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

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
• X ●ΘΛ●ΣX [://:V ●X[●Λ[●O
FACULTE DU GENIE ELECTRIQUE ET INFORMATIQUE

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master en informatique

« Option : Réseaux, Mobilité et système Embarqué »

Thème

Système de détection d'intrusion dans les systèmes RFID

Réalisé et présenté par :

HAMOUME Sylia
MERABET Fatma

Dirigé par :

M^me^ BELKADI Malika

2014/2015

Remerciements

Nous remercions tout d'abord « DIEU » tout puissant de nous avoir donné la santé et le courage d'effectuer ce projet de fin de d'études, dans les meilleures conditions.

Nous tenons aussi à exprimer nos sincères remerciements à notre promotrice M^me^M.BELKADI pour nous avoir proposé ce sujet et de nous avoir dirigés tout au long de sa réalisation.

Nos remerciements vont également aux membres du jury pour l'honneur qu'ils nous font en acceptant d'examiner et juger notre travail.

Nous remercions aussi tous ceux, et celles qui ont participé à l'aboutissement de ce modeste travail.

Merci

Dédicaces

Je dédie notre travail à ma grande famille :

Mes parents, mes frères et mes sœurs (Nadia, Karima, Lila et Dyhia) .

A tout mes neveux et nièces.

A tous mes amis dont (Achour, Smail Nina et Ghiles)

A toutes les personnes qui ont participé de près ou de loin à l'aboutissement de ce travail.

Et surtout à ma meilleure amie et binôme Fatma sans qui ce mémoire n'aurait pas pu être effectué.

Cylia

Dédicaces

Je dédie notre travail à ma petite famille :

Mes chers parents qui m'ont toujours soutenu, mes deux frères Ahmed et Anis

A mes chers grands parents

A toute ma grande famille

A tous mes amis, A tous ceux qui me sont chères. A tous ceux qui m'aiment. A tous ceux que j'aime.

A toutes les personnes qui ont participé de près ou de loin à l'aboutissement de ce travail.

Et surtout à ma meilleure amie et binôme Cylia sans qui ce mémoire

n'aurait pas pu être effectué.

Fatma

Sommaire

Chapitre III : Système de détection d'Intrusion dans les systèmes RFID

Chapitre IV : Le système de détection d'intrusion proposé

Chapitre V : Simulation et étude des résultats

Liste des figures

Chapitre I :

Chapitre II :

Chapitre III :

Chapitre V :

Liste des tableaux

Introduction générale

Introduction générale

Les progrès dans les domaines de télécommunications et de l'électronique ont favorisé l'utilisation croissante du système d'identification par radiofréquences RFID, qui connait aujourd'hui un véritable essor et constitue un exemple typique de technologie pervasive. En effet bien au delà des seuls ordinateurs, de nombreux objets de notre quotidien contiennent des processeurs. Ceux-ci peuvent être nécessaires à leur fonctionnement ou leur fournir de l'information propre de manière à faciliter leur gestion et leur manipulation, c'est le cas des tags RFIDs auxquels il est difficile d'échapper tant qu'ils équipent des entités diverses (automobiles, appareils électroniques, vêtements, livres, ameublement, jouets, emballages alimentaires, animaux …). Ils constituent une sorte de carte d'identité de l'objet en lui attribuant de manière intrinsèque de l'information qu'il est possible de consulter et de modifier à l'aide d'un lecteur.

Malgré la simplicité du concept, l'identification d'objets sans contact suscite de nombreuses inquiétudes tout à fait justifiées. De nombreuses questions se posent tant au sujet de la sécurité que cette technologie apporte qu'au sujet des risques liés à la vie privée qu'elle fait encourir.

Dans les systèmes qui utilisent la technologie RFID, une étiquette clonée peut permettre à un attaquant d'accéder à une installation sécurisée, faire des achats frauduleux, ou perturber les chaînes d'approvisionnement. Les solutions de sécurité dans les systèmes RFID doivent être renforcées pour garantir la sécurité de l'information et empêcher les pirates d'accéder aux données sensibles.

Dans le cadre de ce mémoire, nous proposons d'aborder les aspects de la technologie RFID. Les vulnérabilités de ces systèmes seront passées en revue, les mesures de sécurité mises en œuvre ainsi que différents travaux réalisés. Notre travail est axé sur la conception d'un système de détection d'intrusion, son implémentation et sa réalisation.

Afin de bien mener cette étude, nous avons opté d'organiser notre mémoire en cinq chapitres :

Dans le chapitre I, nous décrivons brièvement les bases de la technologie RFID et ses principales caractéristiques.

Le chapitre II est consacré à la description des problèmes de sécurité auxquels cette technologie est confrontée, il présente les critères généraux de sécurité et les types d'attaque que les RFIDs encourent ainsi que les mesures de sécurité qui ont été prises.

Dans le chapitre III, nous présentons en général ce que sont les systèmes de détection d'intrusion, puis nous donnons un état de l'art sur ces systèmes de détection d'intrusions dans les RFIDs.

Puis le chapitre IV présente la démarche que nous avons suivie pour la conception de notre système de détection d'intrusion, ses objectifs, et son fonctionnement.

Enfin le chapitre V constitue une synthèse de notre travail par l'implémentation, la simulation de notre système et la présentation des résultats relevés.

Chapitre I : Généralités sur les systèmes RFID

Chapitre I : Généralités sur les systèmes RFID

1. Introduction :

L'identification et le suivi des objets deviennent de plus en plus nécessaires dans notre vie quotidienne. Chaque objet manufacturé se voit attribuer un identifiant unique. Cet identifiant ne se présente plus sous une forme graphique mais électronique, il est capable de communiquer sans fil avec des lecteurs appropriés.
La RFID (Radio Frequency Identification) est une technologie alliant la flexibilité d'utilisation des ondes radiofréquences au faible coût des codes-barres. Basée sur la transmission d'ondes RF (Radio Fréquence), elle se présente comme une réponse pertinente, afin de palier au principal besoin de traçabilité, qui est définie comme étant la gestion des mouvements, l'aptitude à retrouver l'historique, l'utilisation ou la localisation d'un article ou d'une activité, au moyen d'une identification enregistrée (ISO 8402)[1]
Ce premier chapitre, est dédié à une présentation générale de la technologie RFID et ses principales caractéristiques.

2. Définition de la RFID :

La radio-identification, plus souvent désignée par le sigle RFID (radio frequency identification) est une méthode développée pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (RFID-tag ou RFID-transponder). Ces radio-étiquettes peuvent être collées, incorporées dans des objets ou des produits, voir implantés dans des animaux. Ainsi, la RFID fait partie des technologies d'identification automatique, au même titre que la reconnaissance optique de caractères ou de codes barre.

3. Historique :

La technologie RFID a connu ses premiers pas dans les années 40, elle fut inventée au Royaume-Uni en 1939. Les RFID se sont ensuite développées comme suit :

1940
la notion de RFID (identification par fréquences radio) est apparue la première fois lors de la seconde Guerre Mondiale ; elle est directement liée au développement de la radio et du radar. Pour identifier des appareils en vol dans l'espace aérien britannique (IFF : Identifie Friendly Foe), les alliés mettaient en place dans leurs avions des transpondeurs (sorte d'imposantes balises) afin de répondre aux interrogations de leurs radars. De nos jours, le contrôle du trafic aérien reste basé sur ce principe.

1970
Les systèmes RFID durant la période allant de 1969 à 1979 restent utilisés de manière restreinte, principalement à usage militaire pour le contrôle d'accès aux sites sensibles, comme le secteur nucléaire.

1980
Les avancées technologiques permettent l'apparition du tag passif. Le tag RFID rétromodule l'onde rayonnée par l'interrogateur pour transmettre des informations. Cette technologie

[1] ISO 8402, « Vocabulaire pour le management et l'assurance de la qualité », AFNOR (Association Française de Normalisation) 1994.

permet de s'affranchir de source d'énergie embarquée sur l'étiquette réduisant de ce fait son coût et sa maintenance.

1990
Début de la normalisation pour une interopérabilité des équipements RFID.

1999
Fondation par le MIT (Massachusetts Institute of Technology) de l'Auto-ID center : centre de recherche spécialisé en identification automatique (entre autre RFID).

2004
L'auto-ID du MIT devient "EPCglobal", une organisation chargée de promouvoir la norme EPC (Electronic Product Code), sorte de super code barre stocké dans un tag RFID. Cette norme est élaborée par les universitaires et adoptée par l'industrie.

A partir de 2005
Les technologies RFID sont aujourd'hui largement répandues dans quasiment tous les secteurs industriels (aéronautique, automobile, logistique, transport, santé, vie quotidienne, etc.). L'ISO (International Standard Organisation) a largement contribué à la mise en place de normes tant techniques qu'applicatives permettant d'avoir un haut degré d'interopérabilité voire d'interchangeabilité.

2009

Création du Centre National de Référence RFID (CNRFID)[2]

4. Le code barres :

Un code à barres souvent appelé « code barre », représente la codification d'une information. Variant selon les algorithmes de codage, cette codification est optimisée selon les besoins pour encoder du texte, des chiffres, des caractères de ponctuation ou encore une combinaison de ces derniers.

La représentation obtenue est optimisée pour une lecture optique. Le contraste comme source d'information. Lors du passage d'une source lumineuse sur les barres sombres et claires d'un code à barres, l'intensité lumineuse varie. Celle-ci, captée par un capteur photosensible, est amplifiée, filtrée et digitalisée pour être convertie en information numérique qu'un décodeur retranscrit en caractères ASCII directement exploitable à un système informatique par le biais d'une liaison hertzienne ou filaire.

Voici les trois types de codes barres les plus utilisés :

- les codes barres unidimensionnels ou linéaires ;

[2] Le Centre National RFID (Association loi 1901) a été mis en place fin 2008 à l'initiative du Ministère de l'Economie, des Finances et de l'Emploi (MINEFE) qui a pour objectif d'encourager le déploiement de solutions RFID et de développer les partenariats entre les offreurs de solutions, les utilisateurs, les laboratoires de recherche et les institutions.

- les codes barres linéaires empilés ;
- les codes barres à deux dimensions.

Le code barre le plus courant est le code EAN (European Article Number) -figure I.1-, crée pour répondre aux besoins de l'industrie alimentaire en 1976. Le code EAN est une évolution de l'UPC (Universal Product Code) américain, introduit aux ´Etats-Unis dès 1973 ; UPC et EAN sont compatibles entre eux.

Figure I.1 : Un code barre EAN (European Article Number)

5. Les RFID vs le code barres :

Ces deux technologies possèdent leurs avantages et inconvénients distincts en fonction des applications pour lesquelles elles sont envisagées :

- En terme de visibilité le tag peut être dissimulé ou intégré à l'intérieur d'un objet et le code barres doit être obligatoirement visible car ils ne peuvent être lu qu'au contacte du lecteur.
- Une seule lecture d'une étiquette code barre se fait à la fois, chaque code à barres doit être orienté de manière particulière face au lecteur alors que dans les RFID plusieurs étiquettes peuvent être lu à la fois quelque soit leur orientation par rapport au lecteur.
- En terme de lecture/ écriture et stockage d'information, les étiquettes RFID ont une grande capacité de stockage et peuvent être lues, écrites ou modifiées. Par contre les étiquettes code barres ne peuvent être que lues et le stockage d'information est restreint.
- Concernant la sécurité de l'information, la technologie RFID offre la possibilité de protéger l'information par différents moyens comme l'ajout de mot de passe et le cryptage des données ce qui n'est pas possible pour le code barres ce qui limite la sécurité et facilite la reproduction et la contrefaçon.

6. Les composants d'un système RFID : [1]

Un système RFID se compose principalement d'un ou plusieurs lecteurs, d'une ou plusieurs étiquettes (tags) et d'un logiciel d'application (middleware). La figure 2 décrit le schéma général d'un système RFID. Le lecteur agit généralement en maître par rapport au tag; si le tag est dans la zone de lecture du lecteur, ce dernier l'active en lui envoyant une onde électromagnétique puis entame la communication et l'échange des données. Le lecteur est relié à un hôte d'application qui récupère l'information pour le logiciel d'application. Un lecteur RFID est donc chargé de l'interface avec le système global relatif à l'application et de la gestion de l'identification des tags qui se présentent à lui. Le tag est, quand à lui, constitué d'une antenne et d'une puce électronique miniature.

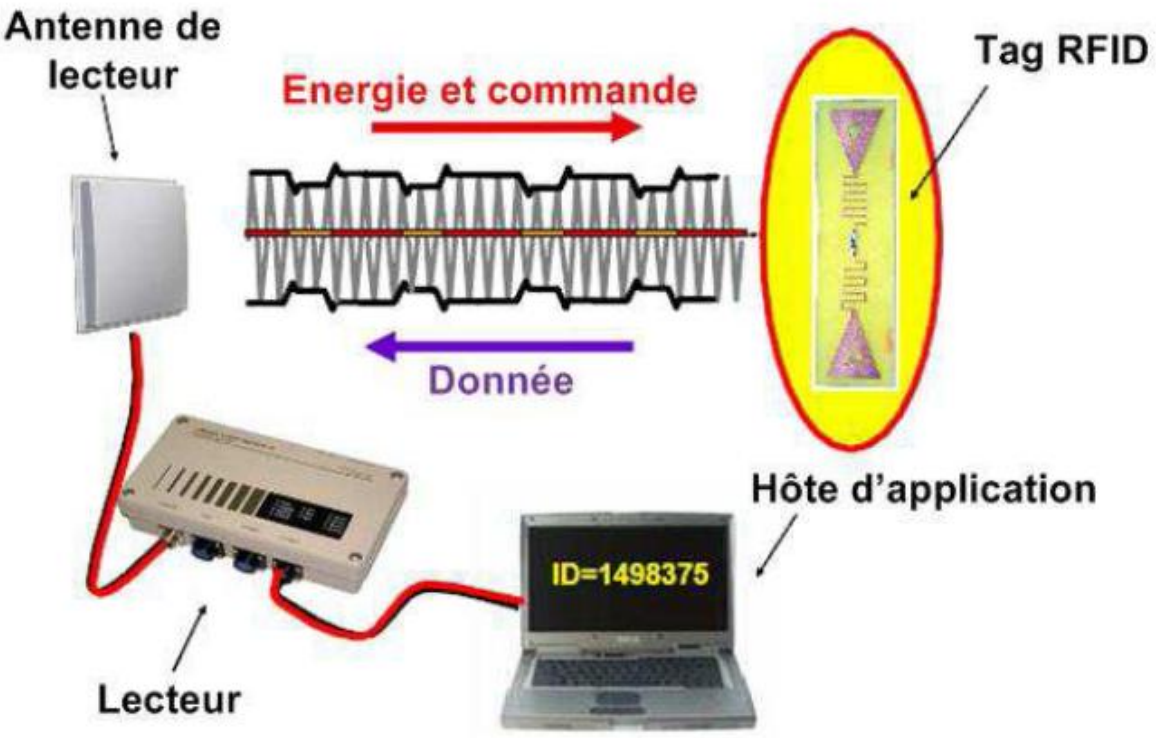


Figure I.2 : Eléments d'un système RFID [2]

La liaison entre le lecteur et l'hôte de l'application peut être une liaison sans fil. Le lecteur interroge les étiquettes passives ou semi-actives en leurs envoyant la commande et l'énergie nécessaire pour interagir avec lui et dans le cas où le tag est actif c'est à dire possède sa propre batterie il peut initier la communication en premier.

6.1 L'étiquette :

L'étiquette (tag) appelée aussi transpondeur, pour transmitter–responder comprend une puce, dotée d'une mémoire et d'un microprocesseur, reliée à une antenne bobinée et lue par un lecteur captant et transmettant l'information.

Ces tags peuvent alors être incorporés dans des objets ou être collés sur des produits. Le format des données inscrites sur les étiquettes est standardisé à l'initiative d'EPC Global (Electronic Product Code).

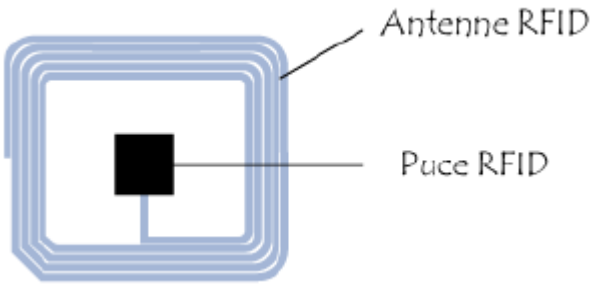


Figure I.3 : l'étiquette RFID

6.2 Le lecteur :

Le lecteur RFID est un émetteur-récepteur radio spécialisé. Il doit générer des signaux à la fréquence porteuse et moduler ces signaux pour transmettre des informations aux tags. Il doit recevoir et identifier sélectivement des réponses à partir des tags. Pour cela, il est doté de circuits de démodulation et de fonctions de traitement lui permettant d'adresser et de communiquer sélectivement et individuellement avec tout tag dans son champ de lecture.

Ainsi le lecteur RFID est l'élément responsable de la lecture des tags radiofréquence et de la transmission des informations qu'elles contiennent (code EPC, information d'état, clé cryptographique…) vers le niveau suivant du système (middleware).

6.3 Le middleware (ou intergiciel) : [3]

Un middleware, est un logiciel intermédiaire entre le réseau et le matériel d'une part, et les applications d'autre part. Cet intergiciel permet de collecter, de filtrer et d'agréger les données. Cela permet aussi une gestion des différents lecteurs plus facile.

Un intergiciel pour étiquettes électroniques est un logiciel tiers destiné à simplifier l'accès et l'exploitation des informations stockées dans des étiquettes RFID.

