.....	5
I.2.1 L'élément déporté	5
I.2.2 L'élément fixe.....	6
I.2.3 L'hôte	7
I.2.4 Bref descriptif du mode de fonctionnement	7
I.3 Applications, fréquences d'utilisation et standardisation.....	8
I.3.1 Applications.....	8
I.3.1.1 Traçabilité logistique et traçabilité produit	8
I.3.1.2 Production industrielle de biens, surveillance et maintenance.....	9
I.3.1.3 Sécurité des produits qualité des biens	10
I.3.1.4 Contrôle d'accès et traçabilité des hommes et des animaux	10
I.3.1.5 Cartes de fidélité, de membre, ou de paiement.....	11
I.3.1.6 Santé	11
I.3.1.7 Services publiques.....	12
I.4 Inquiétudes de la technologie	12
I.4.1 Au niveau « sécurité ».....	12
I.4.2 Au niveau «Santé»	13
I.4.3 Au niveau « Psychique»	13
I.5 Conclusion	13
CHAPITRE II	14
Introduction à la cryptologie	14
II.1 Introduction.....	15
II.2 La cryptologie en quelques mots.....	15
II.2.1 Science du secret	15
II.2.2 Cryptographie, cryptanalyse	15
II.2.3 Cryptographie symétrique, cryptographie asymétrique et la fonction de hachage.....	15
II.2.3 .1 Chiffrement symétrique :	16

II.2.3 .2 Chiffrement asymétrique :	16
II.2.3 .3 Fonction de hachage :	17
II.3 Buts de la cryptologie	18
II.3.1 Confidentialité.....	18
II.3.2 Intégrité.....	18
II.3.3 Identification.....	18
II.3.4 Authentification	18
II.4 Protocoles cryptographiques :	19
II.4.1 Notations.....	19
II.4.2 Les types des protocoles :	19
II.4.2.1 Protocole des buts spécifiques :	20
II.4.2.2 Protocoles de groupes :	21
II.4.2.3 Protocole à divulgation nulle :	22
II.5 Conclusion	22
CHAPITRE III	23
Protocoles délimiteurs de distance des systèmes RFID.....	23
III.1 Introduction.....	24
III.2 Attaques par relayer :	24
III.2.1 Présentation :	24
III.2.1 Principe :	24
III.2.2 Illustration sur quelques technologies.....	25
III.2.2.1 RFID	25
III.2.2.2 Véhicules sans clé	26
III.3 Protocoles de distance bornée.....	26
III.3.1 Motivations	26
III.3.2 Fonctionnement.....	27
III.3.3 Protocole de distance bornée selon Stefan Brands et David Chaum	27
III.3.3.1 Description du protocole	27
III.3.3.2 Problème de sécurité :	28
III.3.3.3 Description du second protocole.....	29
III.3.3.4 Analyse de la sécurité	29
III.3.4 Protocole de distance bornée selon Gerhard P. Hancke et Markus G. Kuhn	30
III.3.4.1 Description du protocole	31
III.3.4.2 Analyse de la sécurité	32

III.3.5 Le protocole de distance bornée pour RFID Swiss-knife	32
III.3.5.1 Description du protocole	33
III.3.5.1 Analyse de la sécurité	34
III.4 Conclusion	36
CHAPITRE IV	37
Implémentation de simulateur	37
IV.1 Introduction :	38
IV.2 Simulation :	38
IV.2.1 Méthode de simulation :	38
IV.3 Outils mis en œuvre	38
IV.3.1 Langage de programmation.....	38
IV.3.2 Environnement de développement.....	39
IV.4 Présentation de l'application	40
IV.4.1 Pseudo code principal.....	40
IV.4.2 Interface principale	41
IV.4.2 Interface de protocole Stefan Brands et David Chaum	41
Conclusion.....	49
BIBLIOGRAPHIE	50
RESUME	53

TABLE DES FIGURES

Figure I- 1: Harry Stochman le fondateur de la Radio Identification	5
Figure I- 2: Exemples d'éléments déportés dotés de Tags RFID	6
Figure I- 3: Exemples d'éléments fixes.....	7
Figure I- 4: Exemples d'hôtes.....	7
Figure I- 5: Simple illustration du principe de fonctionnement.....	8
Figure I- 6 : Illustration de traçabilité des processus	9
Figure I- 7 : illustration de traçages des biens	9
Figure I- 8 : RFID dans la domaine de santé.....	11
Figure I- 9 : domaines d'applications de la technologie RFID	12

Figure III- 1: Attaque par relais sur un système RFID.....	25
Figure III- 2 : Schéma de principe attaque par relais sur véhicules équipés de carte sans fil.....	26
Figure III- 3 :Distance-Bounding protocol selon Stefan Brands et David Chaum	28
Figure III- 4 : Distance-Bounding protocol (second protocol) selon Stefan Brands et David Chaum	30
Figure III- 5 :Distance-Bounding protocol (second protocol) selon Gerhard P. Hancke et Markus G. Kuhn...	31

Figure IV- 1 : Interface principale d'application.....	41
Figure IV- 2 : Interface principale d'application.....	42
Figure IV- 3 : choix de scénario.....	42
Figure IV- 4 : phases de génération des bits	43
Figure IV- 5 : phases d'échange des bits.....	43
Figure IV- 6 : phases d'échange des bits.....	43

Table des tableaux

Table II- 1 : Notations.....	19
------------------------------	----

Introduction générale

La technologie connaît de nos jours son plein essor, touchant tous les secteurs. Les télécommunications viennent en premier lieu, car elles ne cessent de donner naissance à plusieurs standards comme les réseaux sans fil qui sont très répandus du fait qu'ils offrent aux utilisateurs le confort, la liberté et la mobilité.

Ces nouvelles technologies sont devenues omniprésentes dans notre société moderne, elles la développent davantage en ayant des différents effets sur les plans économiques et sociaux. Elles contribuent à la croissance économique, à l'échange des informations, et à leur diffusion. Les technologies d'identification en font partie. Ces dernières possèdent une large palette d'applications qui se répand sur une infinité de domaines allant de la distribution à la sécurité à la logistique à la traçabilité.

Les technologies d'identification ont débuté avec les codes-barres et par des identifications par contact comme les cartes bancaires, les cartes d'appels téléphoniques. Des développements récents des systèmes sans fil et de la micro-électronique ont contribué à la création de nouvelles technologies d'identification sans contact dite technologies de radio-identification (ou RFID pour Radio-Frequency Identification). Ces nouvelles technologies, de par leur grande souplesse, rendent l'échange d'information nettement plus rapide et plus efficace.

Bien que les premiers systèmes RFID qui ont vu le jour fonctionnent essentiellement dans des bandes de fréquences basses, ils ont ouvert la voie au développement d'une nouvelle technologie RFID, plus performante et à faible coût, fonctionnant à des fréquences plus élevées : la technologie RFID UHF (Ultra High Frequency) passive. Cette dernière possède un mode de fonctionnement bien particulier.

Un système RFID est composé de deux entités majeures, l'étiquette et le lecteur. L'identification est réalisée grâce à des étiquettes RFID passives, appelées également «tags», qui sont associées aux produits à identifier. Ces tags sont constitués d'une puce électronique et d'une antenne. Contrairement aux systèmes de communication classiques, ils sont alimentés à distance et ne possèdent aucune source propre d'émission radiofréquence. Ils sont plutôt alimentés à partir d'une onde électromagnétique qui leur provient du lecteur lors de la présence du tag dans la zone de lecture de ce dernier.

La communication entre le tag RFID et le lecteur est insécurisée, ce qui le rend ouvert devant toute attaque logique sur les protocoles cryptographiques.

L'objectif des algorithmes de chiffrement et les protocoles cryptographiques (appelé aussi protocoles de sécurité) est d'assurer les propriétés de sécurité : la confidentialité des données, l'authentification des entités, l'intégrité des données, et la non-répudiation des données.

Parmi les protocoles de sécurité de la technologie RFID est Les distance-bounding protocols qui pourraient être traduit par protocoles délimiteurs de distance, sont des protocoles de sécurité qui permettent à un vérificateur V de s'assurer qu'un prouveur P se trouve à une distance bornée et définie de lui-même. Leur but est d'améliorer les mécanismes d'authentification traditionnels, de fournir une garantie supplémentaire tel un indicateur de distance pour le routage sécurisé des réseaux ad-hoc. Ces protocoles permettent entre autres de se prémunir des attaques du type Man-In-The-Middle et de ses dérivés, en calculant la distance entre V et P .

Souvent des tel protocoles ne sont qu'en cours de spécification et leurs réelles performances ne sont que théoriques. C'est ainsi pour évaluer les performances d'un protocole, la manière la moins couteuse est l'implémentation dans un simulateur. la simulation est un outil d'aide a la décision très utilise par la concepteurs et les gestionnaires des systèmes complexes, Elle consiste a construire un modèle d'un système réel (physique, économique, humain,...etc.) et construire des expérience sur ce modèle afin de bien comprendre le comportement de se système et d'en améliorer les performances.

Dans ce travail, nous allons étudier des protocoles de distance bornée des systèmes RFID. Les protocoles basés sur deux primitives cryptographiques, la fonction de hachage et le générateur des nombres pseudo-aléatoire.

L'objective de cette étude est de simuler ces protocoles « RFID_SIM_DBP » pour assurer le fonctionnement des protocoles et pour représenter réellement des protocoles et des traces d'attaque s'il existe.

Ce mémoire est focalisé autour quatre chapitres. Dans le premier, nous présentons d'une façon générale les différentes technologies de radio-identification existantes RFID. Nous établissons un état de l'art sur les systèmes RFID, ses composant, ses applications etc. Dans le deuxième chapitre, on expose les notions de base de cryptographie et les propriétés de sécurité qui peuvent être assurées dans ce système. Nous présentons les primitives cryptographique exigés dans les protocoles tels que : fonction de hachage cryptographique, générateur des nombres pseudo-aléatoire et l'opérateur Ou-exclusif. Le troisième chapitre nous verrons les protocoles de distance bornée, qui servent à contrer l'attaque par relais. Ainsi, 3 protocoles seront décrits, le premier est celui de Stefan Brands et David Chaum. Le second est celui de Gerhard P. Hancke et de Markus G. Kuhn qui sert de base à la plupart des protocoles proposés depuis. Enfin, nous verrons le Swiss knife, un protocole de distance bornée capable de résoudre une grande partie des problèmes de sécurité de la RFID, le quatrième est consacré à l'implémentation de notre simulateur, ce chapitre présent les différent outils utilisées (JAVA, NetBeans IDE) et les différentes interfaces de l'outil mis en place. Finalement, nous clôturons ce mémoire par une conclusion et des perspectives.

CHAPITRE I

La Technologie RFID

La technologie RFID (Radio Frequency IDentification) est une technologie radio qui promet d'être omniprésente dans la vie de l'individu dans un futur proche, nous avons trouvé intéressant de consacrer ce premier chapitre à une présentation générale de cette technologie.

I.1 Présentation de la technologie RFID

I.1.1 Introduction :

L'identification électronique se divise en deux branches: *l'identification électronique* « avec contact » et l'identification « sans contact » (*Contactless*) dont fait partie la technologie RFID (Radio Frequency IDentification) [1].

L'identification avec contact s'effectue à l'aide de systèmes où la transmission de données est faite avec des contacts électriques. Les cartes à puces actuellement utilisées en Algérie en sont un exemple.

L'identification sans contact présente plusieurs ramifications [1] :

- Les systèmes à vision optique qui nécessitent une visibilité directe et qui ont une distance de lecture de moins d'un mètre quel que soit le type de lecteur utilisé: oeil, caméra, laser, scanner (avec éventuellement un logiciel de reconnaissance de caractères), etc. Les codes-barres en sont de bons exemples.
- Les systèmes à liaison infrarouge qui utilisent les longueurs d'onde aux environs de 800 nm, sont utilisés sur une distance allant du centimètre jusqu'à quelques mètres. Pour satisfaire ces distances avec un grand débit d'informations, le faisceau émis doit avoir une très forte directivité. Nous pouvons citer en exemple : les liaisons IRDA (Infra Red Data Association), et certains systèmes de télépéage.
- Les systèmes à liaisons en fréquence radio qui sont divisés en plusieurs branches dépendant des applications (distance d'utilisation) et des caractéristiques techniques (fréquences, etc.) désirées. Par exemple : l'identification des individus.

I.1.2 Définition

La RFID (Radio Frequency IDentification) est une technologie d'identification automatique qui utilise le rayonnement radiofréquence. Elle sert à identifier des objets porteurs d'étiquettes lorsqu'ils passent à proximité d'un lecteur. Une communication s'établit, et les données contenues dans l'étiquette sont transférées vers le lecteur. Elles peuvent également être modifiées suite à une commande particulière.

I.1.3 Historique

La radio-identification est une technologie d'identification relativement moderne qui a été développée récemment. Cependant, la première application RFID fut utilisée pendant la seconde guerre mondiale lorsque Watson et Watt avaient développé une application dans le domaine militaire permettant de vérifier l'appartenance « amie » ou « ennemie » des avions arrivant dans l'espace aérien Britannique et cela en 1935. Ce système dit IFF (Identify: Friend or Foe) reste le principe de base utilisé de nos jours pour le contrôle du trafic aérien [2].

A partir des années 40, l'idée de l'identification radio fréquence commence à germer avec les travaux de Harry Stockman , suivi des travaux de F. L. Vernon en 1952 et ceux de D.B. Harris . Leurs articles sont considérés comme les fondements de la technologie RFID et décrivent les principes qui sont toujours utilisés aujourd'hui [3].

En 1966, la société SENSORMATIC a été créée, fournisseur d'une application de surveillance ou d'objets de biens appelée EAS (Electronic Article Surveillance) dont le principe est bien connu. Quand un objet quitte un certain périmètre, ceci est détecté et une alarme est déclenchée. Cependant, durant cette période s'étalant des années soixante jusqu'au des années soixante-dix, l'usage des RFID reste essentiellement militaire et surtout orienté vers le contrôle d'accès [3].

Le dépôt du brevet américain de Mario Cardullo d'un transpondeur télé-alimenté passif à mémoire, en 1973, a été le premier véritable ancêtre de la RFID moderne . Son brevet couvre l'utilisation de fréquences radioélectriques, utilisant le son et la lumière comme supports de transmission. Le plan d'affaires (Business Plan) original, présenté aux investisseurs en 1969, couvrait des applications : dans les transport (identification de véhicule automobile, système de péage automatique, plaque d'immatriculation électronique, suivi de véhicule, surveillance des performances des véhicules), dans le secteur bancaire (carte de crédit électronique), dans la sécurité (identification du personnel, portails automatiques, surveillance) et dans le domaine médical (identification, dossier du patient).

En 1975, la démonstration de la rétrodiffusion des étiquettes (tags) RFID, à la fois passives et semi-passives a été réalisée par Steven Depp, Alfred Koelle et Robert Freyman au laboratoire scientifique de Los Alamos. Le système portable fonctionne à la fréquence 915 MHz. Cette technique est utilisée par la majorité des transpondeurs (tags) RFID fonctionnant en UHF (Ultra Hautes Fréquences) et micro-ondes.

A la fin des années 70, l'utilisation de la RFID pour l'identification de bétail commence en Europe et aux Etats-Unis.

Les années 80 ont été marquées par l'invention des microsystèmes et l'avancée de la technologie qui ont conduit à l'utilisation de tags passifs. L'absence de source d'énergie embarquée rend le tag moins coûteux mais l'oblige à obtenir de l'énergie qui lui sera transmise par le lecteur. Les distances de lecture obtenues sont alors de quelques centimètres.

Il a fallu attendre l'année 1990 pour commencer la standardisation des puces RFIDs. L'organisme ISO (International Organization for Standardization) se penche d'abord sur les puces puis sur les lecteurs et commence son travail de normalisation. Aujourd'hui encore la technologie RFID n'est pas encore complètement encadrée par une réglementation à l'échelle mondiale.

L'année 1999 a connu la Création du centre « Auto-ID Center », formé par le MIT (Massachusetts Institute of Technology) et des partenaires industriels ; une organisation sans but lucratif ayant pour mission la standardisation et la construction d'une infrastructure pour un réseau mondial de la RFID.

En 2003, les associations EAN (Efficient Article Numbering Association) International, Auto-ID Center, UCC (Uniform Code Council) [4] et des industriels créent le standard EPC (Electronic Product Code) global Version 1.0 ; intégrant les technologies RFID et Internet pour mettre en place le réseau de traçabilité des objets.