Le but d'un intergiciel entre le réseau et les applications est d'accomplir les taches techniques et les échanges des données. Dans les systèmes RFID, un intergiciel doit gérer les lecteurs, souvent hétérogènes, doit traiter les évènements issus des lecteurs RFID, et doit être connecté aux applications. Dans certains cas, il n'y a pas besoin d'intergiciel, comme dans le cas d'une petite et unique application telle que « compter le nombre d'identifiants lus », ou encore « lire les étiquettes dans le champs du lecteur »

7. **Les types des RFIDs et leurs spécificités techniques** :

Il existe 3 types de transpondeurs : [4]

7.1 Transpondeurs passifs : ce sont les moins chers aujourd'hui. Ils ne possèdent pas leur propre alimentation en énergie et ne sont donc activés que par le signal du lecteur qui leur sert d'alimentation en énergie. On dit que le transpondeur est téléalimenté. Le tag ne peut pas émettre de signaux par lui même sans être préalablement interrogé par le lecteur.

7.2 Transpondeurs semi-passifs : possédant sa propre source d'alimentation en énergie, cela permet d'augmenter les distances de communication, mais fait également augmenter le coût et la taille du transpondeur. En revanche, ces transpondeurs ne peuvent toujours pas émettre de signaux eux même.

7.3 Transpondeurs actifs : ces derniers possèdent un émetteur à haute fréquence ce qui leur donne la possibilité d'émettre sans être obligatoirement interrogés préalablement par lecteur. Pour pouvoir émettre de lui même ce transpondeur a besoin d'énergie, c'est pourquoi il embarque un système d'alimentation. Il permet donc une plus grande distance de communication.

8. Fonctionnement des systèmes RFIDs :

8.1 Puce RFID :

La technologie des puces d'identification RFID est très étendue, elle permet de s'adapter à des multitudes de situations, l'identification, et d'embarquer d'autres informations sur le transpondeur. Mais le besoin de chaque entreprise étant différent, il existe différents modes de fonctionnement des transpondeurs que l'on peut regrouper sous trois différentes catégories :

- ❖ Les puces à usage unique (lecture seule) : la puce contient des données qui sont lues par le lecteur RFID sans possibilité de les modifier. c'est le mode de fonctionnement le plus simple du transpondeur et qui sert principalement pour les problèmes traitant seulement d'identification. Le transpondeur peut être lu uniquement par le lecteur, le transpondeur possède juste les informations qui ont été écrites par le fabriquant du tag. Ces informations peuvent être choisies par l'entreprise, mais une fois ces informations écrites, le transpondeur ne peut être que lu.

- ❖ Les puces réinscriptibles (lecture/écriture) : les données inscrites sur la puce peuvent être modifiées par le lecteur RFID selon les deux modes suivants :

• Lecture/écriture unique : ce mode de fonctionnement est similaire à la lecture seule sauf que cette fois ci, le transpondeur livré par le fabriquant est vierge, il ne contient aucune information. C'est l'acheteur du transpondeur qui va pouvoir écrire des informations dessus. Les informations ne peuvent être écrites qu'une seule fois, ensuite le transpondeur se comporte comme un transpondeur en lecture seule.
• Lecture/écriture multiple : dans ce mode de fonctionnement, le transpondeur peut être livré vierge ou avec des informations. Mais les informations peuvent être effacées et réécrites par l'acheteur du transpondeur presque autant de fois qu'il le souhaite. Ce type de transpondeur est très utile lorsque l'on vient écrire des informations à différents moments d'un processus ou bien lorsque l'on souhaite réutiliser les transpondeurs avec de nouvelles informations.

8.2 Antenne RFID :

L'antenne RFID est un élément primordial du système RFID qui est généralement intégré au lecteur RFID et à l'étiquette RFID, elle permet de transmettre les informations et d'activer les tags afin de recevoir des données dans le cas des étiquettes passives et semi-passives.

Le choix du type de l'antenne à intégrer au lecteur RFID diffère selon le type de lecture, le type d'étiquette, l'utilisation du système RFID, etc. Ainsi, deux types principaux d'antennes se distinguent :

- les antennes intégrées : elles sont intégrées au lecteur, leur utilisation est conseillée pour les lecteurs de basse fréquence à portée limitée.

- les antennes externes : elles ne font pas partie du lecteur, elles sont plus puissantes et s'avèrent donc utiles pour obtenir une plus grande portée.

9. Les gammes de fréquences RFID [6] :

Les systèmes RFID génèrent et réfléchissent des ondes électromagnétiques. Les systèmes RFID doivent notamment veiller à ne pas perturber le fonctionnement des autres systèmes radio. On ne peut, en principe, utiliser que les plages de fréquences spécifiquement réservées aux applications industrielles, scientifiques ou médicales. Ces plages de fréquences sont appelées ISM (Industriel – Scientifique – Médical). Les principales plages de fréquences utilisées par les systèmes RFID sont données dans le tableau suivant

Fréquences	Caractéristiques	Applications
Basses Fréquences 125 Khz	Distance de lecture moyenne (10 à 150 cm) Rapidité de lecture moyenne	Identification d'animaux Pas de lecture/écriture Pas de gestion de l'anticollision
Hautes Fréquences 13,56 Mhz	Distance de lecture faible Quelques centimètres (à puissance d'émission égale)	Contrôle d'accès Lecture/écriture facilités
Très Hautes Fréquences 900 Mhz	Grande distance de lecture Jusqu'à 5 mètres Vitesse de lecture importante	Logistique, gestion de stocks multiples, sans collision Gestion de palettes
Ultra Hautes Fréquences 2 ,4 Ghz	Très grande vitesse de lecture Très grande distance de détection (>10 mètres)	Péage d'autoroute Tag alimenté (actif)

Tableau I.1 : tableau des gammes de fréquences utilisées par la technologie RFID [7]

10. Les normes RFID :

Pour une interopérabilité, les équipements RFID (lecteurs et tags) doivent impérativement être normalisés quant à leur mode de fonctionnement soit, pour une fréquence d'utilisation donnée, que n'importe quel tag soit lu par n'importe quel lecteur. On parle alors de protocole de communication.
Le développement de standards est la responsabilité du comité technique de l'ISO.
L'ISO est l'union internationale des institutions nationales de standardisation, comme la DIN (Allemagne), l'ANSI (USA), l'AFNOR (France) ou la SNV (Suisse).
Les tags RFID fonctionnent selon des normes comme l'ISO 14443 (13.56 MHz) ou EPCglobal 96-bits (915 MHz).

11. Classement des étiquettes RFID selon EPC Global :

Le standard EPC Global de deuxième génération distingue quatre classes de tags :
La classe 1 correspond aux tags les moins performants et donc les moins chers. Ils sont dotés d'une mémoire accessible en lecture seulement, qui contient un identifiant unique (typiquement 128 bits). Lorsque le tag est interrogé par un lecteur, il envoie simplement son identifiant. Les tags de classe 1 se trouvent dans les bibliothèques, les chaînes logistiques, etc.
La classe 2 permet d'implémenter des fonctions sur le tag, typiquement un algorithme cryptographique symétrique et de posséder quelques centaines de bits de mémoire réinscriptible. Cependant, les tags des classes 1 et 2 sont passifs c'est-à-dire qu'ils ne possèdent pas de batterie et doivent donc être présents dans le champ du lecteur pour communiquer. Ces tags ont une distance de communication relativement faible : quelques décimètres en haute fréquence et jusqu'à quelques mètres en ultra-haute fréquence. On considère enfin que leur résistance aux attaques physiques est très limitée : on admet généralement qu'une même information secrète ne doit pas être partagée par plusieurs tags pour limiter les conséquences d'une telle attaque.
Les tags de classe 3 sont semi-passifs, c'est-à-dire qu'ils possèdent une source d'´energie interne pour réaliser des calculs, mais l'´energie apportée par le lecteur est toujours nécessaire pour la communication.
Enfin, les tags de classe 4 sont actifs, possédant une batterie utilisée à la fois pour les calculs et la communication, ce qui leur permet d'initier eux-mêmes des échanges avec un lecteur et de posséder une distance de communication plus importante. Le standard [5] considère également que les tags de classe 4 peuvent communiquer entre eux.

12. Les applications de la technologie RFID :[8]

Les applications des étiquettes RFID sont déjà très nombreuses. Voici listées quelques applications possibles avec les puces RFID ainsi que quelques images illustrant différents exemples d'utilisation de la technologie RFID dans la figure I.4 :

- Traçabilité d'objets tels que les livres (bibliothèque, librairie...).
- Traçabilité d'objets en zone de douanes
- Traçabilité des bagages en zone aéroportuaire
- Marquage des produits dans les grandes surfaces (lutte contre le vol)
- Contrôle d'accès à partir de badges
- Titre de transport
- Gestion de parc de location de véhicules (autolib, vélib...)
- Identification des animaux (chat, chien, vache....).
- Contrôle des performances des athlètes dans des compétitions de masses (marathon) où il est impossible du fait de la densité de faire un contrôle individuel.
- Des puces sous-cutanées sont implantées aussi chez l'être humain: accès à des sites hautement sécurisés.
- Dans le domaine médical comme le contrôle et la surveillance des patients.

Identifier les animaux, suivi alimentation, vaccination, production laitière…

Contrôler l'accès de véhicule

Badge cantine

Contrôle des temps de passage dans des compétitions de masse

Figure I.4 : Exemples d'application de la technologie RFID

13. Avantages et inconvénients : [6]

13.1 Les avantages :

La capacité de mise à jour du contenu par les intervenants à la différence du code à barres pour lequel les données sont figées une fois imprimées ou marquées, le contenu des données stockées dans une étiquette radio fréquence va pouvoir être modifié, augmenté ou diminué par les intervenants autorisés (étiquettes en lecture et écriture multiple).

13.1.1 Une plus grande capacité de contenu

Dans une étiquette radiofréquence une capacité de 1000 caractères est aisément stockable sur $1mm^2$, et peut atteindre sans difficulté particulière 10000 caractères. Dans une étiquette logistique apposée sur une palette, les différentes unités contenues et leurs quantités respectives pourront être enregistrées et lues.

13.1.2 La vitesse de marquage

Le code à barres dans un contexte logistique nécessite le plus souvent l'impression d'un support papier. La manipulation et la pose des étiquettes restent des opérations manuelles ou mécaniques. Les étiquettes radio fréquence peuvent être inclues dans le support de manutention ou dans les conditionnements dès l'origine. Les données concernant les objets contenues ou transportées sont écrites en une fraction de seconde au moment de la constitution de l'unité logistique ou de transport, sans manipulation supplémentaire.

13.1.3 Une sécurité d'accès au contenu

Comme tout support numérique, l'étiquette radio fréquence peut être protégée par mot de passe en écriture ou en lecture. Les données peuvent être chiffrées. Dans une même étiquette, une partie de l'information peut être en accès libre, et l'autre protégée. Cette faculté fait de l'étiquette RF, un outil adaptée à la lutte contre le vol et la contrefaçon.

13.1.4 Une plus grande durée de vie

Dans les applications où un même objet peut être utilisé plusieurs fois, comme l'identification des supports de manutention, ou la consignation du contenant, une étiquette radio fréquence peut être réutilisée 1 000 000 de fois.

13.1.5 Une plus grande souplesse de positionnement

Avec l'étiquette radio fréquence, il est possible de s'abstraire des contraintes liées à la lecture optique, elle n'a pas besoin d'être vue. Il lui suffit d'entrer dans le champ du lecteur pour que sa présence soit détectée.

13.1.6 Une moindre sensibilité aux conditions environnementales

Les étiquettes RFID n'ont pas besoin d'être positionnées à l'extérieur de l'objet à identifier. Elles peuvent donc être mieux protégées des agressions liées aux stockages, aux manutentions ou au transport. De plus leur principe de fonctionnement ne les rend pas sensibles aux souillures, ou taches diverses qui nuisent à l'utilisation du code à barres.

13.2 Les inconvénients :

13.2.1 Les prix restent nettement supérieurs à ceux des étiquettes code à barres pour des unités consommateurs.

Utiliser les étiquettes radio fréquence en lieu et place du code à barres sur les produits de grande consommation, n'est donc pas aujourd'hui économiquement réaliste. Cela le devient pour lutter contre le vol ou la contrefaçon sur les produits à forte valeur ajoutée, ou pour tracer les produits dans le cadre du service après-vente, comme l'électroménager. Par contre au-delà du conditionnement unitaire, le coût de l'étiquette radio fréquence peut devenir marginal par rapport à la valeur des produits contenus.

13.2.2 La perturbation par l'environnement physique

La lecture des étiquettes radio fréquences est perturbée par la présence, par exemple, de métaux dans leur environnement immédiat.

13.2.3 Les perturbations induites par les étiquettes entre elles

Dans de nombreuses applications, plusieurs étiquettes radio fréquences peuvent se présenter en même temps dans le champ du lecteur volontairement ou involontairement. Ceci peut être voulu en magasin, au moment du passage à la caisse ou entre les portiques antivol.

13.2.4 La sensibilité aux ondes électromagnétiques parasites

Les systèmes de lecture RFID sont dans certaines circonstances sensibles aux ondes électromagnétiques parasites émises par des équipements informatiques (des écrans d'ordinateurs) ou des systèmes d'éclairages plus généralement par les équipements électriques. Leur emploi doit donc être testé en tenant compte de l'environnement.

13.2.5 Les interrogations sur l'impact de la radio fréquence sur la santé

Cette question fait débat depuis quelques années, en particulier concernant les portiques antivol et les téléphones portables. Les étiquettes passives ne présentent aucun risque quel que soit leur nombre puisqu'elles ne sont actives que lorsqu'elles se trouvent dans le champ d'un lecteur. Les études portent donc essentiellement sur les lecteurs et visent à définir les critères de régulation de leur puissance d'émission afin d'éviter qu'ils ne créent des perturbations sur les équipements de santé tels que les pacemakers (stimulateur cardiaque), mais aussi sur l'organisme humain.

13.2.6 Sécurité et vie privée

L'utilisation d'ondes électromagnétiques pour transmettre des données entre deux dispositifs rend cette technologie intrusive et vulnérable aux attaques basées sur l'utilisation de la radiofréquence.

14. <u>Conclusion :</u>

Dans ce chapitre nous avons présenté en premier lieu le principe de l'identification par radio fréquence et sa progression au fil des années. Nous avons décrit les composants constituants un système complet RFID et le principe de leur fonctionnement. Par la suite nous avons cité brièvement quelques applications ainsi que les avantages et les inconvénients de cette technologie. Dans le chapitre suivant nous allons aborder la sécurité dans les systèmes RFIDs.

Chapitre II : La sécurité dans les systèmes RFID

1. Introduction :

Au cours de ces dernières années, les progrès de l'IDentification par Radio Fréquence (RFID) a conduit à leur adoption généralisée dans diverses applications telles que l'identification des objets, autorisation d'accès, surveillance de l'environnement, la gestion de la chaîne d'approvisionnement…etc.

La technologie RFID est parvenue à un stade de développement où la sécurité de l'information et la protection de la vie privée ont été reconnues comme des obstacles à la généralisation de son utilisation.

Les solutions de sécurité dans les systèmes RFID doivent être renforcées pour garantir la sécurité de l'information et empêcher les pirates d'accéder aux données sensibles.

Ce chapitre décrit les problèmes de sécurité auxquels cette technologie est confrontée, il présente les critères généraux de sécurité et les types d'attaques aux quelles les RFIDs sont confrontés ainsi que les mesures de sécurité qui ont été mises en œuvre.

2. Classification des applications selon les besoins de sécurité :[9]

Outre la classification des tags, il est essentiel de classer les applications en fonction de leurs objectifs. Un protocole pour identifier des objets dans une chaîne logistique n'aura en effet pas les mêmes besoins qu'un protocole de contrôle d'accès. On distingue ainsi deux grandes catégories d'applications [10] : celles dont l'objectif est uniquement d'apporter des fonctionnalités nouvelles ou d'améliorer des fonctionnalités existantes (tri sélectif de déchets, remplacement des codes-barres, tatouage du bétail, etc.) et celles dont l'objectif est d'apporter de la sécurité (badge d'accès à un immeuble, clef de démarrage d'une voiture, abonnement aux transports publics, etc.).

Dans le premier cas, le but du protocole est d'obtenir l'identité de l'objet interrogé mais aucune preuve de cette identité n'est requise : c'est *un protocole d'identification*. Ce type de protocole est a priori suffisant pour la majorité des applications. Il est par exemple suffisant lorsque la RFID est utilisée pour identifier des objets dans une chaine logistique, en remplacement des codes-barres.

Dans le second cas, il est important qu'une preuve de l'identité soit fournie : c'est un *protocole d'authentification*. Par abus de langage, protocole RFID désigne aussi bien un protocole d'identification qu'un protocole d'authentification. Notons que s'il ne semble pas y avoir de problème de sécurité au sens strict dans le cas du protocole d'identification, en revanche, celui-ci est, comme le protocole d'authentification, sujet aux problèmes liés à la vie privée.

Les deux catégories de protocoles sont illustrées dans les figures suivantes : [11]

Figure II.1 : identification par RF

Figure II.2 : authentification par RF

Identification : Obtenir Identité du tag.
Authentification: Obtenir Identité + Preuve du tag.

3. Critères généraux de sécurité :

Les besoins de sécurité sont généralement classés suivant les critères suivants :

3.1 *La confidentialité :* c'est la garantie que seules des personnes autorisées ont accès et donc connaissent ou utilisent des objets considérés : données, messages ou contenu de messages, services ou fonctionnalités.

3.2 *L'intégrité :* c'est la garantie que les objets considérés sont exacts et complets, ce qui inclut la garantie que seules des personnes autorisées ont pu modifier ces objets.

3.3 *L'accessibilité :* c'est la garantie que les objets considérés sont accessibles et disponibles, mais aussi opérables avec des interfaces standards au moment voulu par les personnes autorisées ; ceci implique, entre autres, que l'infrastructure et les techniques employées passent à l'échelle en nombre d'utilisateurs.

3.4 *L'imputabilité(ou la non-répudiation de l'information):* c'est la garantie que l'auteur d'un objet ne puisse prétendre ensuite qu'il n'en est pas l'auteur, ou bien la garantie que le destinataire d'un message ne puisse prétendre qu'il ne l'a pas reçu ; ceci peut donc nécessiter l'intégrité, l'accessibilité et la traçabilité des objets, c'est à dire la garantie que les accès et tentatives d'accès aux objets considérés sont tracés et que ces traces sont conservées, exploitables et accessibles (un critère connexe à ceux de traçabilité et d'accessibilité est celui de transparence[1]).