En 2004, L'administration américaine de nourriture FDA (Food and Drugs Administration) autorise l'implantation sous cutanée de transpondeur RFID pour des fins médicales.

En 2010-2013, il a été prévu dans le Projet de Loi sur la santé, que tous les Américains se verront implanter une micro-puce dans le but de créer un registre national d'identification, pour permettre un meilleur suivi des patients en ayant toutes les informations relatives à leur santé.

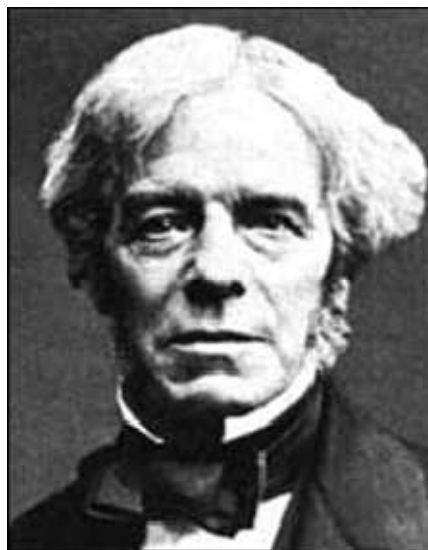


Figure I- 1: Harry Stochman le fondateur de la Radio Identification

I.2 Composition d'un système RFID

Typiquement un système RFID est constitué d'un élément déporté, d'un élément fixe et éventuellement d'un hôte :

I.2.1 L'élément déporté

Couramment dit en langue française identifiant, étiquette, ou Transpondeur (pour transmetteur – répondeur) ; appelé aussi en anglais Tag ou Label.

La Figure I-2 montre quelques tags d'éléments déportés disponibles sur le marché.



Figure I- 2: Exemples d'éléments déportés dotés de Tags RFID

I.2.2 L'élément fixe

Appelé interrogateur, lecteur (Reader), ou Modem (Modulateur /Démodulateur), ceci dit le terme le plus approprié semble être Station de base [1].

NB : le terme fixe est utilisé par abus de langage parce qu'il peut être déporté.

Comme le montre la Figure I-3, des lecteurs peuvent être de différents types.



Figure I- 3: Exemples d'éléments fixes

I.2.3 L'hôte

Souvent, en amont à la station de base on peut trouver un système dit hôte (host) qui peut être un simple ordinateur, un serveur ou un ordinateur lié à un serveur, un progiciel, une base de données, etc... [1], ainsi qu'on peut le voir dans la Figure I-4 .



Figure I- 4: Exemples d'hôtes

I.2.4 Bref descriptif du mode de fonctionnement

La technologie RFID est basée sur l'émission de champ électromagnétique par le lecteur qui est reçu par l'antenne d'une ou de plusieurs étiquettes. Le lecteur émet un signal selon une fréquence déterminée vers une ou plusieurs étiquettes situées dans son champ de lecture (Figure I-5).

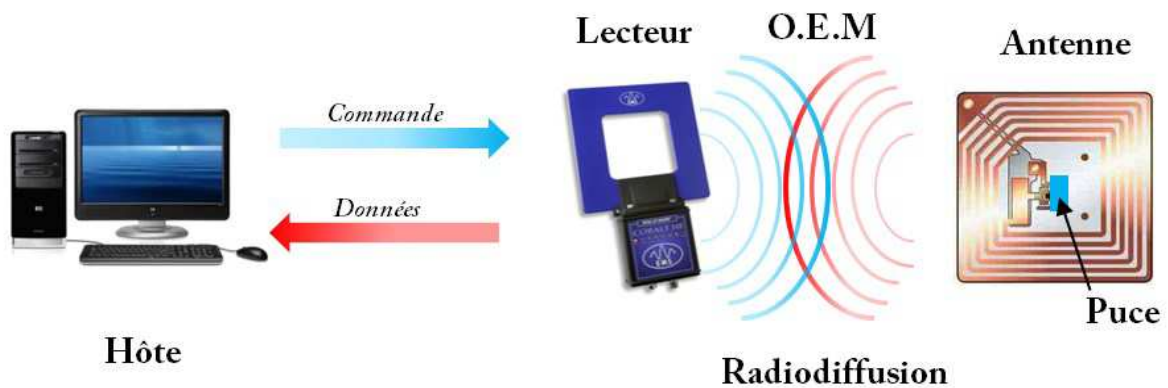


Figure I- 5: Simple illustration du principe de fonctionnement

Ce champ électromagnétique se considère comme étant un support d'énergie d'activation de ces étiquettes.

Une fois les étiquettes activées par le lecteur, elles transmettent alors en retour un signal et donc un dialogue s'établit entre les deux entités, selon un protocole de communication prédéfini, et des données pourront être échangées.

I.3 Applications, fréquences d'utilisation et standardisation

I.3.1 Applications

Les applications des systèmes RFID ne sont pas dénombrables, l'éventail s'élargit de jour en jour par la naissance de nouvelles idées développant de nouveaux systèmes.

Parmi la large palette d'applications existantes, nous allons nous contenter de présenter quelques-unes déjà mises en place [5] :

I.3.1.1 Traçabilité logistique et traçabilité produit

- La traçabilité logistique (Tracking) est une forme de traçabilité qui désigne le suivi quantitatif des produits. Elle porte surtout sur le positionnement géographique des unités logistiques (Figure I-6). Quelques exemples :

- Service/unité logistique interne : Les transpondeurs à l'usage d'une seule personne font partie de ceux ayant une mémoire et généralement au moins un capteur, comme ceux embarqués dans les camions qui enregistrent la masse à vide, la masse chargée et la distance parcourue pour chaque transport.
- Logistique en circuit fermé : pour le suivi des bouteilles de gaz, des conteneurs, des livres dans les bibliothèques, des DVD en location ou tout autre article où il y a recyclage interne des tags.

- La traçabilité produit (Tracing) est une forme de traçabilité qui désigne le suivi qualitatif des produits (Figure I-7). Elle dépend surtout du bon enregistrement et de l'exhaustivité des données liées au produit. Comme exemple nous citons :

- La recherche des causes d'un problème qualité. La traçabilité produit porte surtout sur les caractéristiques des unités consommateurs.
- Le développement d'assouvissement du besoin de traçabilité des industriels, la chaîne d'approvisionnement (Supply Chain) est très gourmande en quantité de transpondeurs.



Figure I- 6 : Illustration de traçabilité des processus



Figure I- 7 : illustration de traçages des biens

I.3.1.2 Production industrielle de biens, surveillance et maintenance

Il s'agit d'une application qui veille sur le bon archivage des documents, sur la protection de l'environnement, par exemple :

- Les systèmes d'archivage : la société MAGELLAN a commercialisé un système d'archivage de documents. Chaque document ou feuille est doté d'étiquette. Simultanément, le lecteur permet d'inventorier 100 000 documents sur une armoire, ou de récupérer des fichiers stockés dans une boîte d'archives, le tout en quelques secondes [6].

- La gestion du patrimoine et surveillance de l'environnement : La société AGRIHOUSE a commercialisé un système de détection des besoins d'irrigation avec des tags actifs RFID couplés à des capteurs hygrométriques, lesquels permettent le déclenchement d'une alerte dès que le seuil d'hydratation de cultures (de pommes de terre ou de maïs) baisse significativement. Ce système donne ainsi les besoins spécifiques d'une culture, qui varient considérablement d'un terrain à l'autre, voire au sein d'un même champ [7].

I.3.1.3 Sécurité des produits qualité des biens

Il s'agit de certains aspects liés à la sécurité, pour les produits qu'on trouve dans les hypermarchés par exemple. Ces produits peuvent être tracés de la réception à la sortie suite à un achat, pour faciliter la logistique, grâce aux étiquettes RFID collées ou imprimées sur les produits en question [8]. Il peut également s'agir de produits électroniques (électroménagers), ou textiles (bobines de fil) ou de véhicules (des systèmes anti démarrage, mesures de poids en charge, anti-intrusion), ou plutôt dans les aéroports (mettre des étiquettes RFID sur les bagages permettant ainsi de réduire le taux d'erreur d'acheminement).

On arrive également à lutter contre la contrefaçon de certains produits comme les médicaments par exemple, grâce à l'utilisation de la technologie RFID, en insérant un numéro unique UID (Unique Identification Number) sur les boîtes.

Quant à l'aspect qualité, cette technologie pourrait être exploitée pour effectuer un inventaire automatique qui permettrait d'alerter sur l'approche de la date limite de consommation d'un produit.

I.3.1.4 Contrôle d'accès et traçabilité des hommes et des animaux

Ceci englobe certaines applications comme :

- Étiquetage et billetterie : cette application est déjà largement répandue dans les transports par le biais de cartes d'abonnement à RFID. Il sera très intéressant de l'étendre et de la mettre en œuvre dans les billets des événements qu'ils soient sportifs ou culturels tels que les billets de matchs de football, les concerts, des jeux olympiques, etc. [8]. L'élimination des contrefaçons est privilégiée dans ce cas.
- Systèmes de contrôle d'accès : il s'agit de l'une des applications les plus usuelles, elle permet en plus d'accéder aux données biométriques de l'individu incluses dans les étiquettes.
- Traçabilité animale : l'identification des bétails est l'une des plus anciennes applications qui remonte aux années 80. La nouveauté est que avec les étiquettes actuelles dotées de mémoire, il est possible d'enregistrer des informations médicales (vaccination) ou même alimentaires en plaçant des lecteurs à côté des mangeoires.
- La traçabilité individuelle : Cela peut s'agir d'une traçabilité géographique ou traçabilité des achats, des activités, etc.

I.3.1.5 Cartes de fidélité, de membre, ou de paiement

Ces applications facilitent aux utilisateurs l'accès aux différents services, par exemples : [8]

- Cartes de fidélité à technologie RFID : leur mise en application élimine le remplissage des formulaires interminables pour la garantie par exemple. Actuellement, elles sont compatibles avec la technologie NFC (Near Field Communication), et donc liées au téléphone portable.
- Les cartes bancaires sans contact : comme la carte de fidélité, la carte bancaire sans contact devient également compatible avec la technologie NFC.

I.3.1.6 Santé

Dans le domaine de la santé, la technologie RFID persiste dans certaines applications comme :

- Assistance aux handicapés : on a inventé un dispositif appelé « Tell Mate » qui sert les non-voyants ou malvoyants à identifier leurs objets les plus usuelles ; et ceci en affectant à chaque objet une étiquette, il faut ensuite enregistrer un commentaire audio correspondant à cet objet. Dès que l'utilisateur le souhaite, il présente l'objet à son lecteur pour obtenir son commentaire associé [9].
- Gestion des hôpitaux : les appareillages disponibles dans les hôpitaux peuvent contenir des étiquettes permettant de tracer leurs nettoyage, désinfection, stérilisation et disponibilité. Autre application très intéressante est d'assurer la traçabilité du don du sang grâce à un système qui contient un capteur de température permettant un contrôle permanent le long de la chaîne de réservation.
- Surveillance médicale : des bracelets peuvent être attribués aux patients remplaçant les feuilles de soins. Ils contiennent le numéro du médecin traitant ainsi que celui de l'infirmière, et sont reliés à une base de données qui stocke les dossiers des malades. Le système peut être accessible via des PDAs (Personnal Digital Assistant) ou autres (tablettes PC, etc).

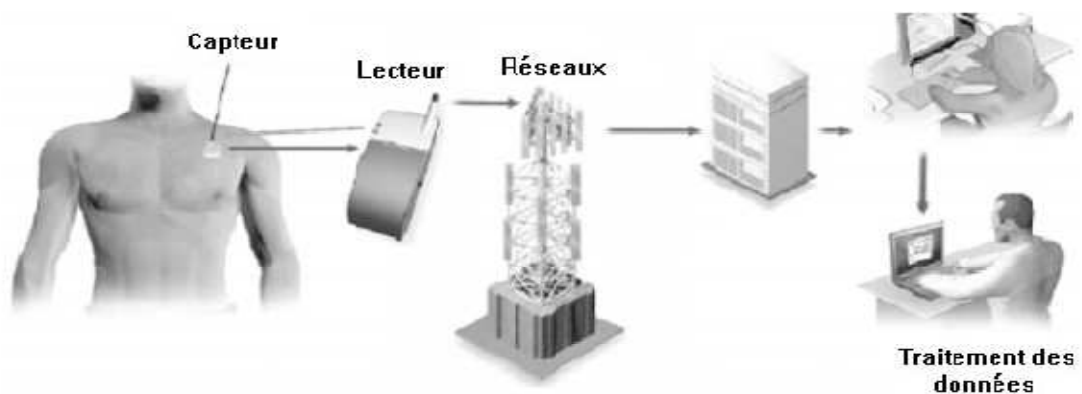


Figure I- 8 : RFID dans la domaine de santé

I.3.1.7 Services publics

Les services publics ont été également affectés par la RFID, par exemples :

- Maintenance des services publics : certains compteurs d'eau, d'électricité ou de gaz ou autre portent actuellement des étiquettes pour pouvoir être relevés depuis la rue.
- Cartes d'identité et passeports : le passeport intègre une image du visage ainsi que les empreintes digitales de huit doigts stockées dans une puce RFID.
- Cartes de sécurité sociale : dotées de puces contenant les informations de chaque personne.

Toutes ces applications et ces exemples nous montrent l'omniprésence de cette technologie dans la vie actuelle de l'individu (Figure I-8).

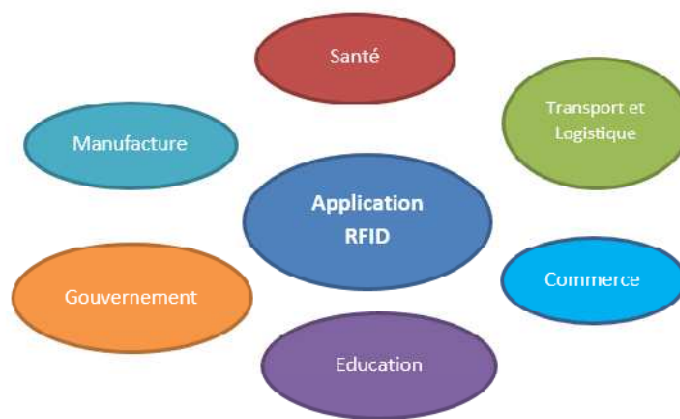


Figure I- 9 : domaines d'applications de la technologie RFID

I.4 Inquiétudes de la technologie

Comme toute nouvelle technologie qui s'intègre dans une société ; la RFID crée des majeurs concernant la sécurité des dispositifs et des individus en terme sanitaire et médicale et en terme psychologique.

I.4.1 Au niveau « sécurité »

A l'heure actuelle, aucun système sécuritaire ne s'est avéré inviolable ; tous ont subis des interceptions de données ou du brouillage ou interférences ou autres.

L'espionnage des systèmes radiofréquences est favorisé, l'interception des communications étant simple à mettre en œuvre. Des expériences ont montré que l'accès aux données d'une carte bancaire reste possible [10].

A son tour, l'utilisateur devra être sensibilisé à la sécurité du système en le supposant inviolable, parce que ce type de défaillance humaine devra être toujours prise en compte, quel que soit le progrès de la technologie.

I.4.2 Au niveau «Santé»

Les normes sanitaires relatives aux rayonnements électromagnétiques sont encore imprécises.

Jusqu'à présent, plusieurs recherches auprès des émissions UHF SHF sont menées en vain, entre temps, les dernières études épidémiologiques confirment le rapport entre la proximité d'antennes relais et le cancer [\[11\]](#).

L'apparition des systèmes couplés comme les NFC ou l'implant de systèmes RFID aux humains suscitent une attention des chercheurs, surtout que la manière d'émission des ondes se fait incessamment comme pour la géo localisation (RTLS), les téléphones portables, etc.

Des décisions seront prises dans le futur, suite à la mise en cause de cette technologie : abandon de la technologie, renforcement des normes sanitaires, ou peut-être d'autres solutions?

I.4.3 Au niveau « Psychique»

La technologie RFID a certainement mis en cause la vie privée de l'individu. L'organisme EPC et les implémentations des puces sous cutanée dès la naissance des humains constituent un véritable risque de destruction de la vie privée de la personne.