[1] Une transmission est transparente si elle ne modifie pas les informations transmises. La transparence peut être sémantique (les valeurs binaires sont toutes conservées), ou temporelle (les intervalles de temps entre les bits sont conservés).

4. Classification des attaques :[12]

Une attaque peut être définie comme toute action ou ensemble d'actions qui peut porter atteinte à la sécurité des informations d'un système ou d'un réseau informatique.
Vu le nombre important d'attaques possibles, elles peuvent être classées selon différents critères :

La première classification

- ***Les attaques passives :*** ce type d'attaques vise l'obtention d'accès pour pénétrer dans le système sans compromettre ses ressources.
- ***Les attaques actives :*** le résultat de ce type d'attaques est le changement non autorisé d'états des ressources du système.

La deuxième classification

- ***Les attaques internes*** : ce type d'attaques est causé :

1. Soit par les utilisateurs autorisés du système qui essayent d'utiliser des privilèges complémentaires dont ils n'ont pas le droit.
2. Soit par les utilisateurs autorisés qui emploient improprement les privilèges dont ils ont le droit.

- ***Les attaques externes*** **:** ce type d'attaques est causé par des utilisateurs externes qui essayent d'accéder à des informations ou des ressources d'une manière illégitime et non autorisée.

La troisième classification

Selon cette classification, les attaques de cette catégorie peuvent porter atteinte à :

- *La confidentialité* des informations en brisant les règles privées.
- *L'intégrité* en altérant les données.
- *La disponibilité* en rendant un système ou un réseau informatique indisponible. Ces attaques sont connues sous le nom des attaques de déni de service.
- *L'authenticité* des informations.

5. Types d'attaques dans les systèmes RFID : [13][14]

Une intrusion ou une attaque à un ordinateur sur un réseau traditionnel a une limitation physique en raison de liens réseau physiques. Un intrus qui tente d'effectuer une attaque nécessite soit une certaine connexion physique au réseau via un câble réseau ou via l'accès à une borne (terminal) sur le réseau de la victime. Ces attaques peuvent être traçables par la détection du trafic sur certaines liaisons du réseau ou bien du traçage avec des adresses IP, etc. Cependant, un accès malveillant aux nœuds de calcul dans un environnement RF ouvert, tels que la RFID, réseau de capteurs sans fil, ou un autre réseau sans fil ou RF n'est pas facile à détecter et difficile à suivre. Par exemple, les données circulant dans l'air, sont facilement détectables par de nombreux appareils non sécurisés. En conséquence, il existe une forte demande pour accroître la sécurité et la confidentialité des réseaux RFID. Pour comprendre les attaques potentielles aux réseaux RFID nous avons résumé plusieurs attaques communes dans ce qui suit.

5.1 Surveillance non autorisée (Eavesdropping) :

Un observateur non autorisé tente de saisir les informations échangées entre lecteurs et étiquettes sans permission, c'est une attaque passive. La communication RFID se produit dans l'air et est donc une cible facile pour un espion de surveiller des données transmises sans être

détecté. En conséquence, l'information (d'entreprise ou personnelle) sensible peut être capturée, enregistrée et analysée par un utilisateur malveillant. Afin de prévenir ce type d'attaque, les algorithmes de chiffrement et de déchiffrement sont utilisés pour suggérer de bonnes méthodes, le cryptage des données tel que le cryptage AES (Advanced Encryption Standard qui est un algorithme de chiffrement symétrique.) est souvent trop cher pour les étiquettes RFID passives

Contre-mesures :

Une des façons les plus faciles de prévenir l'écoute des systèmes est de crypter leurs données lors de la communication avant de les envoyer sur la liaison sans fil. De cette façon, les intrus peuvent être en mesure d'entendre la communication, mais pas la déchiffrer.

Cette méthode permet également d'inclure la protection contre le filtrage en exigeant la connaissance d'une clé secrète pour décrypter les messages provenant de l'étiquette.

5.2 Spoofing :

Dans l'attaque de spoofing, un dispositif malveillant peut cloner une étiquette existante pour interagir de manière fiable avec un lecteur. Par exemple, après avoir employé l'écoute, un tiers non autorisé peut être en mesure d'analyser et capturer les informations cryptées. Souvent, cette information est facile à craquer car le cryptage est généralement simple, en raison de la complexité de la conception limitée de ces tags. Après l'attaquant rompt l'architecture ou la clé secrète de l'algorithme de chiffrement, ce qui le rend capable de cloner le tag pour tromper le lecteur légitime.

Ce type d'attaque arrive à vaincre le contrôle d'accès [15], permettant ainsi l'accès non autorisé à des biens personnels et aux systèmes tel que l'e-paiement [16]. L'authentification mutuelle, le cryptage et l'utilisation des données complexes sont proposés pour prévenir ce type d'attaque. Comme cité précédemment le chiffrement des données est souvent trop cher pour de nombreux systèmes RFID. Lors de l'ajout de l'authentification mutuelle comme une exigence, le coût est de plus en plus prohibitif.

Un exemple d'une attaque du type spoofing a été réalisé par des chercheurs de l'Université John Hopkins et les Laboratoires RSA qui ont réussi à déverrouiller un système d'immobilisation du véhicule en marche arrière, l'ingénierie et la fissuration du système et l'usurpation par la suite du lecteur en utilisant les données obtenues [17].

Contre-mesures:

Les attaques de type spoofing sont généralement évitées en limitant l'accès à la «bonne» information. Sans cette information, l'attaque ne peut pas être effectuée. Une clé secrète est nécessaire dans le cadre d'une procédure d'authentification, elle peut être introduite dans le cadre de l'information "correcte". Cette clé est ensuite stockée dans une zone restreinte de la mémoire qui ne peut être ni lue, ni transmise par l'étiquette en clair. De cette façon, les intrus ne peuvent pas mettre la main sur l'information complète "correct".

Cependant, de nombreux systèmes reposent sur le secret des algorithmes et des protocoles pour améliorer la sécurité fournie par la cryptographie, et donc se contentent d'utiliser de

courtes clés [15]. Ce fut le cas avec le système d'immobilisation usurpé par les chercheurs de John Hopkins University et les Laboratoires RSA. Ceci viole la loi de Kerchoffs qui stipule qu'un système doit être sécurisé même si tout sauf la clé est connu. Ainsi, les attaques de type spoofing sont mieux évitées par des protocoles cryptographiques appropriées qu'avec les clés.

L'authentification mutuelle, le cryptage et l'utilisation des données complexes sont proposés pour prévenir ce type d'attaque.

5.3 Les attaques de déni de service :

Les attaques par déni de service sont des attaques visant à perturber le fonctionnement normal d'un système. Comme la RFID est une technologie sans fil, ces attaques peuvent être menées par exemple par une simple perturbation de la fréquence de fonctionnement. Une attaque Dos (Deni of Service) peut être aussi réalisée en répondant à chaque demande de communication ce qui engendre le blocage des étiquettes. De cette façon, le lecteur détecte toujours une collision et est incapable de distinguer les tags.

Une autre forme d'attaques DoS visant les étiquettes d'un système RFID, en les désactivant ou en les détruisant, le système peut être alors arrêté puisque le lecteur n'est plus capable de lire les étiquettes.

Contre-mesures :

Les attaques DoS sont généralement très difficiles à empêcher. Il n'existe pas de bons mécanismes pour contrecarrer ces attaques. Cependant, elles sont souvent faciles à détecter, et elles peuvent donc être arrêtées avant qu'elles fassent trop de mal.

5.4 L'attaque man-in-the-middle:[18]

L'étude de la sécurité informatique et de la cryptographie classique nous enseigne que les échanges entre deux entités peuvent être sujets à une attaque du type man-in-the-middle perpétrée par une entité extérieure qui intercepte les messages échangés entre les victimes. Ce concept est général et englobe plusieurs types d'attaques possibles. Elles peuvent être actives — elles modifient alors les données échangées — ou passives en « écoutant » les informations qui transitent. Cette notion s'applique à la sécurité informatique dans son ensemble comme le système RFID.

Contre-mesures :

Un mécanisme de défense utilisé dans les protocoles d'authentification se base sur un paradigme d'échange challenge/réponse (défi/réponse). Un défi est envoyé au tag qui renvoie une réponse dépendante du défi et pouvant aussi dépendre d'une clé partagée. Une parade efficace contre ce type d'attaque réside dans l'implémentation d'un protocole d'authentification efficace, ce qui implique de fait une capacité suffisante au niveau des ressources du tag pour des opérations idoines (propres).

5.5 Attaque par relais : [19]

L'attaque par relais est similaire à l'attaque de l'homme du milieu (man-in-the-middle). Cette attaque consiste à faire communiquer le lecteur avec une étiquette truquée qui est reliée (à distance) avec un lecteur truqué qui se trouve à proximité d'une vraie étiquette.

Figure II.3 : Schéma d'une attaque par relais

Ainsi le lecteur pensera être en communication avec une étiquette qui ne se trouvera pourtant pas dans le champ de portée du lecteur. En particulier, quand le lecteur demandera à l´étiquette de s'identifier avec le challenge c (1), l'étiquette communiquera le challenge au lecteur truqué (2) qui interrogera la véritable étiquette (3) et transférera la réponse (4) à l'étiquette truquée (5), qui se fera ainsi passer pour une vraie étiquette (6) comme le montre la Figure II.4

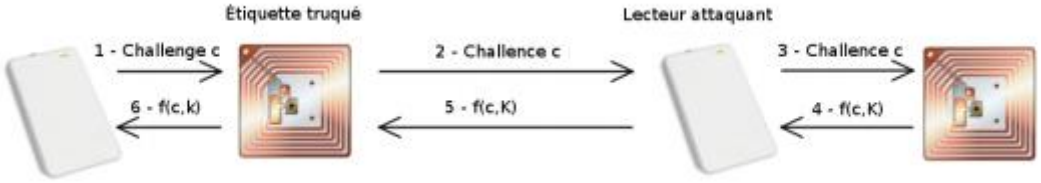


Figure II.4 : Schéma détaillé d'une attaque par relais

L'attaque est possible car une étiquette RFID peut être interrogée sans que son possesseur ne s'en rende compte. On peut alors très vite imaginer un scénario d'attaque, ou une personne mal intentionnée tente d'entrer dans un bâtiment, aidé d'un complice se trouvant à proximité d'une étiquette ayant les autorisations nécessaires. Il suffit alors que la personne mal intentionnée et son complice se coordonnent pour faire transmettre le challenge, et le lecteur se fera duper.

Ce n'est pas le chiffrement qui est ici remis en cause, et peu importe la fonction de chiffrement, le système est vulnérable à ce type d'attaque.

Contre-mesures :

Pour contrer les attaques par relais que nous venons de voir, la solution consiste à mettre en place un protocole de Distance Bounding. Le but d'un protocole de Distance Bounding est de permettre au lecteur de s'assurer que l'étiquette avec laquelle il communique se trouve dans un rayon proche de lui. Le principe de Distance Bounding a été introduit par Stefan Brands et David Chaum en 1993[20]. Il consiste en 3 phases d'échanges de bits : lente, rapide puis lente. En mesurant le temps d'aller-retour des échanges, le lecteur décide ou non, que

l'étiquette est autorisée à continuer la communication avec lui. La partie d'échange rapide de bits est donc primordiale, car c'est à ce moment-là que le timer autorisé doit être court, pour empêcher un attaquant d'avoir le temps de relayer le signal à un complice se trouvant hors du périmètre du lecteur.

5.6 Virus RFID

Généralement, les données stockées sur les étiquettes RFID sont implicitement sûres et les ressources des étiquettes RFID sont trop limitées pour représenter une menace sérieuse. Cependant, il a été récemment montré que cette confiance peut être sans fondement. Selon Rieback,Crispo et Tanenbaum [21], il est non seulement possible de lancer des attaques à un back-end[2] RFID ou au middleware depuis les étiquettes, mais cela peut être fait même avec des étiquettes à faible coût possédant seulement une mémoire capable de stocker 127 caractères. Le code malveillant peut prendre à la fois la forme d'un ver et d'un virus, et peut donc se propager soit par les connexions du réseau ou par le biais du système RFID lui-même. Rieback et al donnent également un exemple simple et pratique de la façon dont un virus de la RFID peut être écrit pour attaquer un système RFID grâce à l'utilisation d'une attaque par injection SQL. D'autres attaques possibles qui peuvent être lancées par des virus RFID comprennent les attaques de dépassement de tampons (buffer over flow) et des attaques par insertion de code. [22]

Contre-mesures :

Jusqu'à présent les attaques qui ont été provoquées par des virus RFID, tels que les attaques de dépassement de tampon ou les attaques par injection SQL sont toutes connues. Il ya aussi des méthodes bien déterminées pour les prévenir, comme la vérification des limites, vérification des paramètres de la liaison, limiter les autorisations de base de données …etc.

Le principal inconvénient est que les concepteurs du système ne semblent pas s'attendre à des logiciels malveillants. Selon Wired Magazine [23], Ari Juels, directeur de recherche chez les Laboratoires RSA, qui comparent la situation actuelle de la RFID avec le début de l'Internet, les caractéristiques de sécurité ne sont pas intégrées dans les systèmes à l'avance, ce qui est payé en termes de virus et d'autres attaques ultérieures. Autrement dit, la propagation et les dommages causés par des virus RFID pourraient être réduits en utilisant des contre-mesures connues au code malveillant dès la conception des systèmes.

6. Sécurité au niveau des étiquettes et lecteurs RFID :

Les informations inscrites sur une étiquette ou un lecteur d'étiquettes, ou encore transmises à/par une étiquette, peuvent être lues/écoutées, détruites/brouillées, ou mises à jour par des personnes non autorisées. Des étiquettes peuvent aussi être contrefaites ou clonées.

Dans ce qui suit nous citerons les contremesures principales à ces problèmes.

[2] Un **back-end** (ou un **arrière-plan**) désigne un étage de sortie d'un logiciel devant produire un résultat.

6.1 Confidentialité au niveau des étiquettes et lecteurs RFID :

Écoute non-autorisée de messages entre lecteurs et étiquettes. Pour de longues distances, de telles écoutes, ainsi que la localisation d'étiquettes, sont difficiles à réaliser. Pour de courtes distances, des lecteurs normaux peuvent être réutilisés. Des contremesures sont :

(i) De protéger contre les radiations électromagnétiques les zones où des lecteurs sont utilisés, par exemple en tapissant les murs avec du papier métallisé ;
(ii) D'encoder les données transférées autant que les possibilités de calcul de l'étiquette le permettent. L'encodage et l'usage de pseudonymes ne sont pas des mesures contre la localisation et le suivi d'étiquettes.

Lecture non-autorisée d'une étiquette. Une lecture est aisée dans les 3 à 5 mètres autour de l'étiquette (par exemple par quelqu'un se promenant dans un supermarché avec un lecteur dans sa poche).

Des contremesures contre les lectures non-autorisées sont :

(i) D'installer des détecteurs reconnaissant les champs magnétiques de lecteurs,
(ii) D'utiliser des méthodes d'authentification .Toutefois, dans les étiquettes EPC Global Class1 le mot de passe contrôlant l'accès à des zones mémoire est partagé par tous les utilisateurs et n'est donc intéressant que pour le stockage temporaire de données sensibles à l'intérieur d'une entreprise, i.e., pour éviter à certains des employés d'accéder à ces informations. Dans le cas général, si un lecteur stocke une liste des mots de passe, celle-ci doit être encodée et/ou maintenue dans une partie protégée de la mémoire de ce lecteur.

6.2 Intégrité et imputabilité au niveau des étiquettes et lecteurs RFID :

Émulation d'étiquette ou de lecteur ; écriture non-autorisée sur une étiquette ou un lecteur. Les données d'une étiquette ou d'un lecteur peuvent être modifiées physiquement, quoique cela soit difficile. Les données d'un lecteur peuvent également être lues ou modifiées via un accès réseau, et donc par exemple par un virus. L'identité et les mots de passe d'un lecteur peuvent aussi être volés par écoute non-autorisée des transmissions de lecteur sur le réseau ou vers des étiquettes.

Un simulateur d'étiquette ou de lecteur peut aussi être approché d'un lecteur ou d'une étiquette, ou même être positionné entre les deux et relayer leurs transmissions, afin de lire ou d'écrire sur l'étiquette ou le lecteur (dans ce dernier cas, "écrire sur le lecteur" signifie lui faire enregistrer une fausse information de la part d'une étiquette, e.g. un nouvel emplacement).

Des contremesures sont :

(i) Des protections physiques des étiquettes et des lecteurs.
(ii) Un contrôle d'accès sur les lecteurs ainsi que, si possible sur les étiquettes.

Ceci implique l'encodage et l'authentification mutuelle de toutes les transmissions, avec si possible l'imputabilité de celles-ci (e.g. si un lecteur modifie des données sur une étiquette,

celle-ci peut associer dans sa mémoire l'identité du lecteur à chacune des données qu'il a modifié).

Clonage d'étiquette. Le numéro d'identification d'une étiquette peut être inscrit sur une autre étiquette ou utilisé dans un réseau pour injecter de fausses données dans une base d'informations.

Des contremesures sont :

(i) D'éviter que les numéros d'identification soient connus d'agents non autorisés en évitant des écoutes ou lectures non-autorisées sur l'étiquette ou le réseau.
(ii) De créer sur l'étiquette des fonctions d'authentification de celle-ci qui soient très difficiles à reproduire, via des fonctions de hachage ou des "circuits logiques non reproductibles"

6.3 Accessibilité aux informations au niveau des étiquettes et lecteurs RFID

Les étiquettes et lecteurs ne doivent pas pouvoir être facilement mis hors service par erreur ou par malveillance, et doivent être accessibles via des standards (comme EPC global) ainsi que, au moins partiellement, via des protocoles peu sécurisés (comme ceux d'EPC global en 2008). Ce dernier point peut être atteint en permettant :

(i) Une restriction adaptée des accès donc pas de mot de passe pour les accès aux parties publiques d'un lecteur ou d'une étiquette
(ii) La génération automatique d'identifiants temporaires lorsque l'étiquette ou le lecteur requiert un identifiant pour toute lecture.