I.5 Conclusion

Dans ce chapitre, nous avons abordé en premier lieu les ramifications de l'identification électronique. Cette dernière se divise en deux branches, celle qui a suscité notre intérêt est l'identification sans contact dite RFID. Nous avons présenté par la suite le principe de cette technologie et sa progression au fil des années. Nous avons décrit brièvement les éléments constituant un système complet RFID, ainsi que leurs principes de fonctionnement. La majeure partie de ce chapitre a été consacrée aux nombreuses applications RFID s'étalant sur des 40 domaines très variés. Enfin, nous avons souligné les inquiétudes auxquelles sont confrontés les utilisateurs de tels systèmes.

CHAPITRE II

Introduction à la cryptologie

Ce chapitre constitue une très courte introduction à la cryptologie. Il n'est pas un cours sur le sujet, mais doit plutôt être vu comme un rapide survol de la cryptologie, et comme le moyen de poser certaines notations utilisées dans le reste de cette mémoire

II.1 Introduction

La sécurité de protocole de cryptographique s'entend en fonction de différentes propriétés (secret de données privées, l'authentification,..., etc.) que le protocole est censé garantir.

Le problème qui se pose dans les protocoles cryptographique est la difficulté de concevoir du protocole. Ainsi, de nombreux travaux et projets visent depuis une vingtaine d'années à élaborer des outils d'analyse et la vérification des protocoles cryptographiques.

Vu la difficulté du problème, ces analyses sont généralement menées dans des modèles dits formels, formulés de manière abstraite vis-à-vis de l'implémentation des primitives cryptographiques [12].

II.2 La cryptologie en quelques mots

II.2.1 Science du secret

La cryptologie est étymologiquement la science du secret. Ceci regroupe en fait de nombreuses notions. Historiquement, la cryptologie a servi à sécuriser certaines transmissions militaires, c'est-à-dire à chiffrer des messages. Plus récemment, et notamment depuis l'avènement de l'ère numérique, la cryptologie a connu d'autres usages, comme celui de la signature numérique ou de l'identification des personnes.

De façon la plus simplifiée possible, la cryptologie consiste en la manipulation de données variables, les messages et les identités, par des données constantes (secrètes ou publiques), les clés, au travers d'algorithmes, les schémas cryptographiques[13].

II.2.2 Cryptographie, cryptanalyse

La cryptologie regroupe deux sciences duales et étroitement liées : la cryptographie, qui est la science de la construction de schémas cryptographiques, et la cryptanalyse, qui est la science de l'étude des attaques sur ces schémas. Comme nous pouvons l'imaginer, ces deux sciences ne vont pas l'une sans l'autre, et parfois, la frontière entre elles est ténue. Ainsi, par exemple, concevoir un schéma résistant à tel ou tel type d'attaque, est-ce faire de la cryptographie ou de la cryptanalyse ?

II.2.3 Cryptographie symétrique, cryptographie asymétrique et la fonction de hachage

Les schémas cryptographiques sont de nos jours de deux types. Le premier type est celui qui existe depuis le début de la cryptographie, dès les temps antiques. Dans cette famille de schémas, deux entités partagent une même clé, secrète pour les autres utilisateurs, et peuvent ainsi opérer des opérations symétriques chacune de leur côté, d'où le nom de cryptographie à clé secrète ou cryptographie symétrique.

Le second type de schémas cryptographiques est très récent, et a inauguré ce qui est parfois appelé l'ère moderne de la cryptographie. Cette forme de cryptographie a été introduite par *Whitfield Diffie* et *Martin Hellman*, dans le célèbre "New directions in cryptography".

Dans cette famille de schémas, deux clés coexistent, l'une privée, c'est-à-dire réservée à un utilisateur, et l'autre publique, c'est-à-dire connue de tous. Ce type de schéma est tel que, pour certaines opérations, comme le chiffrement, seule la clé publique est nécessaire, et que pour certaines autres opérations, comme le déchiffrement, la clé privée est indispensable. Ceci explique le nom de *cryptographie à clé publique* ou de *cryptographie asymétrique*.

II.2.3 .1 Chiffrement symétrique :

Le principe du chiffrement symétrique, ou chiffrement à clé secrète est : la clé utilise pour le cryptage du texte clair (plaintext) est la même pour décryptage du texte chiffré (ciphertext). Le problème se pose dans les algorithmes symétriques est la gestion de clé

Il existe deux classes d'algorithmes de chiffrement symétrique: chiffrement en continu « Block-cipher » et chiffrement par blocs « Stream Ciphers ». Les algorithmes principales de type block-cipher sont : DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), et RC5 (Rivest Cipher). Le chiffrement par bloc, crypte un bloc complet de données à un moment, alors que la taille d'un tel bloc de données est habituellement de 64, 128, 192 ou 256 bits et la transformation de cryptage est fixe.

- **Exemple: Algorithme AES**

L'algorithme AES (Advanced Encryption Standard) et appelé aussi algorithme de Rijndael, conçu par Joan Daemen et Vincent Rijmen, et adopté par NIST en 2000. Il permet de crypter de bloc de taille fixe 128 bits, et les clés adaptées dans le chiffrement avec de longueur de 128, 192 et 256 bits. Ceci laisse une grande flexibilité à l'utilisateur d'AES en fonction du niveau de sécurité et de la performance de calcul. Cet algorithme est plus largement utilisé dans les systèmes limités des ressources informatiques (e.g. les systèmes embarqués) par rapport aux autres algorithmes de chiffrement symétriques.

II.2.3 .2 Chiffrement asymétrique :

On peut l'appeler chiffrement par clé publique, dans cet chiffrement, la clé de cryptage et la clé de décryptage sont différentes. Chaque personne possède deux clés distinctes (une privée, une publique) avec impossibilité de déduire la clé privée à partir de la clé publique.

On peut utiliser des algorithmes à clé publique en : chiffrement/déchiffrement (cela fournit le secret), signatures numériques (cela fournit l'authentification), et échange de clés (ou des clefs de session).

Ces algorithmes reposent sur des principes mathématiques qui sont :

- 1) basée sur la factorisation de grands nombres (e.g. RSA),
- 2) basée sur les logarithmes discrets (e.g. Diffie-Hellman, ElGamal),
- 3) basée sur les courbes elliptiques (e.g. ECC).

- **Exemple : Algorithme RSA**

Le système RSA est inventé en 1978 par Rivest, Shamir et Adleman. Il est basé sur le problème difficile à résoudre de la factorisation de grands nombres. Comme tous les systèmes de cryptage, RSA est composé de trois algorithmes: un pour la génération de clés, un pour le chiffrement et un pour le déchiffrement. La clé publique K_{pub} est composée de (e,n) , et la clé privée K_{priv} est égal à (d, n) , tel que $n = pq$ (où p et q sont des nombres premiers), et d calculé par $ed \equiv 1 \pmod{(q-1)(p-1)}$ tel que d inverse de e dans l'arithmétique mod $(q-1)(p-1)$. Une fois les deux clés sont générées, les deux nombres premiers p et q ne sont plus utilisés. Pour crypter un message m on fait le calcul suivant : $E_{K_{pub}}(m) = m^e \pmod n$. pour l'opération d'inverse (i.e. décryptage) on fait le calcul suivant : $D_{K_{pri}}(m) = m^d \pmod n$.

II.2.3 .3 Fonction de hachage :

On parle de "*haché*", ou de "*condensé*" pour désigner la caractéristique d'un texte unique. Une fonction de hachage *hash* prend comme entrée une valeur de longueur non bornée et renvoie une valeur de longueur n fixée. La probabilité d'avoir deux messages avec le même haché doit être extrêmement faible.

Depuis les travaux de Diffie Hellman [15] en 1976, il a été reconnu que les fonctions de hachage doivent être unidirectionnelles ou à sens unique, c'est-à-dire il est facile de trouver $h(x)$ à partir de x et très difficile de trouver x étant donné $h(x)$. Provoqué formalisation de cette dernière est difficile une deuxième propriété proposée, sans collision (*collision freedom*) c'est-à-dire il est difficile de trouver deux entrées différentes x et x' tel que : $h(x) = h(x')$.

En 1992 Okamoto a proposé une troisième primitive sans corrélation (*correlation freedom*) : une fonction h est dite sans corrélation s'il est difficile de trouver deux entrées différentes x et x' tel que $h(x)$ et $h(x')$ diffèrent uniquement en quelques bits.

- **Exemple : SHA-1**

La fonction de hachage de type SHA-1 (Secure Hash Algorithm) est plus couramment utilisée parmi les fonctions de hachage avec longueur de bloc 160 bits. Il est utilisé dans des protocoles de sécurité tels que : TLS (Transport Layer Security), SSL (Secure Sockets Layer), et IPSec (Internet Protocol Security). Concernant cette fonction, en 2004 une équipe chinoise a trouvé une méthode pour trouver une collision en 2^{69} essais, ce qui a conduit à la publication des nouvelles fonctions de hachage, telles que SHA-256 et SHA-512. Les autres principales fonctions de hachages sont : MD4 (Message Digest 4) est désignée par Rivest en 1990 avec la longueur de bloc 128 bits, Une

collision pour MD4 peut être trouvée en calculant 2^{20} valeurs de hachage. MD5 (Message Digest 5) même longueur que MD4.

II.3 Buts de la cryptologie

Dans cette section, nous listons quelques-uns des principaux buts de la cryptologie, c'est-à-dire les services que la cryptologie délivre. Nous donnons également la ou les *primitives* usuellement utilisées pour atteindre chacun des buts cités [13].

II.3.1 Confidentialité

Comme évoqué dans la section précédente, le but premier de la cryptologie a été la confidentialité, c'est-à-dire l'échange entre entités de messages chiffrés, qui, sans clé de déchiffrement, sont intelligibles. La confidentialité est obtenue principalement au travers de schémas de chiffrement, qu'ils soient à clé secrète ou à clé publique.

II.3.2 Intégrité

Un autre but de la cryptologie est l'intégrité. Ceci désigne le fait qu'une personne veuille s'assurer que le message reçu n'a pas été modifié par une tierce personne. L'intégrité est gérée au travers de fonctions de hachage à clé secrète (en anglais, message authentication code, MAC), ou à l'aide de schémas de signature à clé publique.

II.3.3 Identification

L'identification est la partie de la cryptologie permettant de reconnaître une personne, au travers d'un secret qu'elle seule possède. Pour cela, la primitive cryptographique principale est le protocole d'identification. Un sous-type, appelé protocole d'identification à divulgation nulle de connaissance, est d'un intérêt plus particulier : dans ce type de protocole, le prouveur montre qu'il connaît un secret associé à une donnée publique, sans rien dévoiler de plus sur ce secret.

II.3.4 Authentification

Un dernier but de la cryptologie est l'authentification. Il s'agit l'a pour une personne de prouver qu'un message a bien été envoyé par elle. Cette notion est très proche de l'identification, dans laquelle, en plus, un message interviendrait. L'authentification se gère en cryptographie principalement au travers de schémas de signature à clé publique. L'usage de schémas de signature à clé publique plutôt que de fonctions de hachage à clé secrète permet la non-répudiation, c'est-à-dire qu'une signature valide d'un message donné ne puisse être contestée par le signataire.

II.4 Protocoles cryptographiques :

Un protocole cryptographique ou protocole de sécurité est un ensemble de règles d'échange entre les participants d'un réseau (entités ou agents), basé sur les notions de crypto-systèmes qui permettent de sécuriser les communications dans un environnement hostile afin de réaliser une certaine fonctionnalité.

II.4.1 Notations

Pour décrire un protocole, les notations les plus classiques sont celles du type Alice-Bob (ou modèle A-B). Ce modèle est largement utilisé parce que la syntaxe de ce modèle est très simple et intuitive. Le papier de J. Clark et J. Jacob [14] est parmi les premiers papiers après ces notations pour décrire les protocoles d'authentification.

La syntaxe de ce modèle est basée sur le fait de fournir la séquence des messages transmis lors d'une session réussie du protocole (Table II.1).

Symbole	Signification
A, B, R, T	Nom d'agent honnête, R : Lecteur ; T : Tag
I	Nom d'agent intrus
m	Message
Nr, Nt	Nonce (nombre aléatoire « frais »)
h	fonction de hachage
,	Concaténation
K	Clé symétrique partagée entre K et T (ou entre A et B)
K _x	Clé publique de l'agent X
ID	Identificateur de tag partagé
{m} _K	Le message m crypté avec K
A → B : m	A envoie un message m à B
I(A) → B : m	L'envoi d'un message m par I se faisant pour A

Table II- 1 : Notations

II.4.2 Les types des protocoles :

Nous présentons différents types des protocoles selon les notions des cryptographies étudiées. D'abord, expliquons brièvement les classes de protocoles utilisées avec nombre borné des participants et assurons des buts spécifiques. Puis présentons les protocoles de groupe et les protocoles à divulgation nulle.

II.4.2.1 Protocole des buts spécifiques :

Le domaine d'Internet, de carte à puce, de réseau ad-hoc, de réseau de capteur, de réseau sans fil et systèmes RFID ont des buts plus spécifiques relié par l'objectif du protocole et les caractéristiques de réseau.

- **Protocoles d'authentification:**

Le protocole d'authentification est un protocole cryptographique qui assure la propriété d'authenticité. Cette authentification est, soit unilatérale ou mutuelle. On cite quelques protocoles largement utilisés dans le monde de communication des réseaux (surtout Internet) : EAP (*Extensible Authentication Protocol*), Kerberos, NSPK, PGP (*Pretty Good Privacy*).

On présente par exemple, le protocole d'authentification *Needham-Schroeder Public*

Key (NSPK) [16]:

A et B disposent des clés publiques, K_a et K_b respectivement ;

$$A \rightarrow B : \{A, Na\}_{K_b} \quad (1)$$

$$B \rightarrow A : \{Na, Nb\}_{K_a} \quad (2)$$

$$A \rightarrow B : \{Nb\}_{K_b} \quad (3)$$

(1) l'agent A envoie son nom A et nonce Na . Ce message est chiffré par clé publique de B (2) B reçoit le message $\{A, Na\}_{K_b}$ envoyé par A. Comme il a la clé privée lui permettant d'ouvrir le message, il comprend qu'A veut lui parler et renvoie le nonce Na ainsi qu'un autre nonce Nb qu'il vient d'engendrer, le tout chiffré avec la clé publique K_a d'agent A. B envoie donc à A le message $\{Na, Nb\}_{K_a}$.

(3) A reçoit le message $\{Na, Nb\}_{K_a}$, le déchiffre et reconnaît son nonce Na . Elle en déduit que l'agent B lui a répondu et elle lui renvoie son nonce Nb crypté avec sa clé publique pour lui signifier qu'elle connaît maintenant le message Nb . Elle envoie donc

$$\{Nb\}_{K_b}.$$

Donc, quand A déchiffre (2), elle vérifie que Na est la bonne valeur et en déduit que B connaît Na et est bien authentifié. B fait de même avec (3).

Ce protocole considéré comme étant sûr pendant seize années ; avant que G. Lowe [17] a découvert une attaque et a proposé une correction de ce protocole.

- **Protocoles d'échange de clé :**

D'autres types de protocoles assurent la confidentialité de clé symétrique générée et partagée par plusieurs participants, tels que : le protocole IKE (*Internet Key Exchange*), TLS (*Transport Layer Security*), et protocole AKA (*Authentication and Key Agreement*). On présente le protocole Diffie-Hellman [15] qui été un protocole d'échange de clés entre deux agents A et B. Une variante simple de ce protocole, en trois étapes est présentée ci dessous

:

$$A \rightarrow B : g^{Na} \bmod p \quad (1)$$

$$B \rightarrow A : g^{Nb} \bmod p \quad (2)$$

$$A \rightarrow B : \{Nsec\}_K \quad (3)$$

(1) *A* génère le nonce *Na* et calcule l'exponentiation modulaire de *g* par *Na*, g^{Na} , où *g* et *p* sont des nombres adaptés à Diffie-Hellman connus de tous les participants. *A* envoie ensuite le message g^{Na} à l'agent *B*.

(2) l'agent *B* génère lui aussi un nonce *Nb* et calcule g^{Nb} puis $K = (g^{Na})^{Nb}$. Il envoie le premier à *A* et conserve le second comme clé partagée avec *A*. Dès que *A* reçoit le message g^{Nb} , il est capable de calculer $(g^{Nb})^{Na}$ et il a donc lui aussi la clé partagée. En effet, d'après les propriétés de l'exponentiation modulaire $K = (g^{Na})^{Nb} = (g^{Nb})^{Na}$.