Un lecteur doit pouvoir appliquer différentes politiques de lecture d'étiquettes.

Détachement d'une étiquette d'un produit.
C'est une attaque facile qui peut créer d'importantes confusions. Elle permet par exemple d'échanger les étiquettes de produits.
Des contremesures sont :

(i) De faire en sorte que l'étiquette se brise si elle est détachée.
(ii) D'associer d'autres identifiants au produit (e.g. un code barre, des marques invisibles ou des étiquettes mieux cachées).
(iii) De permettre à l'étiquette de déceler son détachement et donc de l'enregistrer puis, tôt ou tard, de le communiquer.

Destruction mécanique ou chimique d'une étiquette.
Des contremesures sont d'inclure l'étiquette dans un endroit difficile à trouver ou à atteindre et d'inclure plusieurs étiquettes.
Destruction d'une étiquette via un champ électromagnétique. A courte distance, des étiquettes antivol peuvent ainsi être aisément désactivées. Pour d'autres étiquettes, cela peut parfois endommager le produit. L'usage de court-circuit auto-réparant est une contremesure potentielle.
Destruction d'une étiquette via une commande de désactivation. Une contremesure est une procédure d'authentification propre à cette commande. C'est le cas pour les étiquettes EPC Global Class1.
Destruction d'une étiquette active par décharge de sa batterie, via une série de lectures. Une contremesure est de limiter le nombre d'interactions par seconde.

Blocage ou brouillage de transmissions entre lecteurs et étiquettes par émetteurs de brouillage, des "étiquettes bloquantes", du papier métal, de l'eau, une main, etc.
Des contremesures potentielles sont :
(i)De détecter les émetteurs ou les blocages.
(ii)De permettre aux lecteurs d'utiliser différents protocoles ou fréquences.

7. Etude des différentes couches RFID : [24]

Les menaces et les défis croissants ont conduit à plusieurs propositions visant à améliorer les fonctions de sécurité dans les systèmes RFID. Cependant, la plupart des solutions de la sécurité actuelle sont axées sur la fourniture de techniques de contrôles de sécurité grâce à l'authentification et l'intégrité des services aux divers composants des systèmes RFID tels que les étiquettes et les lecteurs [25]. Les techniques d'authentification communes telles que le contrôle de mot de passe, les signatures numériques présentent quelques faiblesses. Par exemple, les mots de passe transmis dans l'air peuvent être interceptés ou brisés par la force brute. Les algorithmes HMAC (de l'anglais *keyed-Hash Message Authentication Code*) et les signatures numériques utilisées pour procéder à l'authentification du lecteur sur les étiquettes, nécessitent de la mémoire et des fonctions cryptographiques complexes pour être pris en charge sur étiquettes.

Ces solutions de sécurité cryptographiques sur tags peuvent ne pas être toujours possible en raison de la faible puissance, le stockage et des capacités de traitement d'étiquettes RFID. En outre, il est difficile de mettre en œuvre des algorithmes complexes dans des étiquettes passives qui sont principalement alimentées par des lecteurs RFID. Ces techniques ne peuvent pas tenir si le nœud adversaire compromet physiquement l'étiquette et obtient la clé secrète (en cas du HMAC).

Les propositions existantes vers la sécurisation RFID sont pour la plupart mises en œuvre dans l'étiquette ou le lecteur. Toutefois, en raison des limitations mentionnées ci-dessus, ces solutions sont le plus souvent inefficaces. De ce fait, il devient nécessaire de soutenir une couche supplémentaire de protection dans ces systèmes. Un système de détection d'intrusion (IDS) est souvent utilisé pour détecter les intrus quand les mécanismes cryptographiques échouent ou sont irréalisables, il devient alors nécessaire de fournir une seconde couche de défense pour accroître les mesures de sécurité RFID. L'intégration du module de détection d'intrusions en sécurité RFID devient maintenant possible puisque le système RFID est composé de différentes couches telles que la couche étiquette, couche lecteur et la couche Middleware.

7.1 La couche étiquette :

Les étiquettes sont utilisées pour stocker l'information utile qui peut être transmise par l'intermédiaire RF sans fil et donc largement utilisées dans des applications telles que le suivi et la gestion des stocks. Mais elles sont également les composants les plus vulnérables dans la communication sans fil vu qu'elles sont une cible potentielle de diverses attaques, y compris les perturbateurs des fonctionnalités et la destruction de tags. Puisque les ressources mémoires sont munies de faibles capacités de traitement cela limite d'avantage les fonctionnalités de

sécurité qui peuvent être placées à bord de l'étiquette. Par conséquent, il est difficile de fournir une couche de sécurité supplémentaire à la couche étiquette.

7.2 La couche lecteur :

Les lecteurs RFID sont les dispositifs chargés de la détection des étiquettes quand elles sont dans la zone de lecture et la lecture des données et des informations stockées dans ces étiquettes. Comme les méthodes de communication entre l'étiquette et le lecteur fonctionnent sur l'interface sans fil RF, elles offrent une sécurité qui présente des difficultés complexes. Par exemple, il est difficile d'éviter les attaques de lecture malveillantes contre les étiquettes telles que le blocage ou la manipulation des données sur un canal sans fil. Les lecteurs sont cependant riches en informations car ils peuvent lire les données de plusieurs étiquettes. Ils peuvent également être modifiés pour lire et observer les données des autres lecteurs voisins dans son champ. Par conséquent, il existe un potentiel pour la couche lecteur de recueillir des informations à partir d'étiquettes ainsi que d'autres lecteurs via l'interface RF ce qui forme une base de données d'audit.

L'information de la base de données peut être utilisée par d'autres couches RFID pour un traitement ultérieur afin de détecter des comportements contradictoires dans le réseau.

7.3 La couche Middleware :

Le middleware est le composant logiciel entre le lecteur et les applications en back-end comme le montre la Figure II.5. Ce module est souvent responsable du traitement du flux de données venant de lecture des tags. Comme cette couche est riche en ressources de calcul, les données recueillies de la couche de lecture audit peuvent être traitées pour la sécurité à l'aide d'un module de détection d'intrusions.

Par conséquent, il est plus approprié de placer le système de détection d'intrusions au niveau de cette couche. Ainsi, l'intégration des données de la couche de lecteur et du module de détection à la couche logicielle intermédiaire peut être utilisée pour identifier et détecter les composants RFID malveillants.

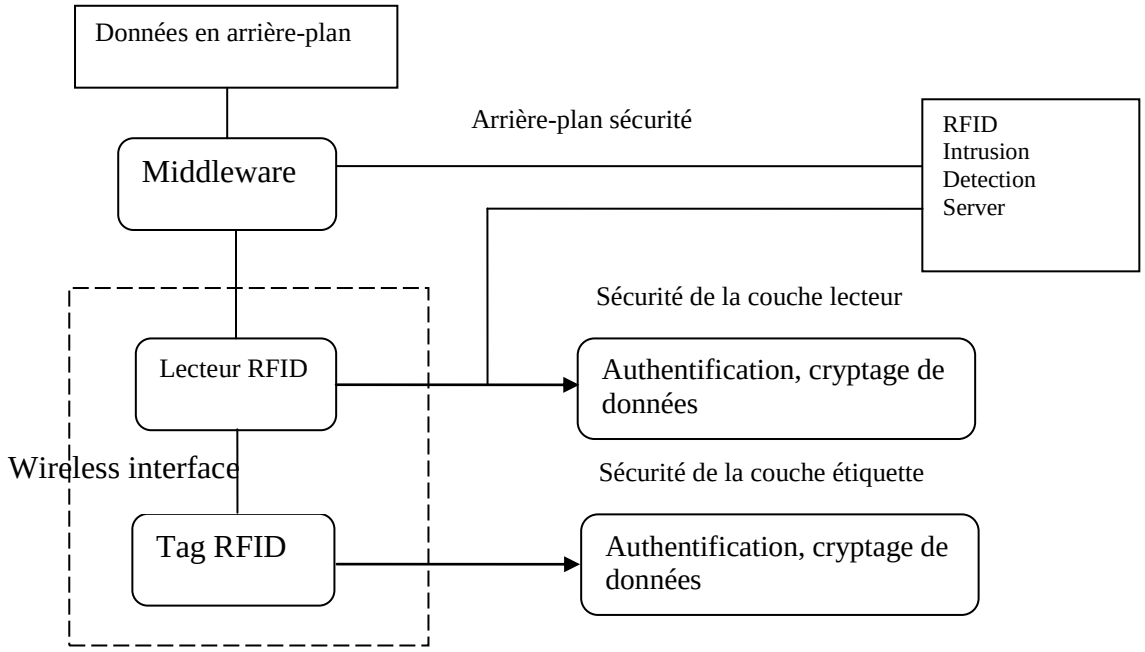


Figure II.5: Différents niveaux de sécurité d'un système RFID

8. Mesures de sécurité : [26]

La sécurité est mise en œuvre au moyen d'un ensemble de mesures – de gestion, opérationnelles et techniques – qui ont pour but de limiter les risques. Les systèmes RFID varient considérablement selon la technologie utilisée, les contextes d'applications et les scénarios. Pour être efficaces, les stratégies relatives à la sécurité doivent reposer sur une série de mesures qui assurent l'équilibre entre le coût, les performances et la commodité d'un système donné dans un cadre réglementaire particulier. L'évaluation des risques est une condition indispensable pour déterminer le niveau de la menace et le degré de vulnérabilité à un moment précis, et pour voir quelles sont les mesures appropriées pour les atténuer. La RFID n'est pas différente à cet égard des autres systèmes d'information.

Les *mesures de gestion* sont les orientations politiques, les procédures et les normes relatives au concept d'ensemble du système. Elles définissent en détail le mode de gestion d'une entreprise et les modalités d'exécution des activités quotidiennes. Les mesures de gestion comprennent notamment : les politiques de sécurité informatique, dont certaines dispositions concernent le contrôle d'accès aux informations de la RFID, la protection du périmètre d'utilisation et la gestion des mots de passe ; la politique d'utilisation de la RFID, qui définit les usages autorisés et non autorisés des technologies RFID ; les accords avec d'autres sociétés lorsque les données associées aux systèmes RFID sont mises en commun entre plusieurs entités ; les stratégies visant à limiter la quantité d'informations stockées sur les étiquttes (lorsqu'il s'agit de données personnelles, par exemple).

Les *mesures opérationnelles* correspondent aux actions effectuées par les utilisateurs du système. Il s'agit notamment du contrôle d'accès physique (caméras de surveillance, portes, murs, etc.), du choix de l'emplacement adéquat pour les étiquettes et les lecteurs (par exemple pour limiter les interférences), de la formation du personnel et de l'utilisation d'identifiants dont le format empêche la divulgation des informations.
Les *mesures techniques* sont les dispositions prises au niveau technologique pour contrôler et restreindre l'accès aux informations et au système. Cela comprend :

Les mesures visant à protéger les données de l'étiquette: dispositif désactivant toutes les fonctionnalités de la puce lorsqu'elle reçoit une instruction d'interruption ,cryptographie , mécanismes de contrôle d'accès, comme par exemple la protection à l'aide d'un mot de passe pour empêcher tout individu d'utiliser la commande d'interruption (« kill ») contre une puce « Class 1 Generation 2 » d'EPC ; mécanismes d'authentification en vertu desquels l'étiquette authentifie le lecteur et/ou inversement ; dispositifs anti-fraude pour empêcher que l'étiquette ne soit arrachée de l'objet auquel elle est attachée.

Les mesures visant à protéger l'interface radio : utilisation d'une fréquence qui évite certaines interférences (dans les liquides, par exemple), réglage du niveau de puissance afin de limiter la propagation des ondes radio et les risques d'interception, blindage de l'étiquette lorsqu'elle n'est pas sensée être en service, afin d'empêcher tout accès non autorisé, ou blindage de l'environnement pour éviter toute interception, enfin, désactivation temporaire des étiquettes actives. Le tableau ci-dessous donne un aperçu des mesures de sécurité dans les systèmes RFID [26].

Mesures de sécurité	Risques pour le processus de gestion	Risques pour les informations confidentielles de l'entreprise	Risques pour la vie privée	Attaques du réseau informatique
Mesures de gestion				
Politique concernant l'utilisation de la RFID	▪	▪	▪	▪
Politiques en matière de sécurité informatique	▪	▪		
Accords avec des entités extérieures	▪	▪	▪	
Minimisation des données stockées sur les puces	▪	▪	▪	
Mesures opérationnelles				
Contrôle d'accès physique	▪	▪		▪
Positionnement approprié des puces et des lecteurs	▪	▪		▪
Destruction sécurisée des puces	▪	▪	▪	
Formation de l'opérateur et de l'administrateur	▪	▪		▪
Séparation des taches	▪	▪		
Formats d'identifiant non parlant		▪	▪	
Mesures techniques				
Contrôle d'accès aux puces	▪	▪	▪	
Fonction d'interruption			▪	
Cryptage des données	▪	▪	▪	
Système d'identification alternatif	▪			
Authentification	▪	▪	▪	
Dispositif anti-fraude	▪	▪		
Sélection des fréquences radio	▪			▪
Ajustement de la puissance de transmission		▪		▪
Blindage électromagnétique		▪	▪	▪
Masquage des codes				
Désactivation temporaires des puces actives		▪	▪	

Tableau II.1 : aperçu des mesures de sécurité des systèmes RFIDs

9. Respect de la vie privée [9] :

Outre les problèmes directement liés à la sécurité, la RFID doit faire face aux problèmes qui touchent la vie privée. Ces problèmes concernent *la divulgation d'informations* qui se pose lorsque les données envoyées par le tag révèlent des informations sur l'objet qui le porte. Plus préoccupant, les produits pharmaceutiques marqués électroniquement, comme préconisé par le Food & Drug Administration aux Etats-Unis, pourraient révéler les pathologies d'une personne : un employeur ou un assureur pourrait déterminer les médicaments détenus par une personne et en tirer des conclusions sur son état de santé. Puis on a la *traçabilité malveillante des individus* qui vue que les tags électroniques n'ont pas vocation à contenir ou à transmettre d'importantes quantités de données, lorsqu'une base de données est présente dans le système, le tag peut n'envoyer qu'un simple identifiant, que seules les personnes ayant accès à la base de données peuvent relier à l'objet correspondant ce qui fait que même si un identifiant ne

permet pas d'obtenir d'informations sur l'objet lui-même, il peut permettre de le tracer ; c'est-à-dire de reconnaître l'objet dans des lieux différents ou à des instants différents. On peut ainsi savoir à quelle heure une personne est passée en un lieu donné, par exemple pour déterminer son heure d'arrivée et de départ de son poste de travail, ou on peut reconstituer son chemin à partir de plusieurs lecteurs, par exemple dans une entreprise ou un centre commercial. On a aussi le *profilage* qui est l'accès aux informations contenues sur les puces attachées aux objets que possèdent ou portent les individus pourraient révéler des aspects de leur vie, comme par exemple leurs intérêts pour des thèmes particuliers (dans le cas de livres marqués avec des puces RFID), ou le fait qu'ils ont de l'argent sur eux (lorsque la RFID est insérée sur des billets de banque) ou portent des objets de valeur.

10. Défenseurs contre opposants [9] :

Du côté des promoteurs de la RFID, la thèse que les tags électroniques mettent en péril le respect de la vie privée est ardemment rejetée. Une distance de lecture réduite à quelques décimètres est le principal argument de défense. Cet argument est contesté par les opposants car, en utilisant une antenne plus performante et une puissance d'émission non réglementaire, il est possible de dépasser la limite annoncée. En outre, il existe de nombreux cas où un attaquant peut suffisamment se rapprocher de sa victime pour lire ses tags électroniques : dans les transports en commun, dans une file d'attente, etc. L'inquiétude des opposants provient également du fait que les tags sont de plus en plus présents dans la vie de tous les jours, sans qu'on le sache. Ils sont souvent invisibles, répondant aux requêtes des lecteurs à l'insu même des personnes qui les portent.

11. Conclusion :

Dans ce chapitre nous avons présenté en général les différents types d'attaques aux quels sont confrontés les systèmes RFID ainsi que les problèmes de sécurité liés à cette technologie ce qui a démontré que l'augmentation de l'utilisation de la radio fréquence n'est pas sans conséquences comme le problème du respect de la vie privée, en particulier celui de la traçabilité malveillante, qui reste entier quelque soit l'application considérée. Ainsi nous avons vu l'étude des différentes couches RFID et les méthodes de sécurité qui ont été entreprises à leurs niveaux. Dans le chapitre suivant nous nous intéresserons aux systèmes de détection d'intrusions dans les RFIDs.

Chapitre III : Système de Détection d'Intrusion dans les systèmes RFID

1. Introduction :

Aujourd'hui, les systèmes informatiques sont déployés dans différents domaines comme les banques, les assurances, la médecine ou encore le domaine militaire. L'accroissement de l'interconnexion de ces divers systèmes, les a rendus accessibles par une population diversifiée d'utilisateurs qui ne cesse d'augmenter.

Malheureusement derrière la convenance et l'efficacité de ces services, les risques et les chances d'intrusions malveillantes ont aussi augmentés. En effet, ces utilisateurs connus ou non peuvent essayer d'accéder à des informations sensibles pour les lire, les modifier ou les détruire ou encore tout simplement pour porter atteinte au bon fonctionnement du système.

Dès lors la sécurité est devenue un enjeu incontournable afin de remédier aux problèmes des attaques potentiels, pour assurer la disponibilité des services, la confidentialité et l'intégrité des données et des échanges.

De nombreux mécanismes ont été développés pour garantir la sécurité des systèmes informatiques. La détection d'intrusions est un mécanisme particulier de gestion de sécurité qui consiste à essayer de détecter ces attaques au plutôt afin de réagir rapidement et d'éviter ainsi que de sérieux dommages soient causés.

Dans le cadre de ce chapitre nous allons présenter en général les systèmes de détection d'intrusions dans les RFIDs et leurs différentes caractéristiques.