(3) le message $\{Nsec\}_K$ est envoyé par *A* à l'agent *B* avec *Nsec* une donnée qui doit rester secrète entre les agents *A* et *B*.

Le protocole de Diffie-Hellman souffre ainsi d'une attaque bien connue de type homme au milieu (man in the middle).

- **Les protocoles de vote électronique:**

Un tel protocole e-vote nécessite au moins les deux propriétés suivantes : vérifiabilité : chacun veut être en mesure de vérifier que son vote a été considéré et que le scrutin final est correct. Anonymat : chacun veut conserver le secret de son vote. Un exemple de ce type de protocole est proposé par Baudron et al. [18]

- **Les protocoles de signature de contrat :**

Les signatures de contrat sur Internet amènent deux problèmes de sécurité, non répudiation et l'équité (i.e. garantir qu'aucun participant n'est désavantagé lors de la signature du contrat). Un exemple de protocole de signature de contrat est GJM [19], l'objectif de ce protocole est de parvenir à la signature du contrat distribué à un abus passage libre.

II.4.2.2 Protocoles de groupes :

La caractéristique importante pour cette catégorie tel que le protocole est défini pour un nombre quelconque d'agents. Certains protocoles permettent, par exemple, l'établissement d'une clé partagée entre *v* individus : IKA Cliques-I [20]. Ce protocole met en jeu la méthode de Diffie-Hellman que nous avons présentée précédemment pour l'établissement d'une clé commune à tous les agents.

II.4.2.3 Protocole à divulgation nulle :

Les protocoles de cette classe sont en effet destinés à la preuve de données sans les divulguer (de l'anglais : zero-knowledge proof). La première approche de « zero-knowledge proof » pratique a été développée par A. Fiat et A. Shamir [21] en 1986 et optimisée par L. Guillou et JJ. Quisquater en 1987. Dans les systèmes « zero-knowledge proof » le vérifieur n'a pas besoin de secret et le prouveur possède un secret diversifié qui ne met pas en péril l'ensemble du système. Il s'agit d'une méthode très puissante pour authentifier des messages, sans donner la moindre information sur le secret utilisé, car une part est laissée au hasard. On demande au prouveur de résoudre un problème qu'il est seul capable de résoudre, le nombre de réponses possibles étant faible. Le protocole consiste à poser une série de questions pour augmenter la conviction du vérifieur avec le nombre de bonnes réponses données par le prouveur.

II.5 Conclusion

Dans ce chapitre nous avons étudié les différentes notions de cryptographie (symétrique, asymétrique, et la fonction de hachage), ainsi nous représentons le but de la cryptographie. Et à la fin nous avons donné une présentation sur les protocoles cryptographiques.

CHAPITRE III

Protocoles délimiteurs de distance des systèmes RFID

Des approches palliatives peuvent être imaginées pour se prémunir des attaques par relais, comme utiliser un protocole qui détermine une borne supérieure sur la réelle distance entre ces deux entités. Un tel protocole est dit de « distance bounding »

III.1 Introduction

Alors que l'identification par radiofréquence (RFID) est devenue une technique incontournable, de nombreuses questions se posent, tant au sujet de la sécurité que cette technique apporte, qu'au sujet des risques liés à la vie privée qu'elle fait encourir. Dans ce chapitre nous offrons une introduction à l'attaque sur la RFID et décrivons les problèmes de sécurité auxquels cette technique est confrontée, en présentant quelques protocoles de distance bornées de protection contre cette menace qui utilisent la primitive cryptographique comme la fonction de hachage(MD-5,SHA-1.)

III.2 Attaques par relai :

III.2.1 Présentation :

Une attaque par relais, connu en anglais sous le nom de « relay attack », est un type d'attaque informatique, similaire à l'attaque de l'homme du milieu et l'attaque par rejeu, dans lequel un attaquant ne fait que relayer mot pour mot un message d'un expéditeur vers un récepteur valide.

III.2.1 Principe :

Le principe de l'attaque par relais établit que deux victimes croient communiquer directement entre elles et ne s'aperçoivent pas qu'un système pirate relaie leur dialogue [22].

Le scénario pour mener à bien une telle entreprise est d'introduire un faux couple d'interlocuteurs dans un dialogue normalement directement conduit entre deux correspondants légitimes [23].

On parle d'attaque passive lorsque le dialogue, initié par une des deux victimes vers son correspondant, est intercepté puis relayé par un attaquant qui a l'intention de tirer profit des données échangées sans pour autant chercher à les modifier. Par contre si un piratage est mené dans le but d'altérer les informations transmises on utilise alors le terme d'attaque active.

Le faux client C_f se charge d'intercepter les informations émises par un vrai serveur S tandis que le faux serveur S_f assure cette même tâche auprès d'un bon client C . Via un moyen de communication adapté, le faux serveur et client doivent établir un relais de la communication sans se faire repérer [23]. L'idée d'une telle manipulation est remarquable dans le sens où elle se réalise sur la couche la plus basse de la liaison afin de s'affranchir des différentes sécurisations de communication habituellement déployées [24]. Dans la pratique le couple d'équipements composant le système frauduleux peut éventuellement être agrégé en un seul dispositif matériel mais sera toujours composé de deux interfaces S_f - C_f assurant chacun les rôles précédemment décrits [25]. Le but de l'attaque par relais est de pouvoir usurper l'identité ou les droits d'un utilisateur.

Le pirate sera en mesure de contourner des systèmes de contrôle d'accès, de frauder des systèmes de paiement, de détourner des votes par bulletins électroniques, de s'introduire et de communiquer sur tout réseau sur lequel il ne serait normalement pas admis. Il pourra également accéder à des fichiers réservés ou inonder (Spam) des messageries de courriers électroniques [26].

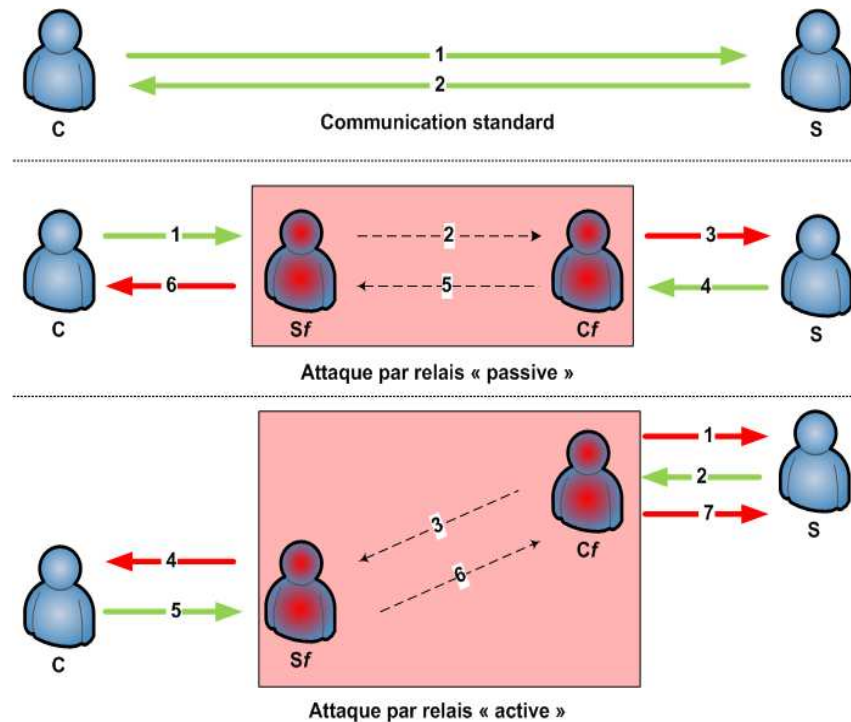


Figure III- 1: Attaque par relais sur un système RFID

III.2.2 Illustration sur quelques technologies

L'attaque par relais est réalisable dans une grande variété de situations et peut donc être exploitée sur tout modèle client-serveur habituellement présent dans les différentes technologies de l'information et de la communication.

III.2.2.1 RFID

En 2005 Gerhard Hancke [27] est passé avec succès de la théorie à la réalisation pratique d'une maquette démontrant une attaque sur des cartes à la norme (ISO/IEC 14443 (en)) destiné à la Radio-identification. Sa démonstration était applicable sur une distance pouvant aller jusqu'à 50 mètres entre la carte et le lecteur attaqués, car elle s'appuie sur une technique basique de relais du canal physique, avec l'exécution d'une simple modulation/démodulation par les équipements pirates placés à proximité des deux extrémités.

III.2.2.2 Véhicules sans clé

En 2010 A. Francillon [28] a décrit un type d'attaque par relais sur des véhicules sans clé (PKES) permettant à un voleur d'ouvrir ou de fermer la voiture tout en se tenant éloigné dans une zone allant de 2 à 8 mètres. Il peut alors autoriser l'ouverture des portes et le démarrage du moteur en provoquant un ordre direct de la vraie clé en UHF fonctionnel jusqu'à 100 mètres.

Le système de la première attaque via un câble coaxial est composé de deux antennes radio connectées ensemble par un câble. Quand l'antenne est présentée près de la porte du véhicule elle capture le signal de la balise. Ce champ magnétique excite l'antenne qui crée, par induction, un signal en sortie d'antenne. Via le câble, ce signal électrique est ensuite transmis à la seconde antenne qui génère un champ magnétique omnidirectionnel. Ce champ radio excite alors l'antenne de la clé qui démodule le signal et envoie au véhicule via UHF l'ordre d'ouverture et de déverrouillage du démarrage.

Le système de la seconde attaque sans câble est composé de deux antennes radio, d'un émetteur et d'un récepteur. L'émetteur capture le signal pour le convertir en ondes 2,5 GHz puis l'amplifie pour transmission. Le récepteur qui reçoit ce signal le convertit et envoie l'ordre de départ à l'antenne de la clé. Le système d'ouverture et de déverrouillage du démarrage est alors activable comme pour l'attaque via câble.

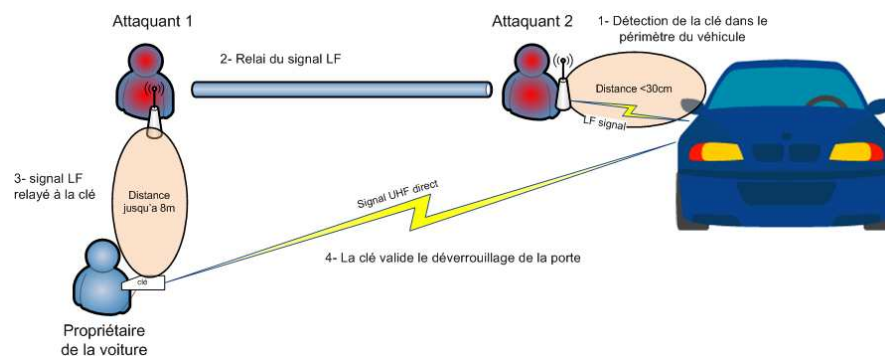


Figure III- 2 : Schéma de principe attaque par relais sur véhicules équipés de carte sans fil

III.3 Protocoles de distance bornée

III.3.1 Motivations

Comme nous l'avons vu dans la première section, l'une des principales attaques sur la technologie RFID est l'attaque par relais.

Afin de l'éviter, des protocoles ont été inventés, c'est le cas du protocole de distance bornée (distance-bounding protocol en anglais). Ce type de protocole permet de prouver à un vérificateur (un lecteur RFID par exemple) qu'un prouveur (une étiquette RFID par exemple) est à une certaine distance bornée de lui-même.

III.3.2 Fonctionnement

Le fonctionnement de ce protocole est simple, lorsque le lecteur pose une question à une étiquette, il calcule le temps de réponse. En multipliant le temps obtenu par la vitesse d'une onde électromagnétique, on obtient une estimation de la distance à laquelle l'étiquette est située du lecteur.

III.3.3 Protocole de distance bornée selon Stefan Brands et David Chaum

Le premier protocole de distance bornée a été proposé par Stefan Brands et David Chaum en 1993 [29].

III.3.3.1 Description du protocole

Ils ont proposé le protocole suivant :

- **Etape 1** : le prouveur et le vérificateur génèrent tous les 2 une séquence aléatoire de k bits. (appelées α pour le vérificateur et β pour le prouveur)
- **Etape 2** : l'échange de bits peut commencer, on répète k fois :
 - le vérificateur envoie α prouveur
 - le prouveur envoie β_i au vérificateur
- **Etape 3** : le prouveur concatène α et β et l'envoie chiffré avec la clé secrète au vérificateur.

L'échange de bits est terminé, le vérificateur doit accepter le prouveur si et seulement si la concaténation chiffrée reçue est la bonne et si le temps maximum entre l'envoi de ses bits et le retour est inférieur à une certaine valeur, définie par le vérificateur. Figure III.3 donne un exemple de l'utilisation de ce protocole.

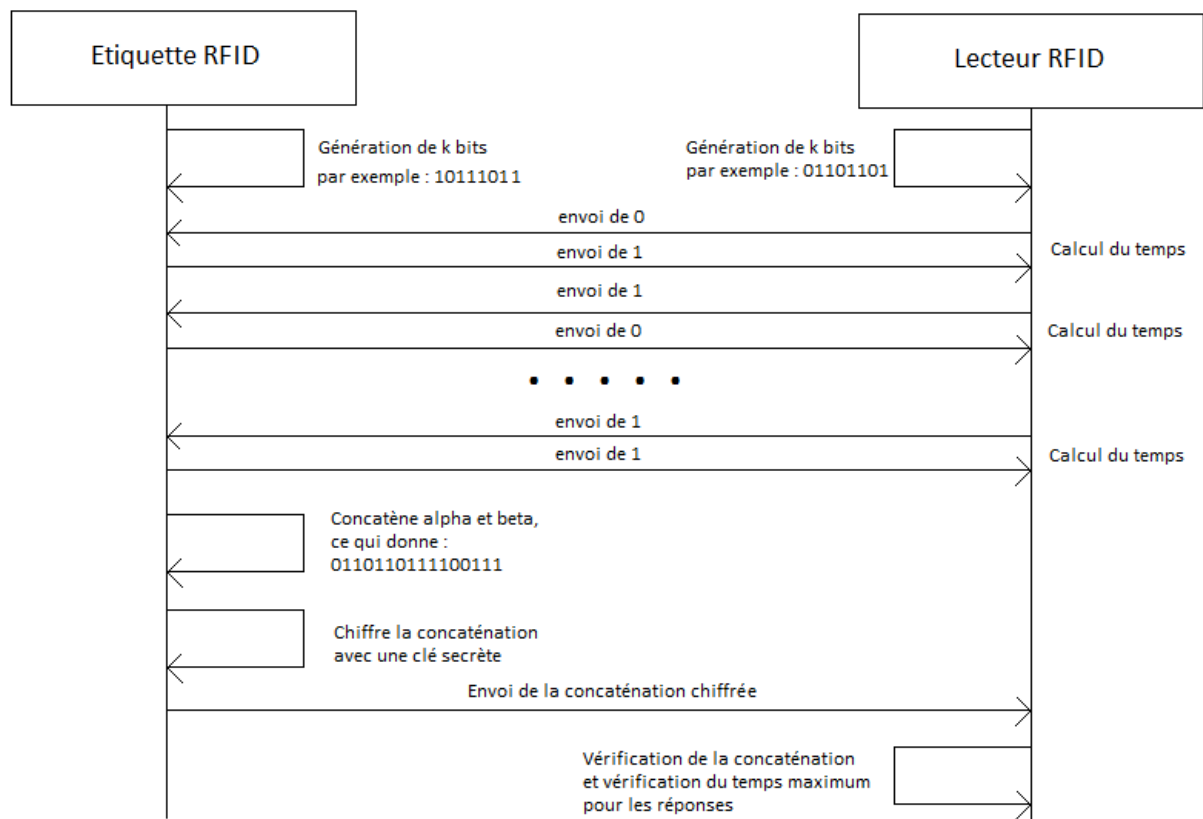


Figure III- 3 :Distance-Bounding protocol selon Stefan Brands et David Chaum

III.3.3.2 Problème de sécurité :

Avec cette solution, un problème existe encore. Il faut être capable de vérifier que le prouveur n'envoie pas les bits trop tôt. Supposons tout d'abord que le prouveur connaisse la clé secrète. On remarque que dans ce système, les bits envoyés par le prouveur n'ont aucun lien avec ceux envoyés par le vérificateur. De ce fait, si le prouveur connaît à l'avance à quel moment le vérificateur va envoyer les bits, alors il peut envoyer les siens dans un temps inférieur à celui nécessaire et cela peu importe la distance à laquelle le prouveur se trouve.

Pour remédier à ce problème, Stefan Brands et David Chaum ont pensé à 2 solutions :

Première solution : elle consiste à attendre un certain temps t tiré aléatoirement entre chaque bit envoyé. Ainsi, le prouveur ne pourra pas savoir quand il doit envoyer le prochain bit puisque même le vérificateur ne le sait pas à l'avance. De ce fait, le vérificateur rejettera le prouveur si le prouveur envoie un bit i avant que lui-même ait envoyé son bit i .

Deuxième solution : elle consiste à lier les bits α et β . Ainsi, le vérificateur pourra être sûr que les bits envoyés par le prouveur sont bien envoyés après ceux envoyés par lui-même. Si un bit ne correspond pas avec ce qui est attendu par le vérificateur, alors le prouveur sera rejeté.

Pour réaliser cela, il est nécessaire de créer une suite de bits m que l'on déclare public. Le vérificateur envoie ses k bits comme précédemment. En retour, le prouveur fait un OU-exclusif entre le bit reçu et m_i puis envoie le résultat au vérificateur. Et tout cela k fois. Pour vérifier que le prouveur a bien envoyé ses bits au bon moment, le vérificateur n'a plus qu'à faire un ou exclusif entre tous les bits reçus et la suite de bits m . Et comme précédemment, il vérifie le temps maximal des réponses.

III.3.3.3 Description du second protocole

Pour finir, les deux auteurs proposent ce schéma de communication :

- **Etape 1** : le vérificateur génère une séquence aléatoire de k bits. (appelée α)
- **Etape 2** : le prouveur génère une séquence aléatoire de k bits (appelée m) et l'envoie au vérificateur.
- **Etape 3** : l'échange rapide de bits peut commencer, on répète k fois :
 - le vérificateur envoie α_i au prouveur
 - le prouveur calcul $\beta_i = \alpha_i \oplus m_i$ et envoie β_i au vérificateur
- **Etape 4** : le prouveur concatène α et β et l'envoie chiffré avec la clé secrète au vérificateur

L'échange de bits est terminé, le vérificateur doit accepter le prouveur si et seulement si $\alpha_i \oplus \beta_i$ est égal à m_i envoyé au début de la communication. Si tel est le cas, alors le vérificateur vérifie que la concaténation chiffrée reçue est la bonne et correspond bien à la signature du prouveur. Enfin, il vérifie si le temps maximum entre l'envoi de ses bits et le retour est inférieur à une certaine valeur. La figure III.4 donne un exemple de l'utilisation de ce protocole.

III.3.3.4 Analyse de la sécurité

Ce protocole est efficace contre l'attaque mafia fraud avec un taux de succès pour un pirate de $(1/2)^n$, n étant le nombre de tours réalisés durant la phase rapide d'échange de bits. Cependant, il ne permet pas de lutter contre les attaques terrorist fraud et ne gère pas les erreurs durant l'échange de bits.

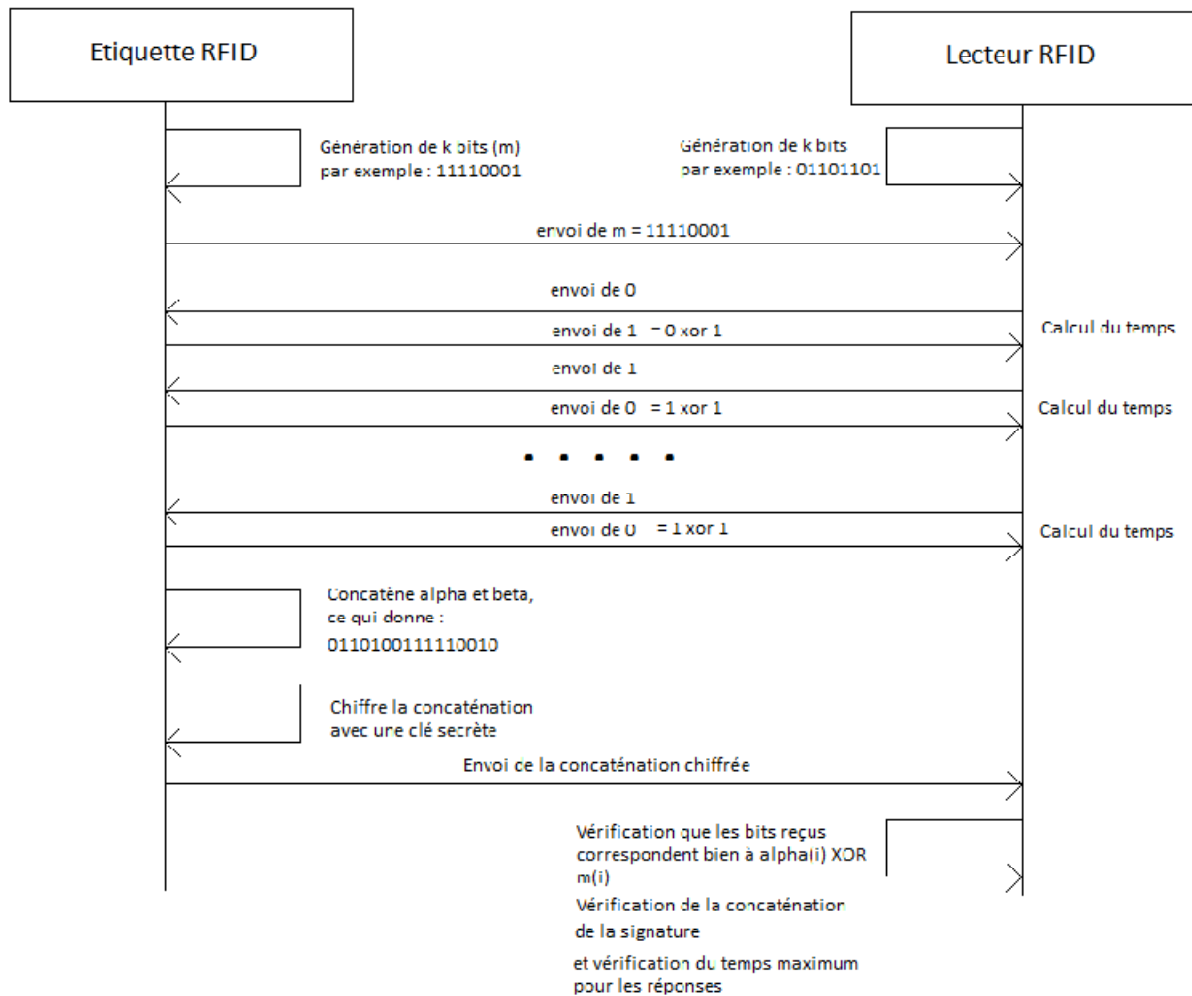


Figure III- 4 : Distance-Bounding protocol (second protocol) selon Stefan Brands et David Chaum

III.3.4 Protocole de distance bornée selon Gerhard P. Hancke et Markus G. Kuhn

Ces deux auteurs ont déposé un article [30] en 2005 sur un protocole de distance bornée. Comme dans le protocole vu précédemment, ce protocole utilise le temps de réponse du prouveur pour vérifier qu'il n'est pas situé plus loin qu'une certaine distance. Ce protocole sert de base à la plupart des protocoles de distance bornée proposés depuis. Une implémentation est proposée à la fin de la section pour servir de démonstrateur qui pourra être modifiée pour développer un autre protocole.

III.3.4.1 Description du protocole

Dans ce protocole, une fonction aléatoire h est connue du vérificateur et du prouveur et une clé secrète k est partagée. Voici les différentes étapes :

- **Etape 1** : le vérificateur envoie un unique numéro N_v choisi aléatoirement au prouveur
- **Etape 2** : le vérificateur et le prouveur calculent tous les deux $h(k, N_v)$ et placent la première moitié du résultat dans un registre R_0 et la deuxième dans un registre R_1 . Ainsi, le prouveur et le vérificateur possèdent les mêmes registres.
- **Etape 3** : l'échange de bits peut commencer, on répète k fois :
 - le vérificateur génère un bit aléatoire C_i et l'envoie au prouveur
 - Si $C_i = 0$ alors le prouveur envoie R_0^i , sinon il envoie R_1^i au vérificateur .
- **Etape 4** : le vérificateur calcule de son côté les valeurs qu'il aurait dû recevoir et les compare à celles reçues. Si les réponses sont identiques et que les réponses ont été reçues dans un temps limité, alors le prouveur est situé à une certaine distance du vérificateur. La figure III.5 donne un exemple de l'utilisation de ce protocole.

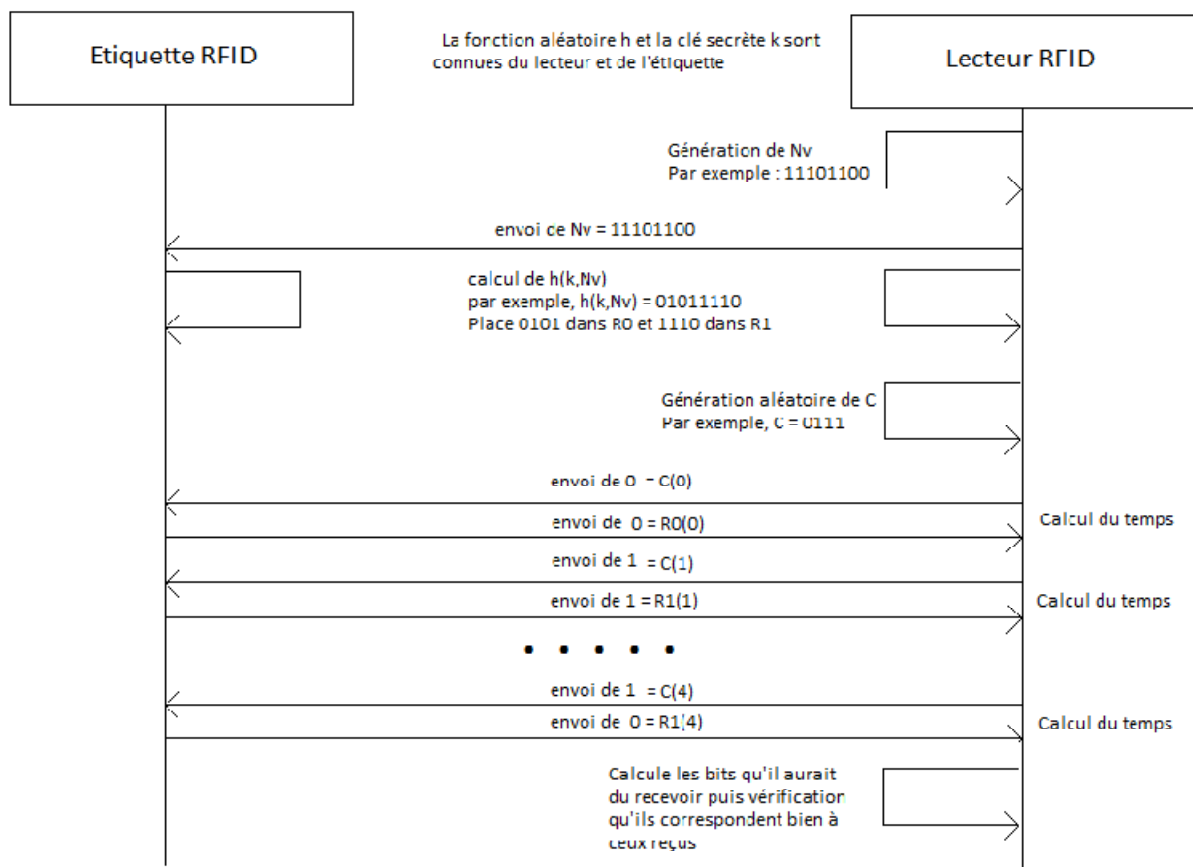


Figure III- 5 :Distance-Bounding protocol (second protocol) selon Gerhard P. Hancke et Markus G. Kuhn

III.3.4.2 Analyse de la sécurité

Ce protocole est efficace contre l'attaque mafia fraud avec un taux de succès pour un pirate de $(3/4)^n$, ce qui est un peu moins bon que le premier protocole vu dans ce rapport.

En effet, on pourrait croire que la probabilité qu'une personne pirate envoie le bon bit à chaque challenge soit de $1/2$ mais ça n'est pas le cas, elle est de $3/4$. Cela est dû au fait que la personne pirate peut accélérer le signal de l'horloge afin d'envoyer un bit C_i avant que le lecteur envoie le sien. L'étiquette répondra en fonction du C_{i0} et dans la moitié des cas, le C_i correspondra au C_i donc la personne pirate va répondre correctement à ce challenge.

Dans l'autre moitié des cas, la personne pirate aura répondu avec un bit aléatoire, ce qui lui donne une probabilité de $1/2$ d'être correct. C'est donc pour cela que la probabilité est de $3/4$ et non $1/2$.

Ce protocole ne permet pas de lutter contre les attaques terrorist fraud car l'étiquette légitime peut envoyer sans aucun problème les registres RO et $R1$ à la personne pirate avant le début de la phase rapide d'échange de bits sans pour autant que la clé secrète soit donnée.

III.3.5 Le protocole de distance bornée pour RFID Swiss-knife

Ce protocole [31] a été établi en 2008 par Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert et Olivier Pereira. Leur objectif est de trouver un protocole capable de satisfaire tous les besoins dans le domaine de la sécurité RFID.

Voici les objectifs de ce nouveau protocole :

- Authentification : ce protocole doit sécuriser l'authentification, à la fin de l'exécution de ce protocole, le vérificateur doit être sûr qu'il communique avec la bonne personne. Le protocole permet également une authentification mutuelle qui permet à l'étiquette d'authentifier le lecteur ;
- Résistance contre l'attaque de type mafia fraud : une étiquette ne peut pas être imitée si elle ne conspire pas avec un pirate ;
- Résistance contre l'attaque de type terrorist fraud : une étiquette ne peut pas être imitée si elle ne révèle pas sa clé secrète à un pirate ;
- Faible puissance de calcul : le nombre d'opérations cryptographiques doit être le plus petit possible ;
- Faible taux de fausse acceptation : le nombre de tours dans l'algorithme pendant la phase rapide doit être le plus faible possible tout en ayant un taux de fausse acceptation le plus faible possible ;
- Respect de la vie privée : le protocole ne doit pas révéler l'identifiant de l'étiquette à une autre personne qu'au véritable vérificateur.

III.3.5.1 Description du protocole

Leur protocole est basé sur le protocole MAP1 de Bellare et Rogaway proposé en 1994 [32] et le MAP1.1 de Guttman en 2004 [33]. Tout d'abord, le lecteur et l'étiquette possèdent tous les 2 une clé secrète partagée notée k et une fonction pseudo-aléatoire notée f qui utilise la clé secrète. Le lecteur commence par générer un nombre aléatoire appelé N_a et l'envoie à l'étiquette. Il génère ensuite un nombre aléatoire appelé d et calcule $m = H(d)$ (où $H(d)$ est égal au poids de Hamming de d). Le lecteur envoie N_a et d à l'étiquette.

L'étiquette génère elle aussi un nombre aléatoire appelé N_b et calcule une clé temporaire $a = f(C_b, N_b)$. L'étiquette calcule ensuite $Z_0 = a$ et $Z_1 = k \oplus a$. Pour finir cette étape, elle calcule R_0 et R_1 de la manière suivante :

Pour i de 1 à m

j : index du prochain 1 de d

$$R_0[i] = Z_0[j], R_1[i] = Z_1[j]$$

L'étiquette envoie N_b au lecteur.

C'est le début de la phase rapide d'échange de bits. Cette phase possède m tours. De 1 à m , le lecteur choisit aléatoirement un C_i appartenant à $\{0,1\}$ et l'envoie à l'étiquette.

L'étiquette retient le C_i sous la forme $C_{i'}$ et envoie $R^i = R_0^i$ si $C_i = 0$ ou R_1^i si $C_i = 1$.

Pendant la phase de question/réponse, le lecteur calcule le temps que l'étiquette met pour répondre.

La phase d'échange rapide est terminée, l'étiquette calcule $T_b = f(c_{1'}, c_{2'}, \dots, c_{m'}, ID, N_a, N_b)$, ID étant son identifiant. L'étiquette envoie T_b au lecteur.

Le lecteur commence par vérifier l' ID dans sa base de données puis calcule R_0 et R_1 de la même manière que l'étiquette. Il calcule ensuite 3 valeurs :

ERR_c = nombre de fois où le $c_{1'}$ est différent du C_i .