2. La détection d'intrusions :

En sécurité informatique, la détection d'intrusions est l'acte de détecter les actions qui essaient de compromettre la confidentialité, l'intégrité ou la disponibilité d'une ressource. La détection d'intrusions peut être effectuée manuellement ou automatiquement.

Dans le processus de détection d'intrusions manuel, un analyste humain procède à l'examen de fichiers logs à la recherche de tout signe suspect pouvant indiquer une intrusion.

Par contre un système qui effectue une détection d'intrusions automatisée est appelé Système de Détection d'Intrusions (SDI).

Lorsqu'une intrusion est découverte par un SDI, les actions typiques qu'il peut entreprendre sont par exemple d'enregistrer l'information pertinente dans un fichier ou une base de données, de générer une alerte…

3. Système de détection d'intrusions :

Un système de détection d'intrusions est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (réseau, hôte).

Le rôle d'un système de détection d'intrusions est de détecter aussi bien un intrus essayant de causer des dommages au système qu'un utilisateur légitime abusant des ressources afin de permettre d'avoir une action de prévention sur les risques d'intrusion [27].

4. Concepts de base :

Nous désirons dans cette section éclairer quelques notions qui seront utilisées dans ce chapitre.

- **Système** : dénote un système d'information contrôlé par un système de détection d'intrusions. Cela peut être un poste de travail, un élément du réseau, une unité centrale, un pare-feu, un serveur Web, un réseau d'entreprise, etc.
- **Alarme** *:* c'est la réponse générée par le système de détection d'intrusions lors de la détection d'une intrusion. Cependant les erreurs de détection peuvent être classées selon deux types :
  - ***faux positif*** *:* signifie qu'un système de détection d'intrusions détecte une intrusion là où aucune intrusion réelle n'a été commise.
  - ***faux négatif*** *: à* l'inverse du « faux positif », le « faux négatif» signifie que le système de détection d'intrusions n'a pas détecté une intrusion ayant réussie.
- **Le journal système :** c'est le fichier contenant tous les événements affectant un processus particulier (application, activité d'un réseau informatique…). Généralement datés et classés par ordre chronologique, ces derniers permettent d'analyser pas à pas l'activité interne du processus et ses interactions avec son environnement.
- **Sonde :** c'est un équipement qui permet d'analyser et de gérer les flux réseau.
- **Audit :** représente la collecte d'informations fournies par le journal système, les journaux propres à certaines applications (comme un serveur de courrier électronique), mais aussi de données provenant de « sondes » installées par les outils de détection eux mêmes, comme des «sniffers » réseau ou des modules applicatifs spécifiques, permettant d'observer l'utilisation de l'application.
- **Fichier log :** Un log (ou fichier log) se présente sous la forme d'un fichier texte classique, reprenant de façon chronologique, l'ensemble des événements qui ont affecté un système informatique et l'ensemble des actions qui ont résulté de ces événements.

5. Architecture classique d'un SDI :

Un système de détection d'intrusions est constitué de trois composants : un capteur, un analyseur et un manager la Figure III.1 illustre les interactions entre eux. Le capteur est chargé de collecter des informations sur l'évolution de l'état du système et de fournir une séquence d'événements qui traduit l'évolution de ce dernier. L'analyseur détermine si un sous-ensemble d'événements produits par le capteur est caractéristique d'une activité malveillante. En fin le manager collecte les alertes produites par l'analyseur, les met en forme et les présente à l'operateur. Eventuellement, le manager est chargé de la réaction à adopter.

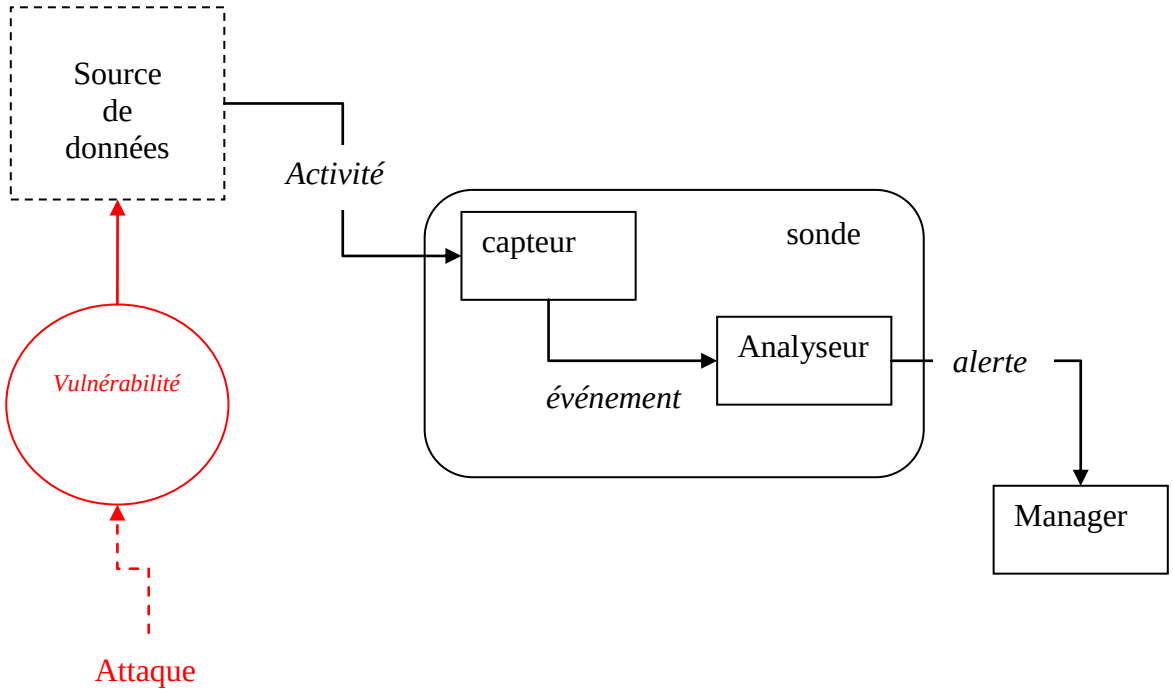


Figure III.1 : architecture classique d'un SDI [28]

6. Les familles d'IDS et leurs variantes : [27]

Selon l'endroit qu'ils surveillent et ce qu'ils contrôlent (les "sources d'informations"), deux familles principales d'IDS sont usuellement distinguées :

Les **N-IDS** (Network based Intrusion Detection System) : Ils assurent la sécurité au niveau du réseau.
Le rôle essentiel d'un SDI réseau (NIDS) est l'analyse et l'interprétation des paquets circulant sur un réseau. Afin de repérer les paquets à contenu malicieux, des détecteurs (souvent de simples hôtes) sont utilisés pour analyser le trafic et si nécessaire envoyer une alerte.
Un NIDS travaille sur les trames réseau à tous les niveaux (couches réseau, transport, application). De plus en plus, en disséquant les paquets et en comprenant les protocoles, il est capable de détecter des paquets malveillants conçus pour outrepasser un pare-feu aux règles de filtrage trop laxistes (indulgentes), et de chercher des signes d'attaque à différents endroits sur le réseau.
Quelques exemples de NIDS : NetRanger, NFR, Snort, DTK, ISS RealSecure [29].
Les SDI réseau facilitent, grâce aux signatures, la détection des scans et offrent une meilleure sécurisation des détecteurs d'intrusions puisqu'ils se contentent d'observer le trafic. Cependant, les problèmes majeurs liés aux NIDS sont de conserver toujours une bande passante suffisante pour l'écoute de l'ensemble des paquets, et de bien positionner l'IDS pour qu'il soit efficace.

Les **H-IDS** (Host based Intrusion Detection System) : Les systèmes de détection d'intrusions basés sur l'hôte (poste de travail, serveur, etc.), assurent la sécurité au niveau des hôtes. Ils

analysent exclusivement l'information concernant cet hôte. Comme ils n'ont pas à contrôler le trafic du réseau mais seulement les activités d'un hôte, ils se montrent habituellement plus précis sur les variétés d'attaques.
Ces SDI utilisent deux types de sources pour fournir une information sur l'activité : les *logs* et les *traces d'audit* du système d'exploitation. Chacun a ses avantages : les traces d'audit sont plus précises, détaillées et fournissent une meilleure information; les *logs*, qui ne fournissent que l'information essentielle, sont plus petits et peuvent être mieux analysés en raison de leur taille. [30]
Il n'existe pas de solution unique HIDS couvrant l'ensemble des besoins, mais les solutions existantes couvrent chacune un champ d'activités spécifiques, comme l'analyse de *logs* système et applicatifs, la vérification de l'intégrité des systèmes de fichiers, l'analyse du trafic réseau en direction/provenance de l'hôte, le contrôle d'accès aux appels système, l'activité sur les ports réseau, etc...
Les systèmes de détection d'intrusions basés sur l'hôte ont certains avantages : l'impact d'une attaque peut être constaté et permet une meilleure réaction, des attaques dans un trafic chiffré peuvent être détectées, les activités sur l'hôte peuvent être observées avec précision. Ils présentent néanmoins des inconvénients, parmi lesquels : les *scans* sont détectés avec moins de facilité ; ils sont plus vulnérables aux attaques de type DoS ; l'analyse des traces d'audit du système est très contraignante en raison de la taille de ces dernières ; ils consomment beaucoup de ressources CPU, etc…

I*DS hybride* Généralement utilisés dans un environnement décentralisé, ils permettent de réunir les informations de diverses sondes placées sur le réseau. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS et d'un NIDS.

De ces deux familles principales, de nombreuses variantes sont issues :
SDI de nœud réseau (NNIDS). Les systèmes de détection d'intrusions de nœud réseau (NNIDS pour *Network Node IDS*) fonctionnent comme les NIDS classiques, c'est-à-dire qu'ils analysent les paquets du trafic réseau, hormis que cela ne concerne que les paquets destinés à un nœud du réseau, et à la différence des NIDS classiques, les NNIDS ne captent pas l'ensemble des trames circulant sur le réseau.

SDI basé sur une application (ABIDS). Les SDI basés sur les applications (ABIDS pour *Application-Based IDS*) sont un sous-groupe des SDI hôtes, parfois mentionnés séparément. Ils contrôlent l'interaction entre un utilisateur et un programme en ajoutant des fichiers logs afin de fournir de plus amples informations sur les activités opérant entre utilisateur et programme.
Ses principaux avantages sont de travailler en clair (contrairement aux NIDS, par exemple) d'où une analyse plus facile, et la possibilité de détecter et d'empêcher des commandes particulières dont l'utilisateur pourrait se servir avec le programme. Deux inconvénients majeurs sont identifiés : le peu de chances de détecter, par exemple, un cheval de Troie (puisque l'ABIDS n'agit pas dans l'espace du noyau) ; en outre, les fichiers logs générés par ce type de SDI sont des cibles faciles pour les attaquants (ils ne sont pas aussi sûrs que les traces d'audit du système, par exemple).

7. Les méthodes de détection d'intrusions :

Plusieurs critères permettent de classer les systèmes de détection d'intrusions, la méthode d'analyse étant le principal. Deux approches dérivant de cette dernière existent aujourd'hui selon qu'elles se basent sur des modèles comportementaux ou sur des signatures d'attaques.

7.1 Approche comportementale : [31]

Cette approche est connue aussi par *l'approche de détection d'anomalies***.** Elle consiste à définir un profil de l'activité normale d'un utilisateur et à considérer les déviations significatives de l'activité courante de l'utilisateur par rapport aux profils de comportements normaux comme anomalie.
L'approche comportementale est fondée sur une description statistique des sujets. L'objectif est de détecter les actions anormales effectuées par ces sujets (par exemple, des heures de connexion anormales, un nombre anormal de fichiers supprimés ou un nombre anormal de mots de passe incorrects fournis au cours d'une connexion). Le comportement normal des sujets est appris en observant le système pendant une période donnée appelée phase d'apprentissage. Le comportement normal, appelé comportement sur le long terme, est enregistré dans la base de données et comparé avec le comportement présent des sujets, appelé comportement à court terme. Une alerte est générée si une déviation entre ces comportements est observée. Dans cette approche, le comportement sur le long terme est, en général, mis à jour périodiquement pour prendre en compte les évolutions possibles des comportements des sujets.
Nous considérons traditionnellement que l'avantage principal de l'approche comportementale est de pouvoir être utilisée pour détecter de nouvelles attaques. Autrement dit, en signalant toute déviation par rapport au profil, il est possible de détecter à priori toute attaque qui viole ce profil, même dans le cas où cette attaque n'était pas connue au moment de la construction du profil.
Cependant, cette approche présente également plusieurs inconvénients. Tout d'abord, le diagnostic fourni par une alerte est souvent flou et nécessite une analyse complémentaire. Ensuite, cette approche génère souvent de nombreux faux positifs car une déviation du comportement normal ne correspond pas toujours à l'occurrence d'une attaque. Citons à titre d'exemple, en cas de modifications subites de l'environnement de l'entité modélisée, cette entité changera sans doute brutalement de comportement. Des alarmes seront donc déclenchées. Pour autant, ce n'est peut-être qu'une réaction normale à la modification de l'environnement. En outre, les données utilisées en apprentissage doivent être exemptes d'attaques, ce qui n'est pas toujours le cas. Enfin, un utilisateur malicieux peut habituer le système (soit pendant la phase d'apprentissage, soit en exploitation si l'apprentissage est continu) à des actions malveillantes, qui ne donneront donc plus lieu à des alertes. Le problème de la détection d'intrusions est couramment approché d'une façon radicalement différente qui est l'approche par scénario.

7.2 Approche par scénario :

La détection d'intrusions peut également s'effectuer selon une approche par scénario. Cette approche définit des signatures soupçonneuses basées sur les vulnérabilités connues du système et de la politique de sécurité. Une intrusion est signalée lorsque la trace d'une attaque connue est présente dans les traces d'audit.

Il s'agit de recueillir des scénarios d'attaques pour alimenter une base d'attaques. Le principe commun à toutes les techniques de cette classe consiste à utiliser une base de données, contenant des spécifications de scénario d'attaques (on parle de signatures d'attaque et de base de signatures). Le détecteur d'intrusions compare le comportement observé du système à cette base et remonte une alerte si ce comportement correspond à une signature prédéfinie. Le principal avantage d'une approche par scénario est la précision des diagnostics qu'elle fournit par rapport à ceux avancés par l'approche comportementale. Il est bien entendu que l'inconvénient majeur de cette approche est qu'elle ne peut détecter que des attaques dont elle dispose de leurs signatures. Or, définir de façon exhaustive la base de signatures est une des principales difficultés à laquelle se heurte cette approche. La génération de faux négatifs est à craindre en présence des nouvelles attaques. En effet, contrairement à un système de détection d'anomalies, ce type de détecteur d'intrusions nécessite une maintenance active : puisque par nature il ne peut détecter que les attaques dont les signatures sont dans sa base de données, cette base doit être régulièrement mise à jour en fonction de la découverte de nouvelles attaques. Aucune nouvelle attaque ne peut par définition être détectée. D'autre part, il existe de nombreuses attaques difficiles à détecter car elles nécessitent de corréler plusieurs événements. Dans la plupart des produits commerciaux, ces attaques élaborées sont décomposées en plusieurs signatures élémentaires. Cette décomposition peut générer de nombreux faux positifs si un mécanisme plus global n'est pas développé pour corréler les alertes correspondantes à ces différentes signatures élémentaires.

Chacune de ces deux approches peut conduire à des faux positifs (détection d'attaque en absence d'attaque) ou à des faux négatifs (absence de détection en présence d'attaque).

Il existe d'autres critères de classification des SDIs tels que :

- *Les sources de données à analyser :* Les sources possibles de données à analyser sont une caractéristique essentielle des systèmes de détection d'intrusions. Les données proviennent, soit de fichiers générés par le système d'exploitation, soit de fichiers générés par des applications, soit encore d'informations obtenues en écoutant le trafic sur le réseau.
- *Le comportement du SDI après intrusion :* Une autre façon de classer les systèmes de détection d'intrusions, consiste à voir quelle est leur réaction lorsqu'une attaque est détectée. Certains se contentent de déclencher une alarme (réponse passive).
- *La fréquence d'utilisation :* Une autre caractéristique des systèmes de détection d'intrusions est leur fréquence d'utilisation : périodique ou continue. Certains systèmes de détection d'intrusions analysent périodiquement les traces d'audit à la recherche d'une éventuelle intrusion ou anomalie passée. Cela peut être suffisant dans des contextes peu sensibles. La plupart des systèmes de détection d'intrusions récents effectuent leur analyse des traces d'audit ou des paquets réseau de manière continue afin de proposer une détection en quasi temps réel. Cela est nécessaire dans des contextes sensibles (confidentialité) ou commerciaux (confidentialité, disponibilité).

C'est toutefois un processus coûteux en temps de calcul car il faut analyser à la volée tout ce qui se passe sur le système.

8. Système de détection d'intrusions dans les systèmes RFID :

Il existe plusieurs systèmes de détection d'intrusions pour différents systèmes informatiques, comme les systèmes **Haystack** [32], **MIDAS** [33] et **IDES** [34, 35, 36].

Ainsi les idées, opérations et technologies pour la sécurisation des informations dans les RFIDs sont fondamentalement les mêmes que celles des systèmes informatiques normaux. Toutefois, les limites matérielles des tags ainsi que l'utilisation de la radiofréquence comme moyen de communication qui donnent la possibilité à un intrus d'accéder aux tags facilement et sans préavis font que la technologie RFID soit distinguée des autres systèmes. Plusieurs travaux ont été réalisés sur les systèmes de détection d'intrusions dans les RFIDs. Des chercheurs ont mis en œuvre des approches relatives à ce domaine. Dans ce qui suit nous présentons quelques travaux qui ont été réalisés: [37, 38,39]

Geethapriya et Ramalingam:

Geethapriya Thamilarasu et Ramalingam Sridhar[37], ont utilisé dans leur travail le modèle de détection d'intrusion statistique basé sur l'activité enregistrée dans le journal d'audit pour détecter un comportement anormal. Pour déterminer les anomalies ils ont observé les transactions faites entre le lecteur et les tags pour voir s'il y a déviation.