ERR_r = nombre de fois où le $C_{i'}$ est égal au C_i et R_i est différent de $R_{C_i}^i$.

ERR_t = nombre de fois où le temps mis pour répondre est différent du temps maximum autorisé

Le lecteur calcule $ERR_c + ERR_r + ERR_t$ et le compare à un seuil T fixé. Si la somme est supérieure à T alors l'étiquette est rejetée.

La dernière étape est optionnelle, elle correspond à l'authentification mutuelle. Le lecteur calcule $T_a = f(N_b)$ et l'envoie à l'étiquette.

L'étiquette $T_a = f(N_b)$ calcule et compare avec la valeur reçue.

La figure III.5 donne un exemple de l'utilisation de ce protocole.

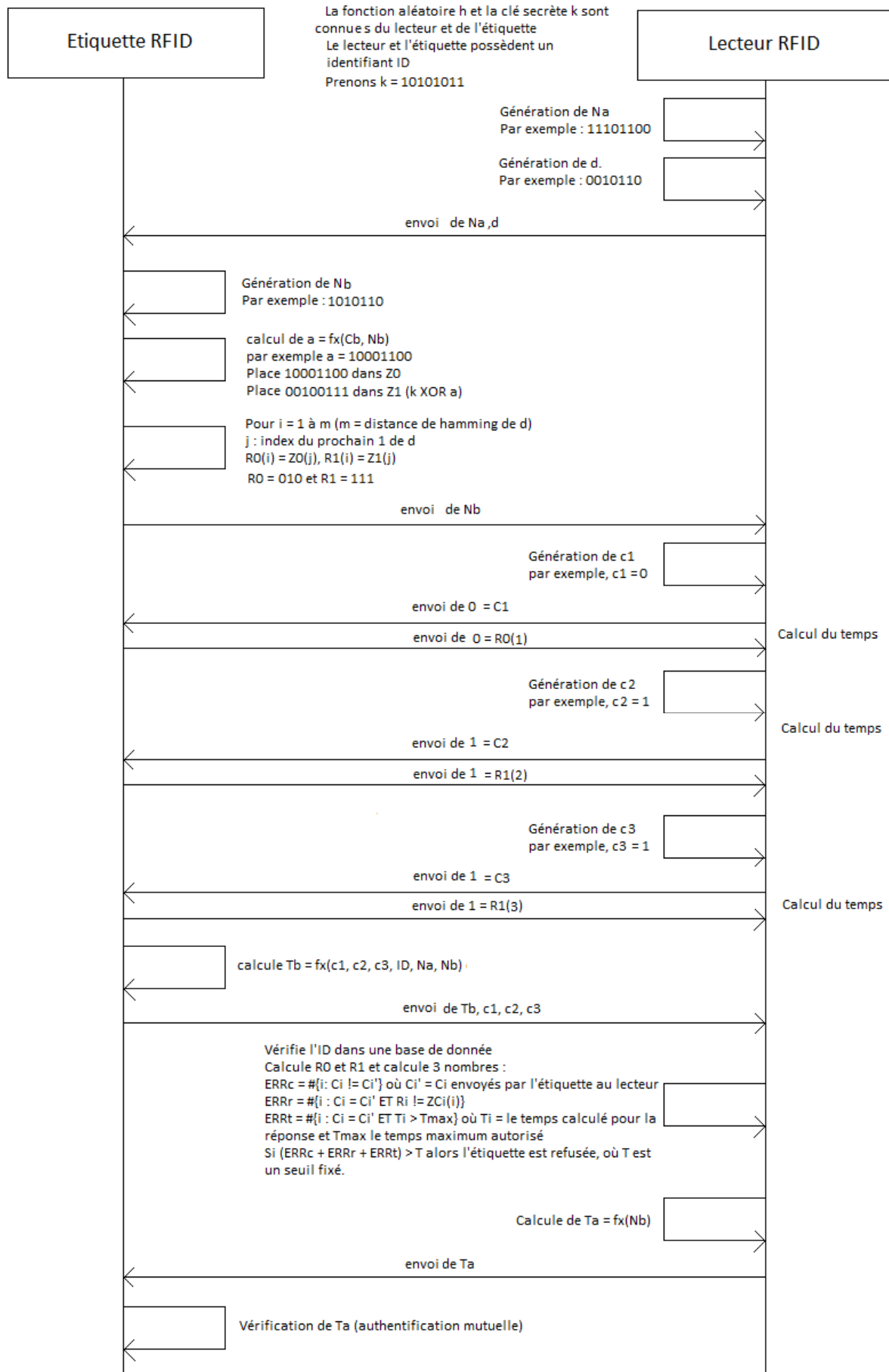
III.3.5.1 Analyse de la sécurité

Mafia fraud : Ce protocole est efficace contre l'attaque mafia fraud avec un taux de succès pour un pirate de $(\frac{1}{2})^n$. En effet, dans ce protocole, nous ne pouvons pas envoyer un challenge à l'étiquette avant celui du lecteur car après la phase rapide d'échange de bits, l'étiquette envoie tous les bits qu'elle a reçu. Ainsi, il est facile de vérifier si une personne pirate a envoyé des challenges avant ceux du lecteur. C'est pour cela qu'une personne pirate aura 1 chance sur 2 à chaque tour pour répondre correctement, d'où la probabilité énoncée.

Terrorist fraud : Dans ce protocole, à chaque tour, l'étiquette devra retourner une valeur en utilisant Z0 ou Z1 avec une probabilité de 1/2 pour les deux. Si l'étiquette légitime dévoile Z0 à la personne pirate, alors cette dernière aura 3 chances sur 4 de répondre correctement, donc la probabilité qu'il réponde avec succès à tous les challenges est de $(\frac{3}{4})^n$. Contrairement au protocole de Hancke et Kuhn, nous ne pouvons envoyer Z_0 et Z_1 car cela donnerait la clé secrète. Ce protocole est donc efficace contre les attaques de types terrorist fraud avec un taux de succès pour une personne pirate de $(\frac{3}{4})^n$.

Respect de la vie privée : Contrairement aux 2 protocoles que nous avons décrit au début de la troisième section, celui-ci permet d'authentifier une personne à l'aide de son identifiant. Ce dernier n'est jamais envoyé en clair donc ce protocole respecte la vie privée.

Tolérance aux erreurs : Ce protocole peut accepter quelques erreurs durant l'échange de bits. En effet, si quelques bits ont été corrompus, l'authentification pourrait tout de même réussir si ce nombre d'erreurs n'est pas trop important. Ceci est dû au fait que nous utilisons un seuil d'acceptation noté T. Ce seuil doit être choisi pour que la probabilité qu'un pirate s'authentifie avec $(m - T)$ tours d'échanges de bits soit suffisamment petite. Par exemple, si l'on choisit $m = 30$ et que l'on permet 2 erreurs ($T = 3$) sur ces 30 tours alors un pirate a 1% de chance de réussir dans le cas de l'attaque terrorist fraud. Si l'on choisit $m = 20$ et que l'on permet 4 erreurs ($T = 5$) sur ces 20 tours alors un pirate a 1% de chance de réussir dans le cas de l'attaque mafia fraud.



III.4 Conclusion

L'attaque par relais est la plus importante et nécessite des solutions de bas niveaux, car malgré l'utilisation de très bons algorithmes cryptographiques, cette attaque est toujours présente. En effet, elle ne fait que relayer des informations sans avoir à détenir de secrets particuliers.

Pour contrer ces attaques plusieurs protocoles de distance bornée ont été définis. les protocoles de distance bornée dont le but principal est de calculer à quelle distance une étiquette est située du lecteur durant l'authentification.

CHAPITRE IV

Implémentation de simulateur

Dans ce chapitre, nous allons détailler les outils et les bibliothèques utilisées pour réaliser notre simulateur (SIM_RFID_DBP).

IV.1 Introduction :

Au cours de ce chapitre, et pour répondre à cette question, nous essayons de présenter brièvement notre application, nous allons détailler les outils et les bibliothèques utilisées pour réaliser notre simulateur (SIM_RFID_DBP). Pour cela nous avons basé sur la conception détaillée dans le chapitre précédent.

IV.2 Simulation :

La simulation est un outil d'aide à la décision très utilisé par le concepteur et les gestionnaires des systèmes complexes, Elle consiste à construire un modèle d'un système réel (physique, économique, humain...etc.). Et conduire des expériences sur ce modèle afin de bien comprendre le comportement de ce système et d'en améliorer les performances. Peut être utilisé pour études, prédiction, réalisation...etc.

IV.2.1 Méthode de simulation :

Il existe deux catégories de méthode de simulation : la simulation continue et la simulation discrète.

- La simulation continue : si le modèle du système contient en grande partie des variables continues qui évoluent dans le temps, ce modèle conduit à un système d'équations différentielles. Fréquemment, il se trouve que le système d'équations ne peut pas être résolu analytiquement. On utilise alors la simulation dite continue, ou des combinaisons de méthodes numériques essaient d'aboutir à la solution du modèle.
- La simulation discrète, on l'utilise pour simuler le fonctionnement des systèmes discrets et stochastiques. C'est la méthode de simulation la plus développée jusqu'à présent et englobe trois stratégies : la simulation à événements discrets, la simulation des activités et la simulation des processus. Parmi des stratégies de simulation discrète, nous intéressons par la simulation des événements.

IV.3 Outils mis en œuvre

IV.3.1 Langage de programmation

Langage Java : Java est une technologie composée d'un langage de programmation orienté objet et d'un environnement d'exécution. Préalablement nommé Oak, il a été créé par James Gosling et Patrick Naughton chez Sun Microsystems avec le soutien de Bill Joy.

Le langage Java fut officiellement présenté le 23 mai 1995 au SunWorld.

Programmation orientée objet : La programmation orientée objet consiste à modéliser informatiquement un ensemble d'éléments d'une partie du monde réel en un ensemble d'entités informatiques. Ces entités informatiques sont appelées objets. Il s'agit de données informatiques regroupant les principales caractéristiques des éléments du monde réel (taille, couleur, ...).

Un objet est caractérisé par plusieurs notions telles que les attributs, les méthodes et l'identité. Cette identité est construite généralement par un identifiant découlant naturellement du problème. [34]

IV.3.2 Environnement de développement

L'EDI NetBeans : est un environnement de développement - un outil pour les programmeurs pour écrire, compiler, déboguer et déployer des programmes. Il est écrit en Java - mais peut supporter n'importe quel langage de programmation. Il y a également un grand nombre de modules pour étendre l'EDI NetBeans. L'EDI NetBeans est un produit gratuit, sans aucune restriction quant à son usage.

Également disponible, La Plateforme NetBeans; une fondation modulaire et extensible utilisée comme brique logicielle pour la création d'applications bureautiques. Les partenaires privilégiés fournissent des modules à valeurs rajoutées qui s'intègrent facilement à la Plateforme et peuvent être utilisés pour développer ses propres outils et solutions. [35]

Le Java Cryptography Extension (JCE) : est une interface de programme d'application (API) qui fournit un cadre uniforme pour la mise en œuvre des fonctions de sécurité dans Java. Il a été initialement développé pour compléter le kit de Java 2 Software Developer (SDK), Standard Edition, versions 1.2.x et 1.3.x, mais a depuis été intégrée dans le SDK Java 2, version 1.4. [36]

L'architecture JCE est basé sur le fournisseur, et de nouvelles applications peuvent être ajoutés de façon transparente. JCE prend en charge plusieurs applications de la sécurité numérique, tels que les suivants:

- chiffrement symétrique
- Les chiffres asymétriques
- chiffres flux
- Les chiffrements de blocs
- La génération des clés
- stockage de la clé
- Les signatures numériques
- Message Authentication Code (MAC) des algorithmes

IV.4 Présentation de l'application

IV.4.1 Pseudo code principal

Fonction de hachage

```
Import java.security.MessageDigest;
Import java.security.NoSuchAlgorithmException;
public static String hashage(String msg, String type) {
//type (type de method utilisé ans le cryptage

    byte[] uniquemsg = key.getBytes();
    byte[] hash = null;
    try {
        hash = MessageDigest.getInstance(type).digest(uniquemsg);
    }
    catch (NoSuchAlgorithmException e) {System.out.print(e.getMessage());
    }

    StringBuffer hashString = new StringBuffer();
//conver le resultat vers text
    for ( int i = 0; i < hash.length; ++i ) {
        String hex = Integer.toHexString(hash[i]);
        if ( hex.length() == 1 ) {
            hashString.append('0');
            hashString.append(hex.charAt(hex.length()-1));
        } else {
            hashString.append(hex.substring(hex.length()-2));
        }
    }
    return hashString.toString();
}
```

Génération de nombre pseudo aléatoire

```
Import java.util.Random;
public static int nombrePA {
    Random R1 = null;
    R1 = new Random();
    Int s1 = R1.nextInt(1000000000)
    Return s1 ;
}
```

Operation Ou-Exclusif

```
Import java.math.BigInteger;  
public static int Xors ( int x1 , int x2 )  
    {return x1^x2}  
public static Bigint Xorsbig ( int x1 , int x2 )  
    {return x1^x2}
```

IV.4.2 Interface principale

Cette fenêtre présente les différents protocoles réalisés

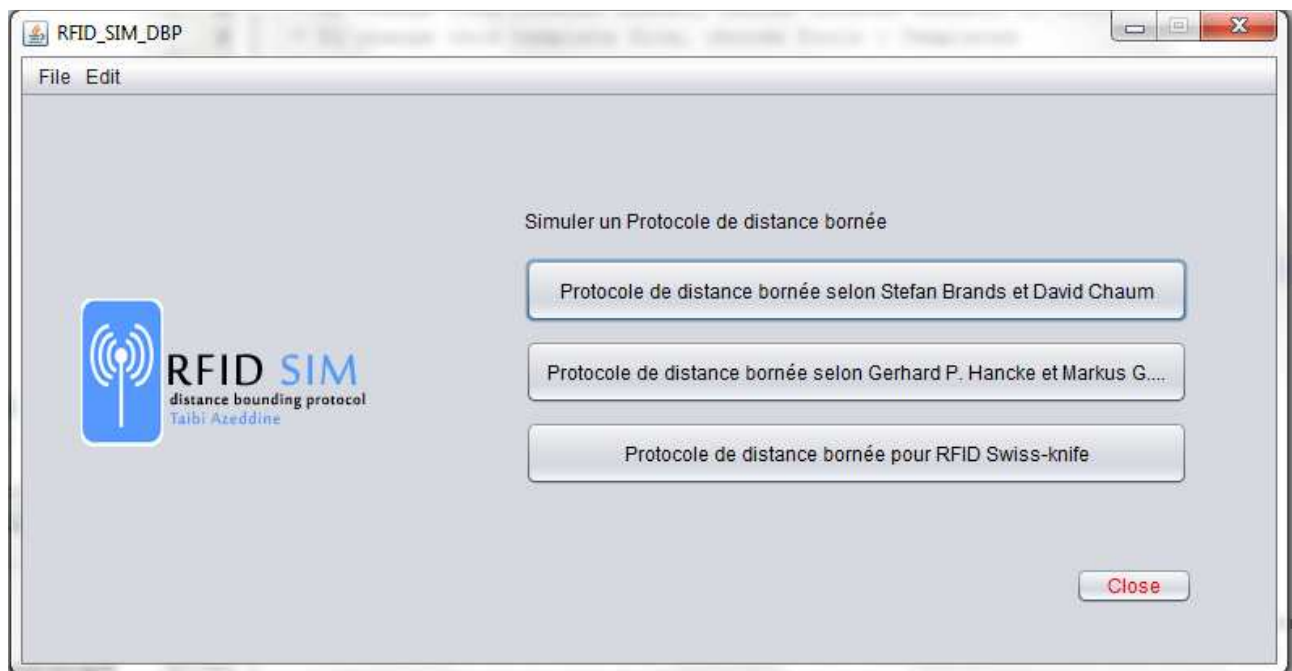


Figure IV- 1 : Interface principale d'application

Comme le montre la figure, notre application comporte :

- Un menu principal : Fichier , Aide.
- Trois boutons (les protocoles).

IV.4.2 Interface de protocole Stefan Brands et David Chaum

Cette fenêtre concerne en suite de tâche de la simulation de protocole délimiteurs de distance Stefan Brands et David Chaum.

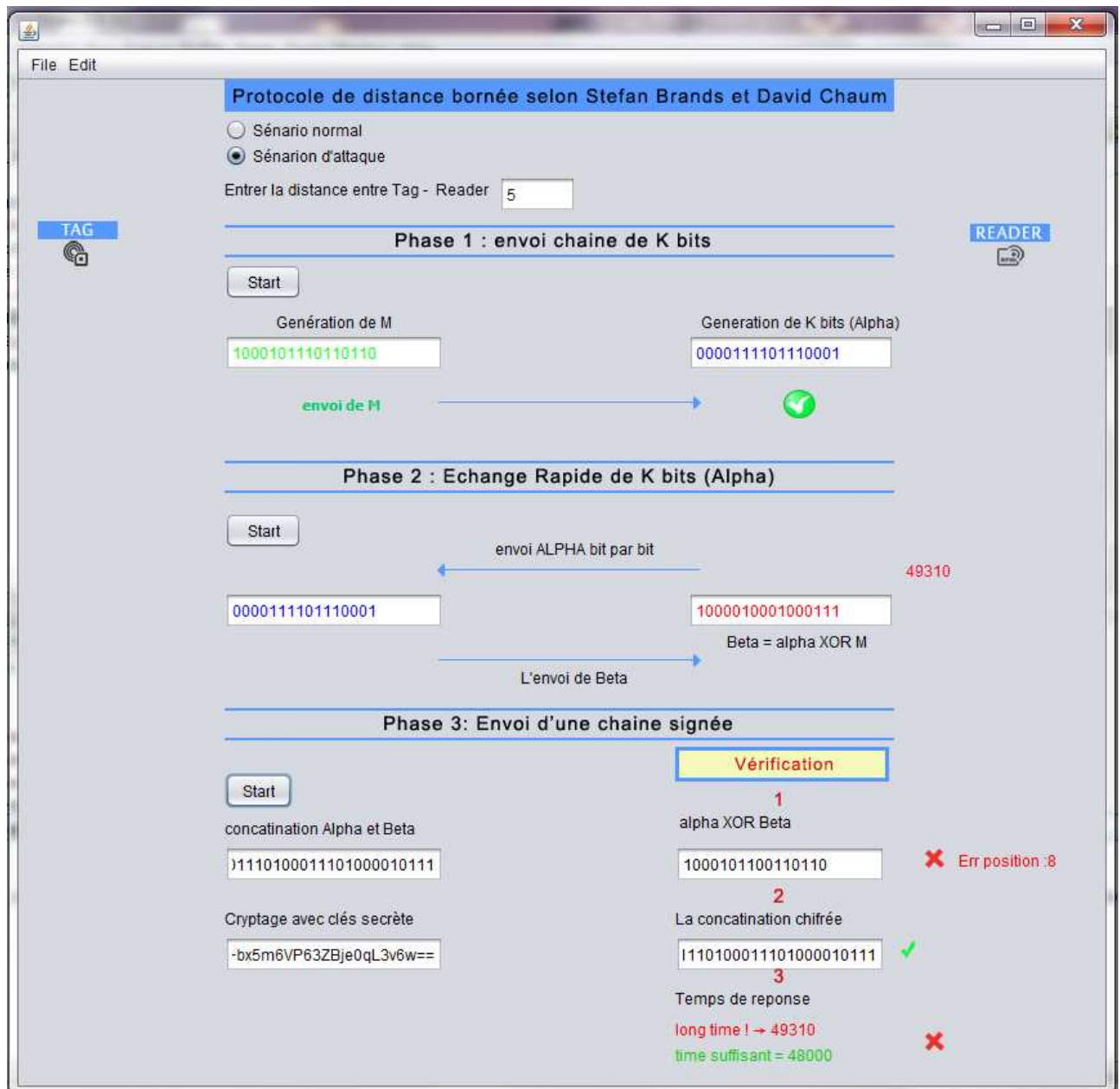


Figure IV- 2 : Interface principale d'application(protocol Stefan Brands et David Chaum)

L'opération de simulation s'effectue selon les étapes suivantes :

- 1) Sélectionner le scénario de simulation et la distance entre le TAG et le Reader.
 La figure représente la zone de sélection.

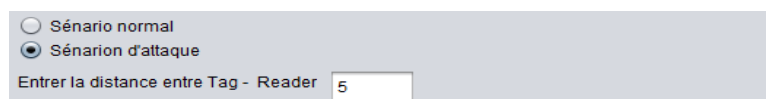


Figure IV- 3 : choix de scénario

- 2) Dans cette partie, le programme le prouveur et le vérificateur génèrent tous les 2 une séquence aléatoire des bits.

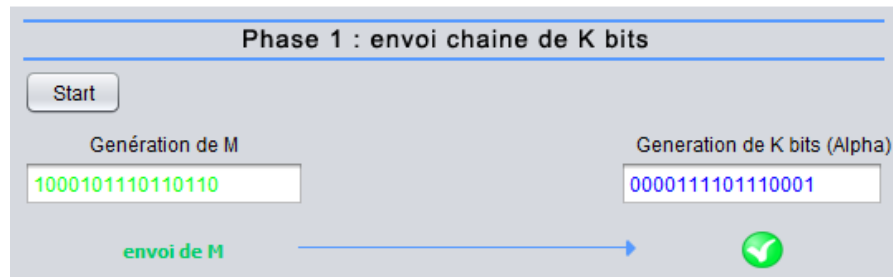


Figure IV- 4 : phases de génération des bits

- 3) Dans cette partie, l'échange rapide de bits peut commencer.

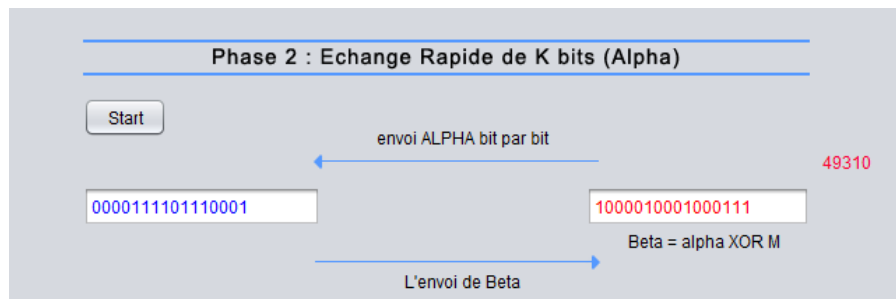


Figure IV- 5 : phases d'échange des bits.

- 4) Dans cette partie, le prouveur concatène α et β et l'envoie chiffré avec la clé secrète au vérificateur

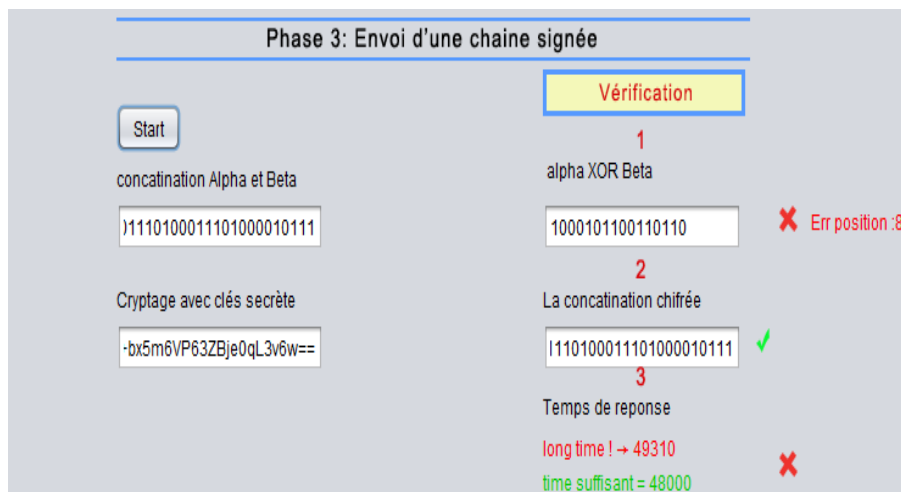


Figure IV- 6 : phases d'échange des bits.

Le vérificateur doit accepter le prouveur si et seulement si $\alpha_i \oplus \beta_i$ est égal à m_i envoyé au début de la communication. Selon l'exemple précédent, l'opération Xor n'est pas correcte, alors Le vérificateur refuse le prouveur.

En plus, le vérificateur vérifie que la concaténation chiffrée reçue est la bonne et correspond bien à la signature du prouveur. Enfin, il vérifie si le temps maximum entre l'envoi de ses bits et le retour est inférieur à une certaine valeur. Dans notre exemple cette condition ne peut être réalisée.

IV.4.3 Interface de protocole Gerhard P. Hancke et Markus G. Kuhn

Cette fenêtre concerne en suite de tâche de la simulation de protocole délimiteurs de distance Gerhard P. Hancke et Markus G. Kuhn .

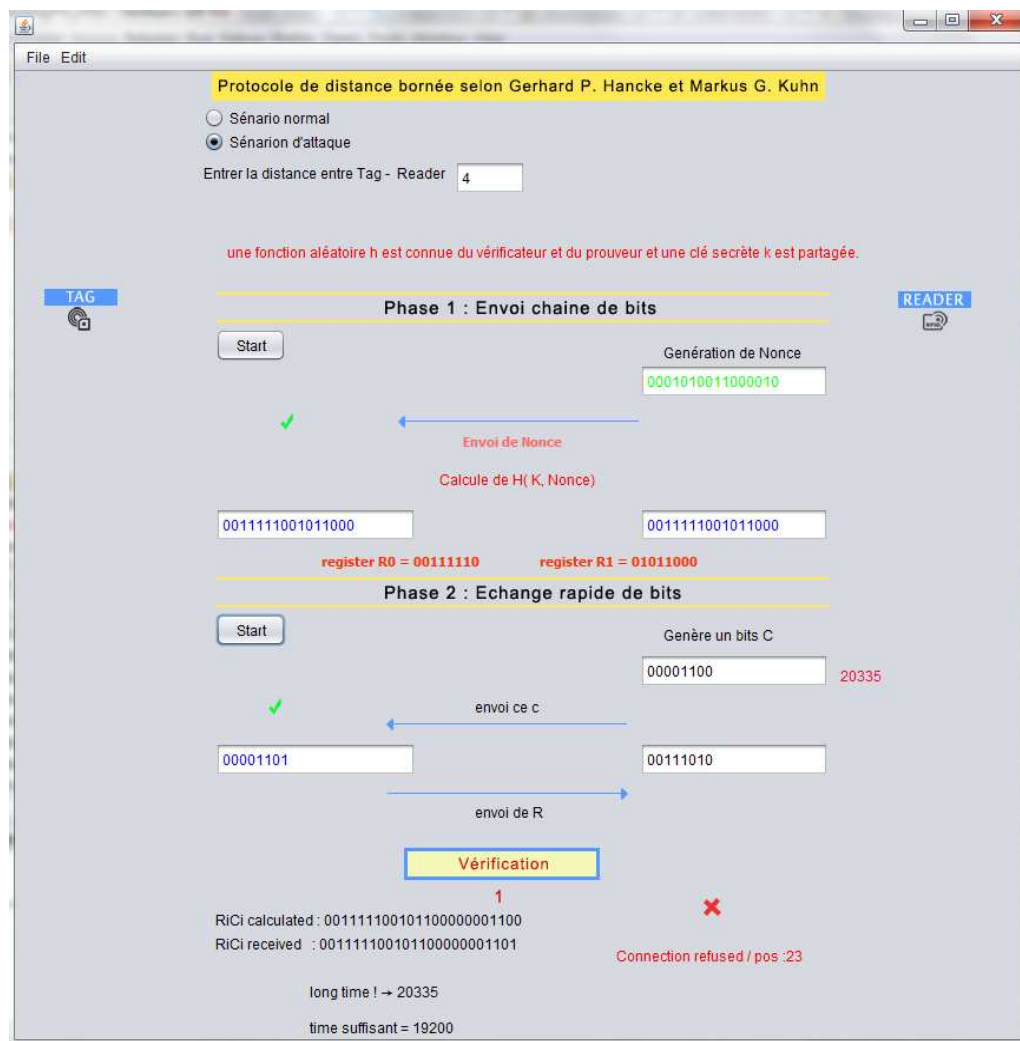


Figure IV- 7 : P. Hancke et Markus G. Kuhn (avec attaque)

Et l'image suivante montre le même protocole sans attaque.

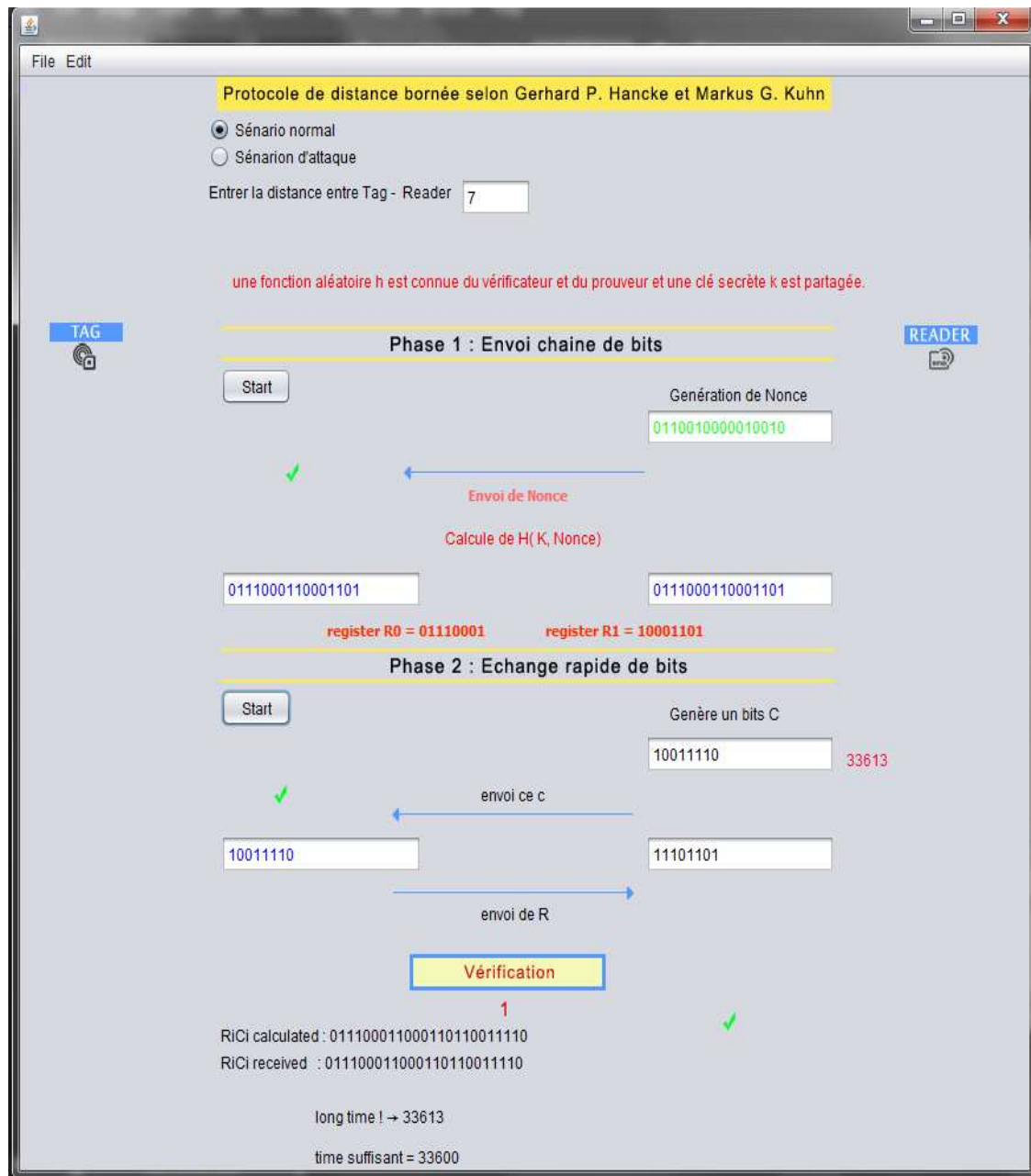


Figure IV- 8 : P. Hancke et Markus G. Kuhn (sans attaque)

Dans ce dernier protocole ,en utilisant l’algorithme de Grain en tant que fonction aléatoire h . Ainsi, la clé secrète k correspond à la clé secrète utilisée dans Grain, N_v correspond au vecteur

d'initialisation utilisé dans Grain. L'algorithme Grain génère donc la suite aléatoire qui sera séparée dans les deux registres R0 et R1.