Ils modélisent leur modèle de détection d'intrusions par l'étude de l'attaque Man-in-the-middle (MIM) dans le système RFID. Sachant que <T, R> représente l'étiquette (Tag) et le lecteur(Reader) authentique et que <T', R'> représente le tag et le lecteur malveillants. Selon le scénario représenté par la Figure III.2, deux cas sont distingués :

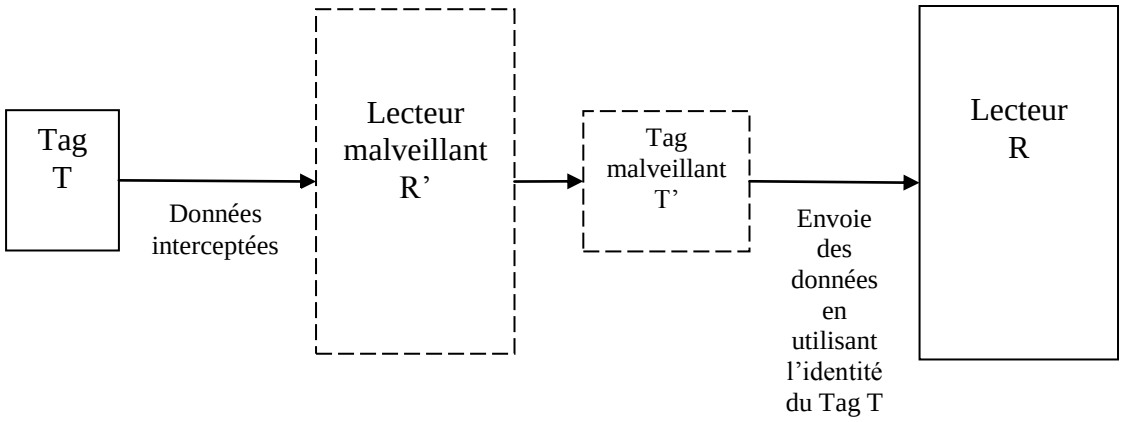


Figure III.2 : scénario de l'attaque MIM

Cas 1: un lecteur malveillant R' intercepte la demande de lecture de R et communique ensuite avec T en se faisant passer pour R. R' reçoit les données et les informations secrètes de l'étiquette T et relaie cette information à R en utilisant le tag T'. Ainsi la communication entre T et R est perturbée et les utilisateurs malveillants gagnent l'accès aux services du lecteur.

Cas 2: l'attaque MIM peut également être utilisée pour manipuler le contenu d'un tag authentique. R' peut s'identifier comme étant un lecteur R valide et peut ainsi écrire de fausses données sur les étiquettes réinscriptibles. La falsification de données peut être utilisée pour perturber le réseau ou pour permettre à une entité illégale d'accéder au système RFID.

Un lecteur est utilisé comme chien de grade « watchdog reader » pour surveillé la communication entre les lecteurs et les étiquettes en observant à la fois le tag T et les données en rediffusion depuis le tag T' qui porte le même identifiant que T (TagID) et qui est localisé dans un autre endroit.

Pour détecter une attaque MIM un compteur d'événement pour le type des transactions RFID (lecture et écriture) est créé pour chaque étiquette.

Pour signaler une anomalie dans ces événements, les métriques suivantes sont utilisées :

Fréquence de lecture: nombre moyen d'opérations de lecture sur un Tag T

Fréquence d'écriture: nombre moyen d'opérations d'écriture sur un Tag T

Intervalle de temps: durée de temps entre deux événements du même type peut être utilisée pour observer toute activité incompatible. Par exemple, si la même étiquette est lue par le même lecteur consécutivement, une anomalie est détectée.

Valeur RSS (Received Signal Strength): dans le premier cas de l'attaque MIM, identifier l'emplacement du tag peut être utile pour détecter les attaques. La plupart des lecteurs RFID sont maintenant en mesure d'estimer l'intensité du signal reçu (RSS). L'utilisation de la métrique RSS, détermine l'emplacement de l'étiquette avec une grande précision.

Dans cette étude un profil d'utilisateur normal sans aucune intrusion est établi en se basant sur le journal d'audit.

Les données observées à partir du chien de garde sont communiquées à la couche middleware pour les traiter. En utilisant une méthode statistique de détection, la déviation observée par rapport au comportement normal du système est considéré comme une intrusion.

Luke Mirowski et Jacky Hartnett :

Le changement de la propriété du tag compromet les objectifs de la sécurité de l'identification par radiofréquence. Quand un attaquant clone ou vole l'étiquette d'un objet autorisé, il sera autorisé à accéder à ses propriétés. Deckard, est une approche qui prévient le changement de la propriété du tag. C'est un système qui utilise les principes de détection d'intrusion pour la recherche du comportement anormal qui peut indiquer quand un changement de la propriété du tag a eu lieu.

La technologie RFID suppose que l'objet en possession d'un tag est l'entité autorisée. Par conséquent, un changement de la propriété du tag, compromet l'objectif de la sécurité d'un système RFID, les attaquants ne peuvent pas être différenciés des sujets autorisés.

Luke Mirowski et Jacky Hartnet utilisent l'enregistrement d'audit d'une étiquette pour construire un profil représentant le comportement normal de l'objet étiqueté, qui sera ensuite utilisé pour déterminer le moment où le comportement de l'objet s'écarte significativement.

Ils supposent qu'un écart important par rapport au comportement normal est indicatif d'un changement de la propriété du tag. Ce système serait utile pour détecter quand un attaquant commence à utiliser une étiquette clonée ou volée. Pour mieux illustrer ce principe, nous donnons l'exemple suivant : lorsque Mallory vole ou clone l'étiquette d'Alice, l'utilisation de cette étiquette par Mallory sera différente de son utilisation par Alice. Ainsi, un changement de la propriété du tag est supposée être visible par un important écart dans les dossiers d'audit des étiquettes. Par conséquent, Ils ont développé un profil unique appelé Profil de la fréquence d'emplacement (LFP : Location Frequency Profile) pour repérer les comportements qui peuvent indiquer un changement de la propriété du tag. Aussi ils ont supposé qu'un écart significatif loin du comportement normal est un indicateur d'un changement dans la propriété de l'étiquette. Ainsi, la LFP définit un seuil réglable administrateur appelé écarts de moyenne (DFM).

Deckard fonctionne de la manière suivante : Tout d'abord, le lecteur enregistre les détails du fonctionnement d'un lecteur RFID dans un enregistrement d'audit. Cet enregistrement est ensuite stocké dans un journal d'audit. Deuxièmement, le moteur de traitement effectue régulièrement une mise à jour sur chaque profil d'étiquette. Chaque profil est récupéré à son tour de la base de connaissances en collaboration avec ses enregistrements d'audit associés. Pour déterminer la LFP, il calcule le nombre moyen de fois qu'un tag a été utilisé, et la gamme de temps où il peut être utilisé selon le seuil DFM. Le DFM signifie le nombre d'écarts loin de la moyenne d'une observation courante qui peut se produire.

Enfin, un enregistrement de l'activité est produit pour signaler le résultat d'une mise à jour du profil; négatif si le seuil des profils a été dépassé par la mise à jour courante du profil ou positif si aucun comportement anormal n'a été détecté.

M. Esposito et G. Della Vecchia :

Du point de vue de la technologie RFID, la menace de sécurité la plus difficile dans plusieurs applications RFID est le clonage de tags, c'est à dire quand un attaquant fait une copie exacte d'une étiquette RFID, en utilisant l'identifiant unique de l'étiquette originale, de manière à créer des étiquettes clonées indiscernables à partir des originales.

M. Esposito et G. Della Vecchia, ont présenté une ontologie basée sur la détection d'intrusions pour des systèmes RFID qui intègre des informations provenant de la couche middleware RFID pour détecter le clonage de tags.

Ils ont ainsi appliqué des ontologies et des règles pour mettre en œuvre une technique de suivi et de traçabilité "track and trace" d'objets qui repose sur le raisonnement que «quand vous savez où objet l'authentique étiqueté est, ceux qui sont faux / clonés peuvent être détectés ». Elle se réfère à générer et à stocker les profils dynamiques de la RFID et à marquer le

mouvement d'objets à travers la chaîne d'approvisionnement. De tels profils sont construits, en exploitant l'ensemble des événements de la localisation relatifs à un objet étiqueté qui peuvent être récupérés à partir d'un système de traçage. Les objets étiquetés sont également caractérisés par des profils statiques, c.-à-d chemins fixes composés de points d'intérêt (POI) à travers la chaîne d'approvisionnement qui spécifient les conditions d'utilisation normales pour des objets marqués.

Un moteur d'inférence a été utilisé pour fournir le SDI avec la capacité de raisonnement automatique à propos d'ontologies et de règles afin de réellement appliquer le modèle formalisé de détection et de déduction quand un objet étiqueté est cloné ou victime d'une attaque de clonage.

9. Caractéristiques d'un bon SDI :

9.1 Efficacité :

L'efficacité d'un système de détection d'intrusions est déterminée par les mesures suivantes :

- **Exactitude** : Le système de détection d'intrusions n'est pas exact s'il considère les actions légitimes des utilisateurs comme atypiques ou intrusives.
- **Performance :** La performance d'un système de détection d'intrusions est mesurée par le taux de traitement des traces d'audits. Si la performance du système de détection d'intrusions est pauvre, donc la détection en temps réel n'est pas possible.
- **Perfection :** Un système de détection d'intrusions est imparfait s'il n'arrive pas à détecter une attaque.
- **Tolérance aux pannes :** Un système de détection d'intrusions doit être résistant aux attaques, en particulier dans le cas des attaques de déni de service.
- **Opportunité :** Un système de détection d'intrusions doit exécuter et propager son analyse d'une manière prompte pour permettre une réaction rapide dans le cas d'existence d'une attaque.

9.2 Limites : [40]

La détection d'intrusions présente des limites et peut se montrer impuissante dans certains cas. Ces limites s'appliquent aux techniques de détection d'abus comme à celles de détection d'anomalies.

Attaques sur les drapeaux TCP. Les SDI sont vulnérables à certaines attaques sur les drapeaux TCP *(TCP flags)* [15], comme par exemple :

- envoi d'un faux SYN ;

- insertion de données avec mauvais numéro de séquence ;

- FIN/RST *spoofing* avec mauvais numéro de séquence ;

- désynchronisation après connexion ;

- désynchronisation avant connexion [SYN (mauvaise somme de contrôle + mauvais numéro de séquence) puis SYN] ;

- FIN/RST *spoofing* avec mauvaise somme de contrôle ;

- *Data spoofing* avec mauvaise somme de contrôle ;

- FIN/RST *spoofing* avec TTL court;

- insertion de données avec un TTL court, etc.

Placement du *SDI.* Au niveau du placement du SDI. L'important est de bien identifier les ressources à protéger et ce qui est le plus susceptible d'être attaqué [41]. Il convient alors d'implémenter précautionneusement le SDI en fonction du placement choisi [42].

Pollution/surcharge. Les SDI peuvent être pollués ou surchargés par la génération d'un trafic important lourd à analyser. Une quantité importante d'attaques superficielles peut également être envoyée afin de surcharger les alertes du SDI.

Des conséquences possibles de cette surcharge peuvent être la saturation de ressources (disque, CPU, mémoire), la perte de paquets, le déni de service partiel ou total.

Contournement/évasion. Les SDI peuvent également être contournés ou outrepassés. Dans le cas d'une attaque par évasion, le système de détection d'intrusion rejette un paquet qui sera pourtant accepté par la destination. Il se peut, par exemple, qu'une différence de systèmes d'exploitation entre la machine supportant le SDI et la machine surveillée fasse que certains paquets rejetés par le système de détection d'intrusion soient acceptés par la destination (comme des paquets UDP avec une somme de contrôle erronée, rejetés par la plupart des systèmes d'exploitation sauf les plus anciens).

10. Conclusion

Dans ce chapitre nous avons introduit en premier lieu une vue générale sur les systèmes de détection d'intrusions par leur définition et la présentation des différentes familles existantes, puis nous avons présenté quelques exemples de SDI dans les systèmes RFID. En second lieu nous avons abordé les caractéristiques que doit avoir un bon SDI.

Chapitre IV: Le système de détection d’intrusion proposé

1. Introduction :

Les systèmes de détection d'intrusions sont des systèmes de sécurité conçus pour surveiller les données circulant dans les réseaux notamment dans les systèmes RFID, pour détecter les intrus et faire face non seulement aux attaques connues, mais aussi à celles inconnues. Nous proposons un système de détection d'intrusions qui se base sur l'approche par scénario ainsi que sur les échanges entre lecteurs et étiquettes.

Dans ce chapitre nous allons décrire la démarche à suivre pour la conception du système de détection d'intrusions proposé, en commençant par la description de son principe de base, ainsi que ses objectifs principaux, puis nous allons détailler son fonctionnement.

2. L'idée de base :

L'idée de base de notre travail est de développer un système de détection d'intrusions utilisant la détection par scénario qui offre l'avantage de la précision et qui a permis de définir des signatures soupçonneuses basées sur les vulnérabilités connues du système. Cette technique accorde un taux élevé de détection et ainsi tenter de minimiser le taux de fausses alertes [43]. Afin de voir l'impact de ce SDI sur les systèmes RFIDs, nous avons profité des avantages qu'offrent les composants du système RFID. Le système de détection d'intrusions développé vise à atteindre certains objectifs dont nous citons :

1. Offrir un niveau de sécurité acceptable :

Prendre en charge les services de sécurité requis pour les systèmes RFIDs et minimiser le taux de fausses alertes.

2. Faire face à l'attaque de clonage :

Détecter les principaux facteurs qui peuvent engendrer ce type d'attaque.

3. Garantir les performances des RFIDs :

Ne pas dégrader les performances du système RFID.

3. Règles utilisées pour la détection :

Notre système de détection se base sur l'approche par scénario. Cette approche signifie la détection d'une mauvaise utilisation, elle est caractérisée par l'existence d'une base de connaissances qui comporte des modèles d'attaques connus à priori appelés signatures. Elle consiste à examiner les activités du système en cherchant des événements ou l'ensemble des événements qui décrivent une attaque connue, elle compare donc entre les comportements observés et les scénarios d'attaques prédéfinis.

Le choix de l'approche par scénario a été motivé par le fait qu'elle permet d'avoir un taux élevé de détection et une meilleure exactitude. Ci-dessous nous illustrons les règles utilisées pour la détection de l'attaque de clonage.

La technologie RFID fonctionne sur l'hypothèse que chaque étiquette est unique ; ce qui veut dire qu'il n'y pas deux étiquettes avec le même numéro d'identification. Cette hypothèse permet au lecteur d'identifier de manière unique une étiquette et de savoir exactement quel objet est à portée du lecteur. Toutefois, il a été démontré par un certain nombre de chercheurs que l'unicité des étiquettes ne peut pas être garantie parce que leurs numéros d'identification peuvent être clonés. Le clonage d'étiquettes est le vol d'identité d'un tag, et cela pour une utilisation non autorisée, à des fins malveillantes. En ayant un clone dans le système, un attaquant peut facilement tromper le système en lui faisant croire qu'il est l'étiquette légitime (d'origine). Il est possible de détecter une telle attaque en se rendant compte qu'il y a une déviation par rapport aux scénarios établis dans le système.

Les règles ci-dessous sont utilisées pour la détection par scénarios dans notre système de détection d'intrusion :

Règle de temps : un tag ne doit pas dépasser un intervalle de temps déterminé dans la zone d'un reader.

Règle de l'unicité : deux étiquettes ne peuvent pas posséder un même numéro d'identification.

4. Fonctionnement du système proposé:

Dans ce qui suit nous déterminons la manière dont les systèmes RFID assurent les différentes règles définies précédemment :

Règle de l'unicité : puisque le système repose sur le principe que deux objets différents ne peuvent pas porter le même identifiant donc le fait de lire deux étiquettes portant le même numéro d'identification au même moment peut être une intrusion (un clonage).

Règle de temps : si une étiquette dépasse la durée de temps délimitée dans la zone du reader, une intrusion est suspectée.

5. Déroulement du système de détection d'intrusion proposé :

Dans cette section nous nous étalons sur le fonctionnement détaillé du système de détection d'intrusion proposé :

a) Détection de l'attaque du clonage :

L'attaque du clonage vise à s'introduire dans un système d'une façon illégale dans le but d'accéder à ses données pour les exploiter ultérieurement. Afin de se protéger de cette attaque, les traitements suivants seront effectués à chaque fois qu'un tag est lu par le lecteur :

- A chaque lecture d'un tag, un évènement lecture du tag sera lancé, afin de récupérer son identifiant, et son timestamp.
- Si un tag dépasse le tempsmax(la durée délimitée de la lecture) un évènement tag cloné détecté sera déclenché.

b) Confirmation si c'est une vraie attaque :

Dans ce qui suit nous décrirons notre méthode d'authentification des tags, pour que le lecteur confirme qu'il reçoit des données depuis un tag légitime :

Authentification du tag par question/réponse :

Le schéma communément utilisé pour réaliser l'authentification est dit par question/réponse : le lecteur envoie un challenge (une question) au tag qui prouve son identité en répondant à ce challenge.

Evidemment, un adversaire n'est pas capable de répondre à la place du tag. Les étapes suivantes expliquent comment notre système doit répondre à ces spécificités :

- Notre système contient un ensemble de tags légitimes. Chaque tag est muni d'une information secrète qui se présente sous forme d'une fonction implémentée avant l'utilisation du tag.

- Les tags transmettent uniquement leurs identifiants pendant leurs lectures. Ainsi un utilisateur malveillant d'une étiquette clonée ne pourra pas accéder à la fonction d'authentification secrète d'une étiquette légitime.
- Si une étiquette lue ne respecte pas les règles définies par notre système, ce dernier détecte une tentative d'accès dérobée au système par un tag qui peut être cloné. Afin de confirmer que c'est une vraie intrusion le lecteur générera un challenge auquel le tag devrait donner la bonne réponse selon la fonction d'authentification qu'il possède.
- Si l'étiquette répond par la réponse attendue par le lecteur alors le système affichera un message qu'une fausse alerte a été déclenchée. Sinon le tag sera considéré comme illégitime.