Voici des exemples d'utilisation du programme :

Bonne vérification :- Du côté Reader :

prover received

RiCi calculated : 01011111101100101000011011001010

RiCi received : 01011111101100101000011011001010

Connection accepted

-Du côté Tag :

Connection accepted

Mauvaise vérification 1 :- Du côté Reader :

prover received

RiCi calculated : 01011111101100101000011011001010

RiCi received : 01011111101100101000011011001010

Connection refused

-Du côté tag :

Connection refused

Explications : On s'aperçoit que la séquence de bit reçue est identique à celle calculée, le problème est que le client a attendu 2 secondes à chaque fois avant de répondre au serveur alors que le serveur autorise un maximum de 1 seconde entre chaque réponse : le client est logiquement refusé.

Mauvaise vérification 2 :- Du côté Reader :

prover received

RiCi calculated : 01011111101100101000011011001010

RiCi received : 11011100010000100101011111111011

Connection refused

-Du côté tag :

./bin/client key_fake.txt IV.txt 50 1

Connection refused

Explications : On s'aperçoit que la séquence de bit reçue est différente à celle calculée malgré le fait que le prouveur réponde assez rapidement aux questions du vérificateur. Le problème vient

de la clé utilisée qui diffère uniquement d'un octet entre celle utilisée pour le client et celle pour le serveur. Le client est logiquement refusé.

IV.4.4 Interface de protocole Swiss-knife

L'image suivante représente l'interface principale de protocole Swiss-knife.

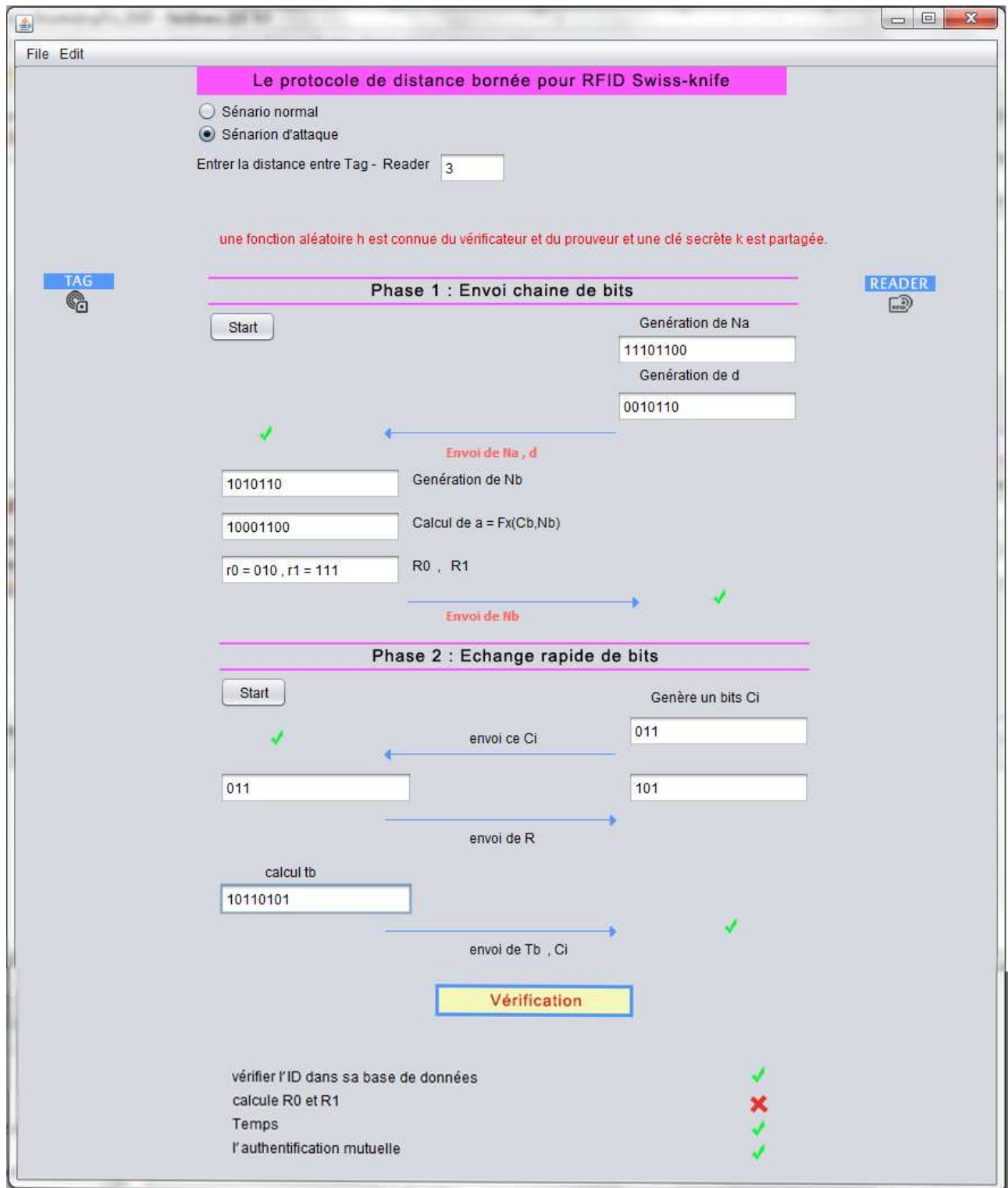


Figure IV- 9 :l'interface de protocole Swiss-knife.

Conclusion

L'identification par radio fréquence est un terrain qui devrait encore être développé dans les années à venir, et plusieurs ingénieurs et chercheurs travaillent déjà sur des standards pour mieux l'encadrer et parvenir à unifier les modulations et techniques pour traiter les informations qui circulent s'appuyant sur ce système.

Comme nous l'avons vu, la sécurité de la technologie RFID est un enjeu important dans l'avenir et de nombreuses personnes travaillent ou ont travaillé sur ce domaine afin de proposer des solutions aux attaques dont cette technologie fait face.

Parmi ces attaques, l'attaque par relais est la plus importante et nécessite des solutions de bas niveaux, car malgré l'utilisation de très bons algorithmes cryptographiques, cette attaque est toujours présente. En effet, elle ne fait que relayer des informations sans avoir à détenir de secrets particuliers.

Pour contrer ces attaques plusieurs protocoles de distance bornée ont été définis. Dans notre mémoire, nous avons étudié 3 protocoles (Hancke et Kuhn, Swiss Knife, Brands et Chaum). Afin d'utiliser ces protocoles, il est nécessaire d'utiliser une fonction pseudo-aléatoire et une fonction de hachage.

Au long de notre travail, nous avons concentré notre étude sur la conception et l'implémentation d'un simulateur. On a utilisé l'environnement de développement EDI NetBeans (langage Java). Parmi les extensions de java largement utilisés, on cite *Java Cryptography Extension (JCE)*. JCE fournit un cadre et la mise en œuvre pour le cryptage, la génération de clé, et le calcul de différents types de fonctions de hachages (e.g SH1, MD5, .. etc.)

Dans notre simulateur en essayer d'atteindre les objectifs suivants :

- Assure le fonctionnement des protocoles de distance bornée des systèmes RFID.
- Faire comparaison entre les différents protocoles étudiés.
-

BIBLIOGRAPHIER

- [1] D. Paret, RFID At Ultra And Super High Frequencies Theory And Application, New York: John Wiley & Sons, 2009.
- [2] D. Bechevet, «Contribution au Developpement de Tag RFID UHF et microondes sur materiaux plastiques,» Thèse de Doctorat, Institut National Polytechnique de Grenoble, 2005.
- [3] Hunt et D. V, «Rfid-A Guide To Radio Frequency Identification,» John Wiley & Sons, 2007.
- [4] O. m. d. douanes, La référence unique de l'envoi (RUE) de l'OMD (Organisation mondiale des douanes), CE RFID, 2004.
- [5] W. Leif et M. Gerhard, «A Roadmap for RFID Applications and Technologies,» 2008. [En ligne]. Available: <http://www.rfid-in-action.eu/public/results/roadmap.html>.
- [6] «<http://www.magellan-rfid.com>,» magellan-rfid, . Available: http://www.magellan-rfid.com/applications/document_tracking.
- [7] AGRIHOUSE, «[agrihouse.com](http://www.agrihouse.com),» Available: <http://www.agrihouse.com>.
- [8] F. Letient, «Etat de l'art et applications des RFID,» Travail d'Etude et de Synthèse Technique, Grenoble, Juin 2008.
- [9] E. P. Morgen, «RFID Tags Guide the Blind,» 1 janv 2008. Available: <http://www.spectrum.ieee.org/biomedical/devices/rfid-tags-guide-the-blind>.
- [10] <http://www.boingboing.net/2008/03/19/bbtv-how-to-hack-an.html>.
- [11] O. Gerd, «Etudes épidémiologiques sur l'incidence des cas de cancer à proximité des antennes relais,» Janv 2008. [En ligne]. Available: http://www.robindestoits.org/Etudes-epidemiologiques-sur-l-incidence-des-cas-de-cancer-1997-2007-a-proximite-d-antennes-relais-par-le-Dr-erd_a349.html.
- [12] CHIKOUCHE Noureddine, «PROBLÈMES DE SÉCURITÉ DANS LES SYSTÈMES EMBARQUÉS », mémoire magistère, septembre 2010 .
- [13] Benoit Chevallier-Mames. « Cryptographie à clé publique: Constructions et preuves de sécurité », thèse Doctorat, Novembre 2006.
- [14] J. Clark and J. Jacob. "A Survey of Authentication Protocol Literature," Rapport technique, University of York, Department of Computer Science, November 1997.
- [15] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22(6), p.p.644-654, November 1976.
- [16] R. Needham and M. Schroeder, "Using encryption for authentication in large networks

- of computers,” Communications of the ACM, vol. 1(12), pp.993–999, 1978.
- [17] G. Lowe. “Breaking and Fixing the Needham-Shroeder Public-Key Protocol Using FDR,” In T. Margaria and B. Steffen, editors, Proceedings of TACAS'96, LNCS 1055, pp. 147.166. Springer-Verlag, 1996.
 - [18] O. Baudron, P. Fouque, D. Pointcheval, G. Poupard and J. Stern, “Practical Multi-Candidate Election System,” Proceedings of the 20th ACM Symposium on Principles of Distributed Computing (august 26 - 29, 2001, Newport, Rhode Island) N. Shavit Ed., p.p.274-283, ACM Press, 2001.
 - [19] J. A. Garay, M. Jakobsson, and P. MacKenzie, “Abuse-free optimistic contract signing,” In Advances in Cryptology Proceedings of Crypto'99, LNCS, vol. 1666, pp. 449-466. Springer Verlag, 1999.
 - [20] M. Steiner, G. Tsudik, and M. Waidner. “Key agreement in dynamic peer groups,” Technical report, Information Sciences Institute, January 1999.
 - [21] A. Fiat and A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems,” In CRYPTO '86, LNCS, vol.263, pp. 186–194, 1986.
 - [22] Gildas Avoine, Mohamed Ali Bingöl, Süleyman Kardas, Cédric Lauradoux et Benjamin Martin, « *A framework for analyzing RFID distance bounding protocols* », Sabanci University Research Database, 24 novembre 2010
 - [23] Gildas Avoine, « *RFID et sécurité font-elles bon ménage* », actes.sstic.org, 2006
 - [24] Yacine Gasmi, Ahmad-Reza Sadeghi, Patrick Stewin, Martin Unger et N. Asokan, « *Beyond secure channels* », ACM DL Library, 2007
 - [25] Carine Boursier, Pierre Girard et Christophe Mourtel, « *Activation des cartes à puce sans contact à l'insu du porteur* », Symposium sur Sécurité des Technologies de l'Information et des Communications, 2008
 - [26] Albert Levi, Erhan Çetintaş, Murat Aydos, Çetin Kaya Koç et Ufuk Çağlayan, « *Relay Attacks on Bluetooth Authentication and Solutions* », Scientific Literature Digital Library and Search Engine, 2004
 - [27] Gerhard Hancke, « *A Practical Relay Attack on ISO 14443 Proximity Cards* », Project report, janvier 2005
 - [28] Aurelien Francillon, Boris Danev et Srdjan Capkun, « *Relay Attack Relay attacks on Passive Keyless Entry and Start Systems in Modern Cars* », Cryptology ePrint Archive, 2010
 - [29] D. Chaum S. Brands. Distance-bounding protocols. in advances in cryptology - eurocrypt 93, volume 765 of lecture notes in computer science, pages 344-359. springer, 1994.
 - [30] M. G. Kuhn G. P. Hancke. An rfid distance bounding protocol. in the 1st international

conference on security and privacy for emergin areas in communications networks (securecomm'05), pages 67-73. ieee computer society, 2005.

- [31] F. Koeune F. Standaert O. Pereira C. Kim, G. Avoine. The swiss-knife rfid distance bounding protocol. 2009.
- [32] P. Rogaway M. Bellare. Entity authentication and key distribution. in advances in cryptology crypto 93, pages 232-249, santa barbara, usa, 1994. springer-verlag – Incs vol. 773.
- [33] L. D. Zuck J. D. Guttman, F. J. Thayer. The faithfulness of abstract protocol analysis : Message authentication. journal of computer security, 12(6) :865-891,2004.
- [34] Audrey COLBRANT, Elodie NOUGUIER, JACOTHELLON (Rapport de projet développé en Java) 2005/2006.
- [35] https://netbeans.org/index_fr.html(11.06.2014)
- [36] <http://searchsoftwarequality.techtarget.com/definition/Java-Cryptography-Extension>, (11.06.2014)

RESUME

L'identification par Radio Fréquence (RFID) est une technologie émergente qui promet d'être omniprésente dans un futur proche, elle permet l'identification d'objets en échangeant des données à travers des signaux Radiofréquence. Cette technologie est en pleine expansion et est utilisée dans de nombreux domaines de la vie courante. Le prix de ce système est variable et peut être peu élevé. Dans ce cas, ses capacités en terme de calculs et de mémoire sont très limitées alors que dans le même temps, nous avons besoin de sécurité et nous avons besoin d'utiliser certaines fonctions cryptographiques.

Pour assurer le fonctionnement d'un protocole et pour assurer l'évaluation de la performance d'un protocole, la manière la moins coûteuse est l'implémentation dans un simulateur. Notre travail s'articule sur la conception et de la réalisation d'un outil de simulation des protocoles de distance bornée des systèmes RFID exigeant les fonctions de hachage et les générateurs des nombres pseudo-aléatoire.

Mots-clés : protocoles de distance bornée, RFID, simulation, attaques par relais.

ملخص

تحديد الهوية بموجات الراديو (RFID) هي تكنولوجيا ناشئة ينتظر انتشارها في كل مكان مستقبلا. تتيح تحديد الكائنات عن طريق تبادل البيانات عبر إشارات الراديو. هذه التكنولوجيا تشهد توسعا سريعا وتستخدم في العديد من مجالات الحياة اليومية. سعر هذا النظام متغير ويمكن أن يكون منخفضا. في هذه الحالة، فقدراتها من حيث الحساب والذاكرة محدودة فلهذا نحن بحاجة إلى الحماية وإلى استخدام بعض وظائف التشفير.

من أجل تقييم أداء البروتوكول فإن الوسيلة المستعملة وبأقل كلفة هي تطويره في تطبيق محاكاة. يركز عملنا على تصميم وإنجاز تطبيق محاكاة لبروتوكولات المسافة المحدودة لـ RFID، والتي تستعمل دوال هاشاج ومولدات الأرقام العشوائية.

كلمات مفتاحية : بروتوكولات المسافة المحدودة، التعريف بترددات الراديو، المحاكاة، هجوم التتابع.

ABSTRACT

The Radio Frequency Identification (RFID) is an emerging technology that promises to be ubiquitous in the near future. it allows the identification of objects by exchanging data through Radio Frequency signals. This technology is rapidly expanding and is used in many areas of daily life. The price of this system is variable and can be low. In this case, its capabilities in terms of computation and memory are very limited while at the same time, we need security and we need to use some cryptographic functions.

To ensure the operation of a protocol and the evaluation of its performance, the cheapest way is the implementation in a simulator. Our work focuses on the design and the implementation of a simulating tool of distance bounding protocols for RFID systems requiring hash functions and generators of pseudorandom numbers.

Key-words: Distance bounding protocols, Radio Frequency Identification (RFID), simulation, relay attack.