6. Conclusion :

Dans le but de répondre aux exigences de sécurité de la technologie RFID concernant le clonage des étiquettes du système, nous avons proposé dans ce chapitre notre système de détection d'intrusions permettant de détecter les comportements anormaux pouvant générer ce type d'attaque.

Dans le chapitre suivant nous allons mettre en œuvre notre système de détection d'intrusions proposé en utilisant le serveur Rifidi Edge et l'émulateur de lecteurs et d'étiquettes RFID (Rifidi) ainsi qu'un environnement de développement adéquat (Eclipse). Nous allons donc détailler l'évaluation de notre solution par la simulation et l'étude des résultats obtenus.

Chapitre V: Simulation et études des résultats

1. Introduction :

Dans le chapitre précédent, nous avons proposé un système de détection d'intrusion pour sécuriser les systèmes RFID contre le clonage des étiquettes RFID. Dans ce chapitre nous allons étudier ses performances à travers son implémentation. Cette étude consiste à simuler le comportement de l'algorithme proposé dans les systèmes RFID et tester sa réponse (les résultats). L'objectif de ce chapitre est donc de démontrer l'efficacité du système de détection proposé en termes de sécurité ainsi que d'autres métriques de performances. Pour cela nous commencerons par définir les outils nécessaires pour l'implémentation et la simulation de notre système. Ensuite, nous décrirons la mise en œuvre de toutes les structures de données et processus décrits dans le chapitre précédent. Nous terminerons ce chapitre par une présentation des résultats relevés lors des tests de performances de notre système.

2. Présentation des outils de développement :

Rifidi est un environnement de développement complet. Il permet de construire une infrastructure « virtuelle » RFID composé de lecteurs, d'étiquettes, et d'évènements RFID qui se comportent comme leurs homologues dans le monde réel. Il comporte trois parties : l'émulateur Rifidi, le serveur Rifidi Edge, et Eclipse.

2.1. L'émulateur Rifidi :

L'émulateur Rifidi permet à un développeur d'imiter fidèlement tout dispositif RFID et simuler des opérations sur les tags. Cet outil accorde un développement rapide de la RFID et donne la possibilité de faire des tests sans nécessité du matériel RFID.

L'émulateur Rifidi est utilisé pour étudier le comportement du système lorsque le lecteur lit une étiquette. Une fois ouvert, l'émulateur Rifidi est une fenêtre composée de quatre parties principales comme illustré dans la figure V.1 :

- la partie supérieure gauche de l'écran contient un cadre qui montre les lecteurs qui sont dans le système.
- la partie inférieure gauche de l'écran est munit d'une liste des étiquettes créées.
- le centre de l'écran, représente la liste des étiquettes du lecteur sélectionné lors de l'exécution.
- le bas de l'écran comporte la console qui permet de visualiser le comportement des tags (tiquettes) lues.

L'utilisation de l'émulateur Rifidi est simple. La première étape consiste à ajouter au moins un lecteur, puis sélectionner un type de lecteur, donner un nom pour ce dernier, régler le port, définir les GPIOs, cliquer sur le bouton *finish* et le lecteur est ajouté. Après ces étapes le système est prêt en cliquant sur le bouton de lecture, il est possible de démarrer l'émulation. Il est possible de créer de nouveaux lecteurs en cliquant simplement sur le symbole «+» de la partie supérieure gauche.

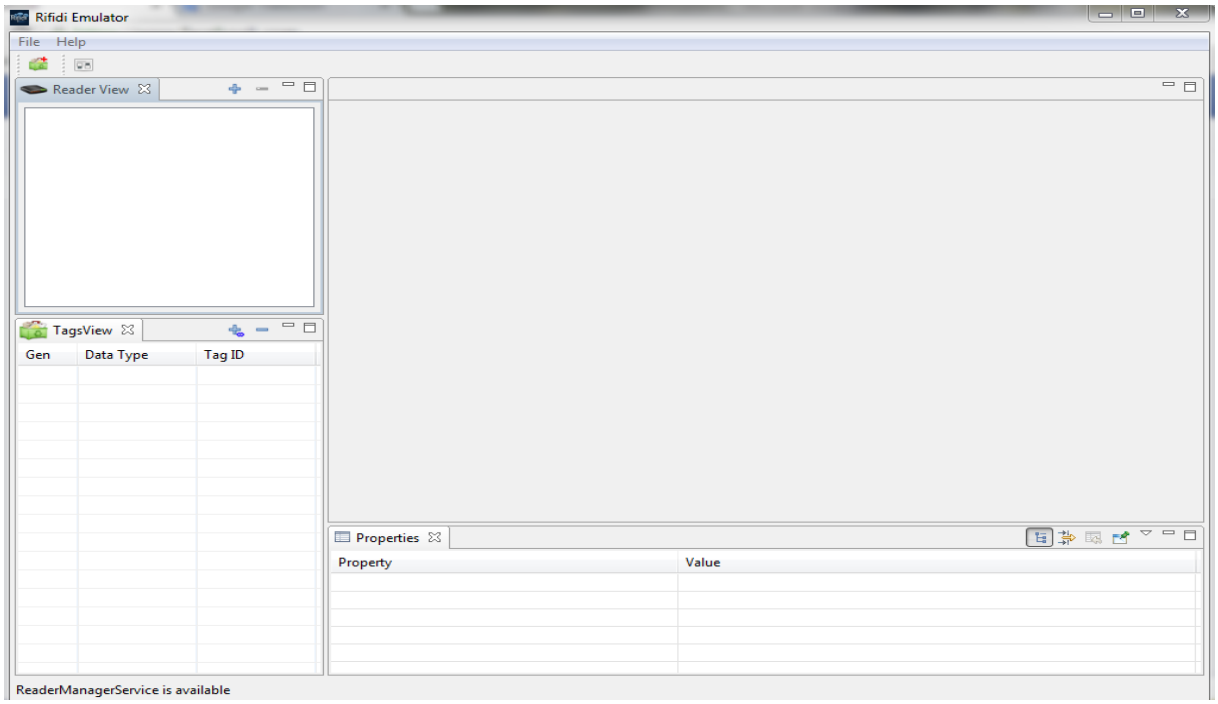


Figure V.1: l'émulateur Rifidi

Le type de lecteur est émulé comme le montre la Figure V.2

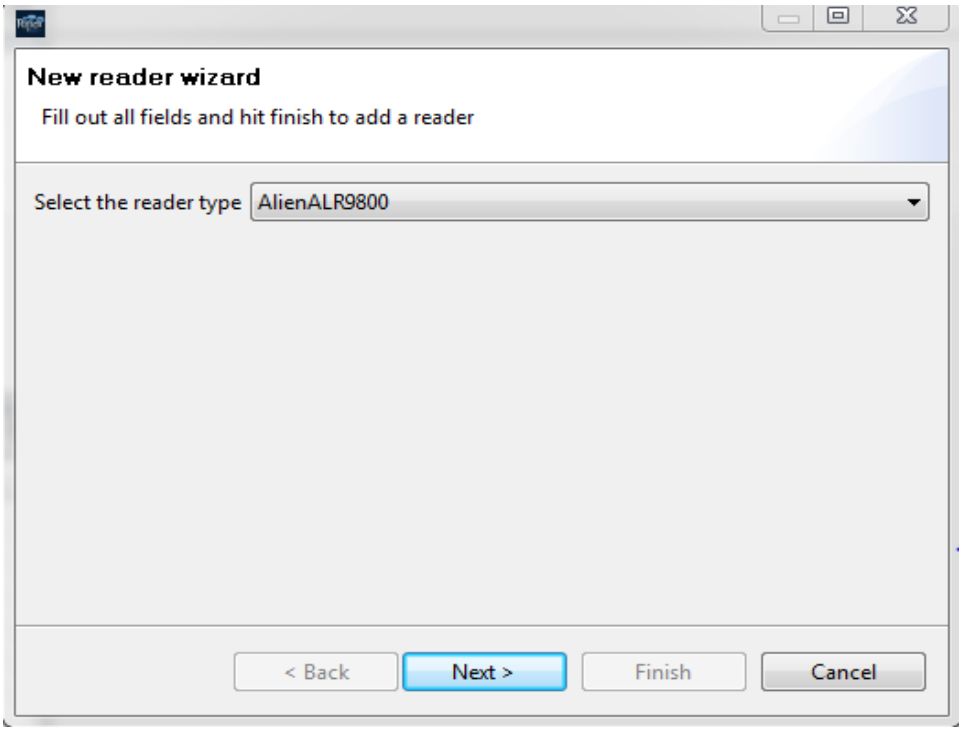


Figure V.2: sélection du type du lecteur.

Après avoir sélectionné un lecteur particulier, il est démarré comme indiquer dans la Figure V.3.

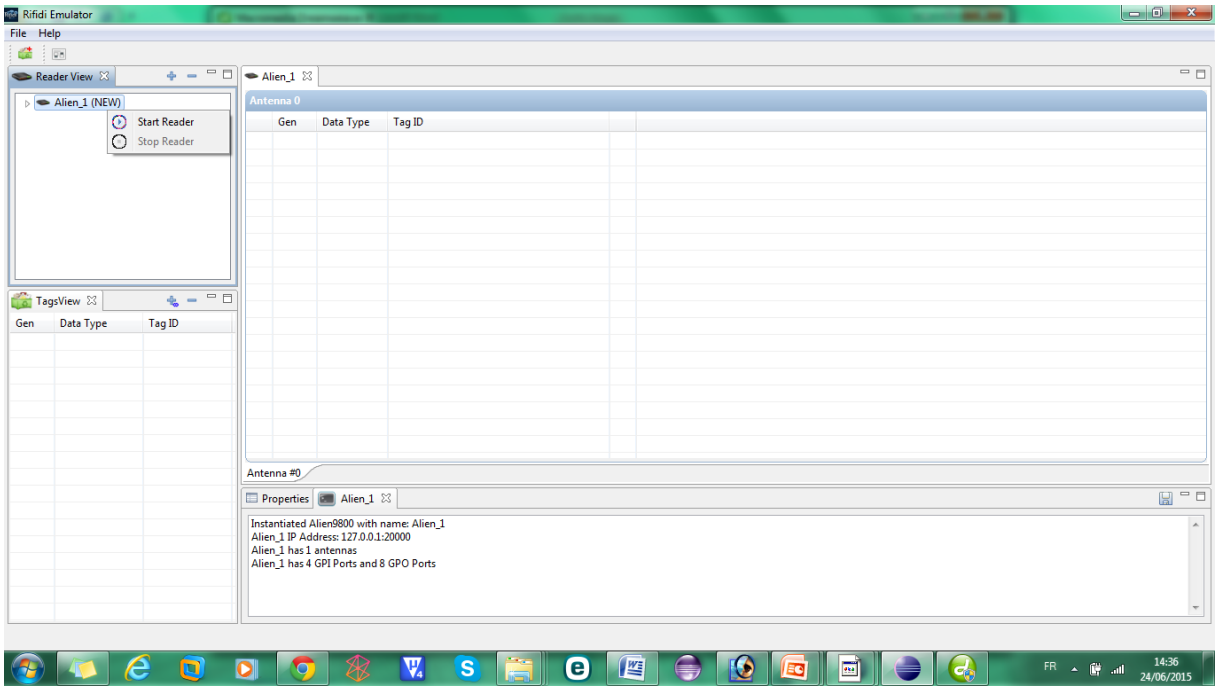


Figure V.3: démarrer le lecteur.

De manière similaire aux lecteurs les étiquettes peuvent être créées conformément à la Figure V.4 en cliquant sur le « + » de la partie inferieure gauche de l'interface principale du l'emulateur :

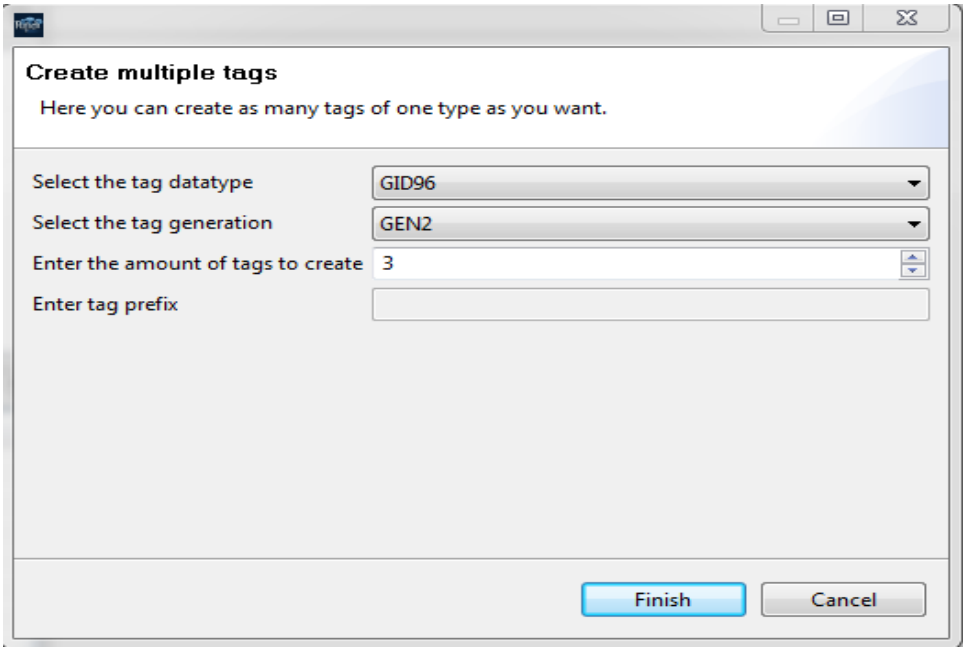


Figure V.4 : création des tags.

Les propriétés du lecteur doivent être modifiées pour qu'il communique avec les étiquettes. Le lecteur commence à communiquer avec les étiquettes comme l'indique la Figure V.5. La communication est visualisée à l'aide d'un lecteur Alien (voir l'Annexe B) ou en utilisant le **telnet.**

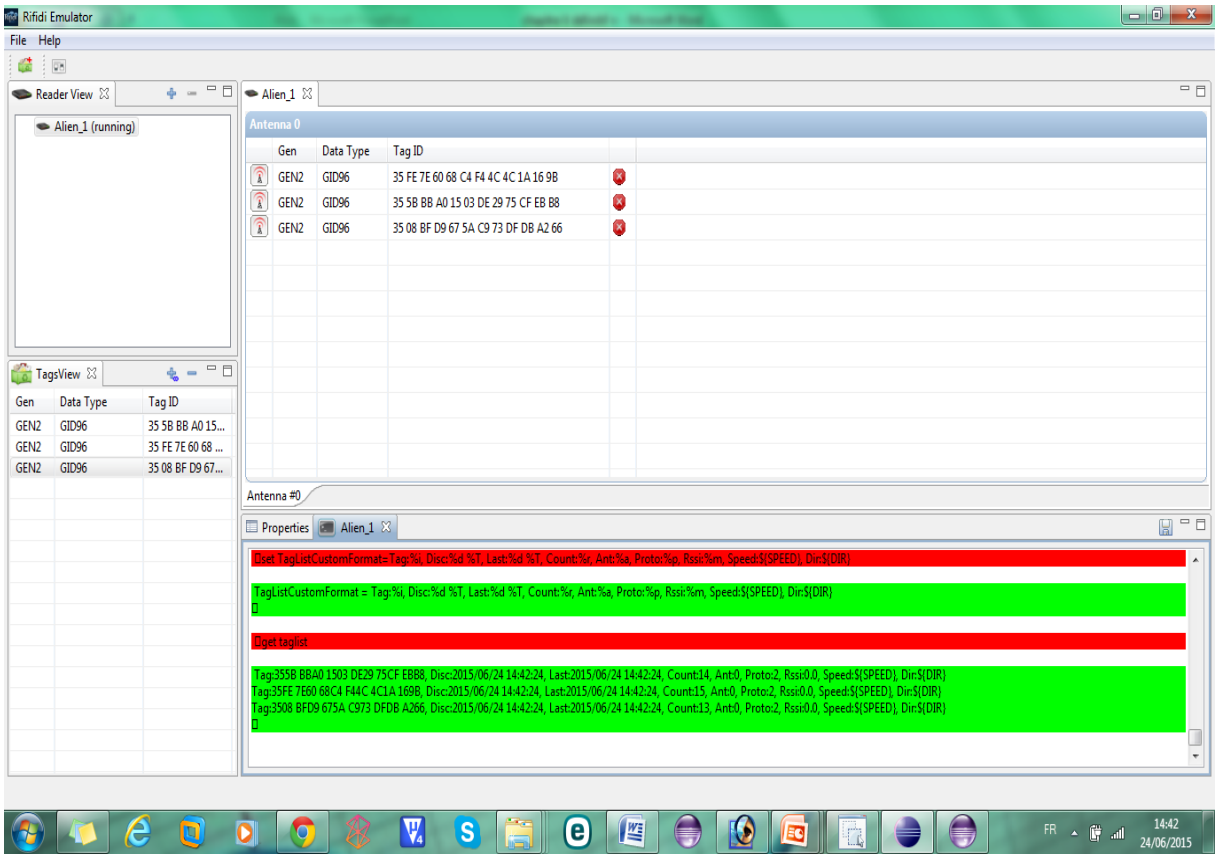


Figure V.5 : communication entre le lecteur et les tags.

2.2. Rifidi Edge server :

Le serveur Rifidi Edge est une plate-forme middleware d'application qui fournit aux développeurs un moyen de développer et de déployer des applications RFID. Les caractéristiques et les outils disponibles sont dans le Kit de Développement Standard Rifidi Edge server (SDK).

Le serveur Edge est téléchargé avec deux programmes :

Edge server : qui fait le travail de base de connexion, la collecte d'informations des tags et assure que les données soient disponibles et livrées aux lecteurs.

Workbench : est l'interface utilisateur qui permet le contrôle du serveur, l'enregistrement et l'accès aux informations des lecteurs et des tags RFID.

- **Installation du Rifidi Edge :**

1. Lancer le fichier d'installation.

2. Choisir le dossier ou installer le serveur.

3. Suivre le reste des étapes du processus d'installation.

- **Exécution du Rifidi Edge** :

1. Trouver le raccourcis RifidiEdge dans le menu Démarrer et cliquer dessus.

2. Une console s'affichera, montrant que le serveur a commencé.

- **Execution du Workbench :**

1. Trouver le raccourcis Workbench dans le menu Démarrer et cliquer dessus.

2. Cliquer sur "Edge server" dans l'onglet "Edge Server View".

3. Faire un clic droit sur le serveur Edge, puis cliquer sur "Connect".

- **Configurer le Serveur :**

1. Dans Workbench, clique droit sur Edge Server et sélectionner "New Reader ".
2. Ajouter le lecteur Alien généré avec l'émulateur avec son adresse IP et son port.
3. Définir les autres options souhaitées, puis cliquez sur **"finish"**.
4. Faire un clique droit sur le lecteur créé, puis cliquer sur "Create Session". Une nouvelle session sera créée. Les sessions représentent une connexion physique au lecteur.
5. Ouverture de la session dans la Figure V.6. La lumière de la session doit devenir verte. Cela signifie que la connexion a été établie. Si la lumière est jaune, cela signifie que le serveur tente de faire le lien, mais quelque chose cloche. Dans ce cas il faut s'assurer que l'IP et le port sont corrects et que le lecteur dans l'émulateur a été démarré.

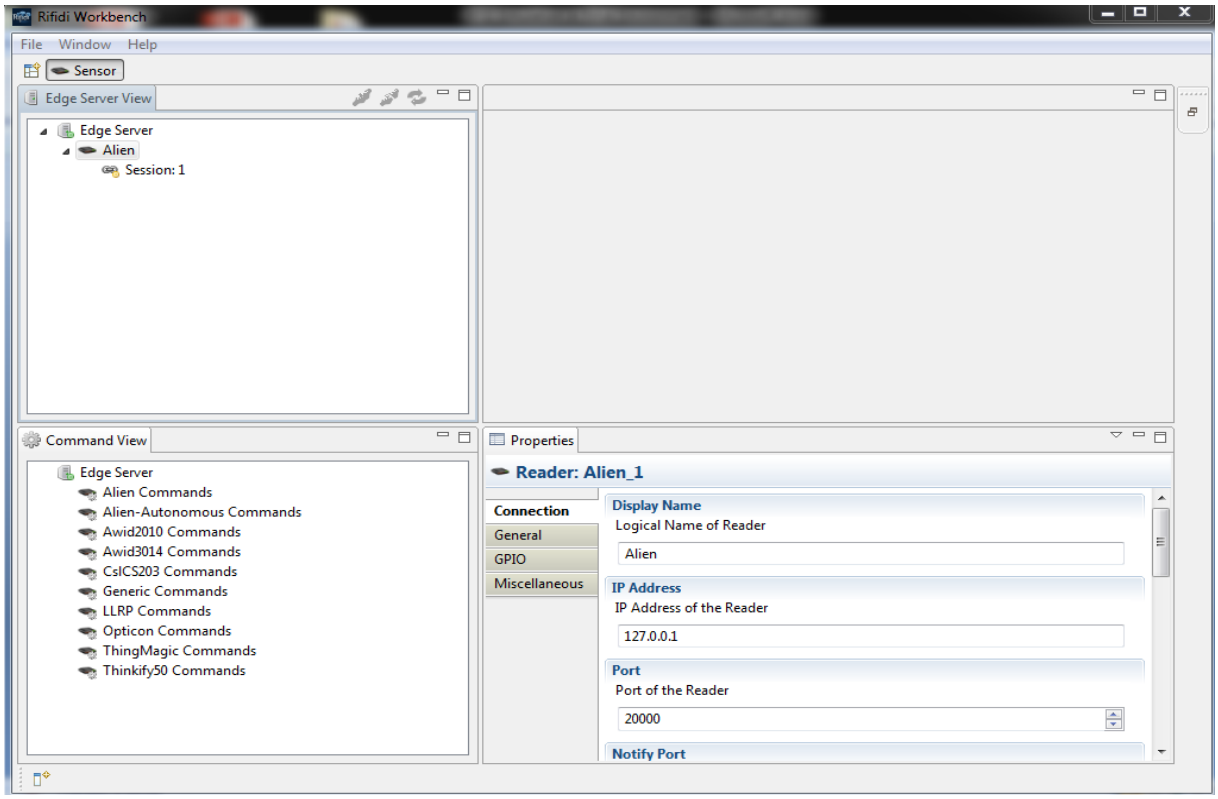


Figure V.6 : configuration du Rifidi Edge server

2.3. Eclipse :

L'émulateur Rifidi est écrit en Java et se compose de plugins Eclipse ce qui fait qu'il est plus facile de compiler et de construire à l'intérieur de l'environnement Eclipse.

Installation d'Eclipse :

a) La version d'Eclipse qu'il faut utiliser est «Eclipse RCP/ Plug-in Developers, car Rifidi ne fonctionnera pas sur les autres versions.
b) Accéder à http://www.eclipse.org/downloads/ et télécharger la version "Eclipse for RCP /Plug-in Developers".
c) Décompresser le paquetage.
d) Double-clique sur le fichier exécutable pour le lancer comme montré dans la FigureV.7

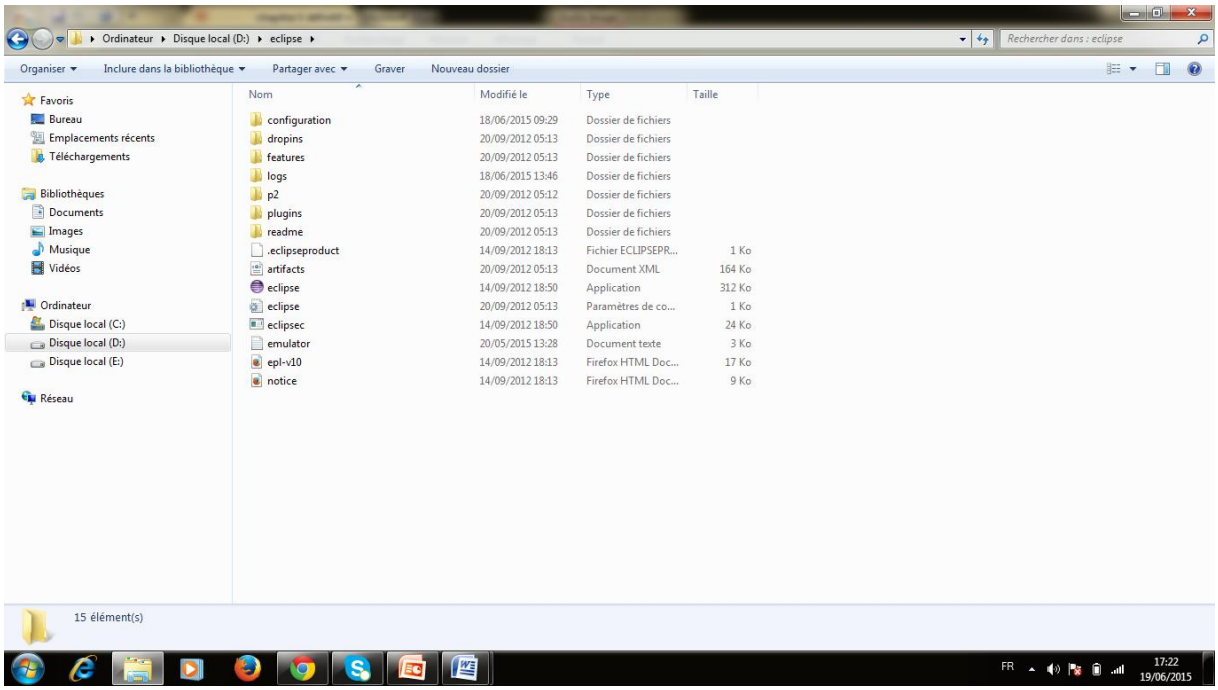


Figure V.7 : lancement d'Eclipse

e) Si Eclipse n'est pas déjà utilisé, il faut sélectionner un espace de travail. Après l'ouverture d'Eclipse aller à workbench.

f) S'il ya un espace de travail existant déjà, il faudra en créer un nouveau.
Aller à file -> switch workspace -> other
Sélectionner un nouveau répertoire pour votre espace de travail Rifidi (figure V.8).

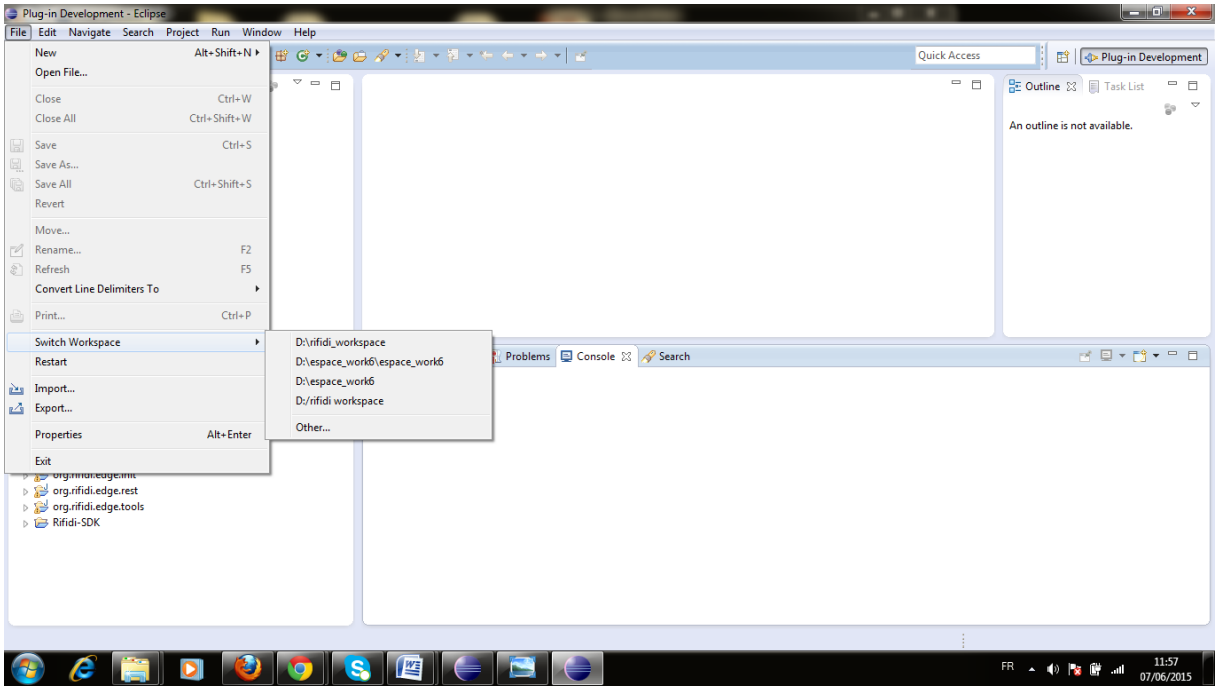


Figure V.8 : sélection du workspace

3. Implémentation du système proposé :

Dans cette partie, nous allons présenter l'implémentation de la solution que nous avons précédemment présentée. Nous commencerons par la description des structures échangées entre les différents composants du système RFID, puis nous nous étalerons sur l'implémentation des algorithmes de détection utilisés et nous terminerons par la présentation de l'implémentation de l'attaque choisie et tester les performances du système proposé.

Utiliser le projet template pour implémenter notre système de détection d'intrusions :

Notre système de détection d'intrusion surveille une zone de lecture d'un lecteur Alien, pour détecter l'arrivée et le départ des étiquettes, dans le but de détecter les étiquettes qui ne respectent pas les règles définies dans le chapitre IV.

L'arrivée et le départ des étiquettes dans la zone de lecture sont signalés comme des évènements « TagArrived » et « TagDeparted ».La gestion de ces évènements revient à créer des classes qui vont les envoyer via Esper, qui est un moteur de traitement d'événements. Il permet aux utilisateurs d'insérer des événements sous la forme d'objets Java dans le moteur et chercher des modèles dans ces données en utilisant des requêtes comme suit :

La classe qui signale l'arrivée d'un tag dans la zone de lecture :

```
public class DockDoorArrivedEvent {
	private final TagReadEvent tag;
	public DockDoorArrivedEvent(TagReadEvent
tag) {
		super();
		this.tag = tag;
	}
	public TagReadEvent getTag() {
		return tag;
	}

}
```

La classe qui signale le départ d'un tag de la zone de lecture :

```
public class DockDoorDepartedEvent {
	private final TagReadEvent tag;
	public
DockDoorDepartedEvent(TagReadEvent tag) {
		super();
		this.tag = tag;
	}
	public TagReadEvent getTag() {
		return tag;
	}
}
```

Créer une règle Esper et ajouter ces deux évènements dans la méthode _start() de la classe templateApp comme suit :

```
addEventType(DockDoorArrivedEvent.class);
addEventType(DockDoorDepartedEvent.class);
```

Dans META_INF modifier Spring.xml le fichier qui permet d'jouter un ou plusieurs services et de les injecter dans l'application:

- Créer une nouvelle instance de templateApp avec index= "0"(groupe de l'application), value=″Templates"(le nom du groupe) et index="1" (l'index de l'application dans le groupe auquel elle appartient), value= "TemplateApp"(le nom de l'application).
- Ajouter le nom de la zone de lecture.
- Enregistrer l'application dans le service OSGI

Ajouter le dossier Template à Rifidi_SDK qui contient les propriétés de l'application et de la zone de lecture utilisée.

Dans ce qui suit nous présenterons la procédure de détection d'intrusion que nous avons implémentée :

```
Procédure Détection_Intrusions()
Debut
 Pour chaque tag reçu faire ;
Si (Validation (tag)==faux) Alors
                                    Signaler une alerte ;
Finsi
Si  ( (tempsactuel-timestamps)== tempsmax )Alors
 /* tempsmax : l'intervalle du temps maximal */
 /*   que le tag peut passer dans la zone de lecture*/
                                                Si (Validation (tag)==faux) Alors
                                                                    Signaler une alerte ;
                                                Finsi
Finsi
 Fin.
```

L'algorithme de la fonction validation :

```
Fonction Validation(TagReadEvent)
Debut
  Récupérer l'identifiant du tag ;
  Envoie d'un challenge au tag ;
  Si (réponse_reçue==réponse_attendue) Alors  /*réponce_reçue : réponse envoyée par le tag*/
                                              /*réponse_attendue: réponse calculée par le lecteur*/
                                            Retourner vrai ;
  Sinon retourner faux ;
  Finsi ;
  Fin.
```

❖ **Type d'étiquettes utilisées :**

La structure générale des encodages EPC(Electronic Product Code) d'un tag est une représentation binaire, constituée d'un à plusieurs niveaux : un en-tête de longueur variable suivie par une série de champs numériques, la structure de l'identifiant et la fonction de l'étiquette sont entièrement déterminée par la valeur de l'en-tête.

Dans notre simulation nous avons utilisé les étiquettes GID96 General Identifier (GID). L'identificateur général est défini pour un EPC 96 bits. Il est composé de trois champs : le numéro du gérant général (General Manager Number), classe d'objets (Object Class) et d'un numéro de série (Serial Number). Le codage de la GID comprend un quatrième champ, désigné par l'en-tête, pour garantir l'unicité dans l'espace EPC, comme indiqué dans le tableau suivant :

	Header	General Manager Number	Object Class	Serial Number
GID-96	8 bits	28 bits	24 bits	36 bits
	0011 0101	268 435 455 (valeur décimale max)	16 777 215 (valeur décimale max)	68 719 476 735 (valeur décimale max)

Tableau V.1 : Présentation du tag General Identifier GID-96

Le numéro General Manager identifie essentiellement une entreprise ou une organisation, qui est une entité responsable du maintien des numéros dans les domaines suivants : classe d'objet et numéro de série. EPCglobal attribue à chaque entité un numéro General Manager unique.

Le troisième composant est une classe d'objets, et est utilisée par une entité de gestion EPC pour identifier une classe ou un type d'objets. Ces numéros de classe d'objet, doivent être uniques dans chaque domaine General Manager Number.

Le numéro de série, est unique au sein de chaque classe d'objet. En d'autres termes, l'entité de gestion est responsable de l'attribution unique des numéros de série pour chaque instance au sein de chaque classe code d'objet.

4. Evaluation expérimentale :

Dans le but de tester la performance de notre solution proposée pour la détection de l'intrusion clonage nous avons simulé des attaques de clonage en récupérant l'identifiant des étiquettes reçues à partir de l'émulateur Rifidi afin de s'authentifier comme étant des tags légitimes.

Métrique d'évaluation du système proposé :

La mesure utilisée pour tester le rendement du système proposé :

Taux de faux négatifs: cette notion concerne le taux d'attaques non détectées ayant réussies à accéder au système RFID. Dans notre cas le taux de faux négatifs (FNR : False Negative Rate) est calculé avec la formule suivante [43] :

$$FNR = \frac{FN}{TP+FN}$$

TP : représente le nombre des activités malveillantes détectées par le système.

FN : représente le nombre d'attaques non détectées par le système.

Résultats et interprétations :

Nous avons utilisé un lecteur de type Alien parce qu'il possède des plugins (c'est des paquets qui complètent des logiciels hôtes pour leurs apporter de nouvelles fonctionnalités) plus performants par rapport aux autres lecteurs du fait qu'il est le premier lecteur implémenté dans l'émulateur.

Nous avons défini un système de 200 tags, et le nombre d'étiquettes clonées insérées varie entre 20, 50, 100, 150 ou 200. Nous avons pu évaluer notre approche en utilisant le taux des faux négatifs et le taux d'alertes, comme décrit ci-dessous :

La figure suivante représente le taux de faux négatifs produit par notre système :

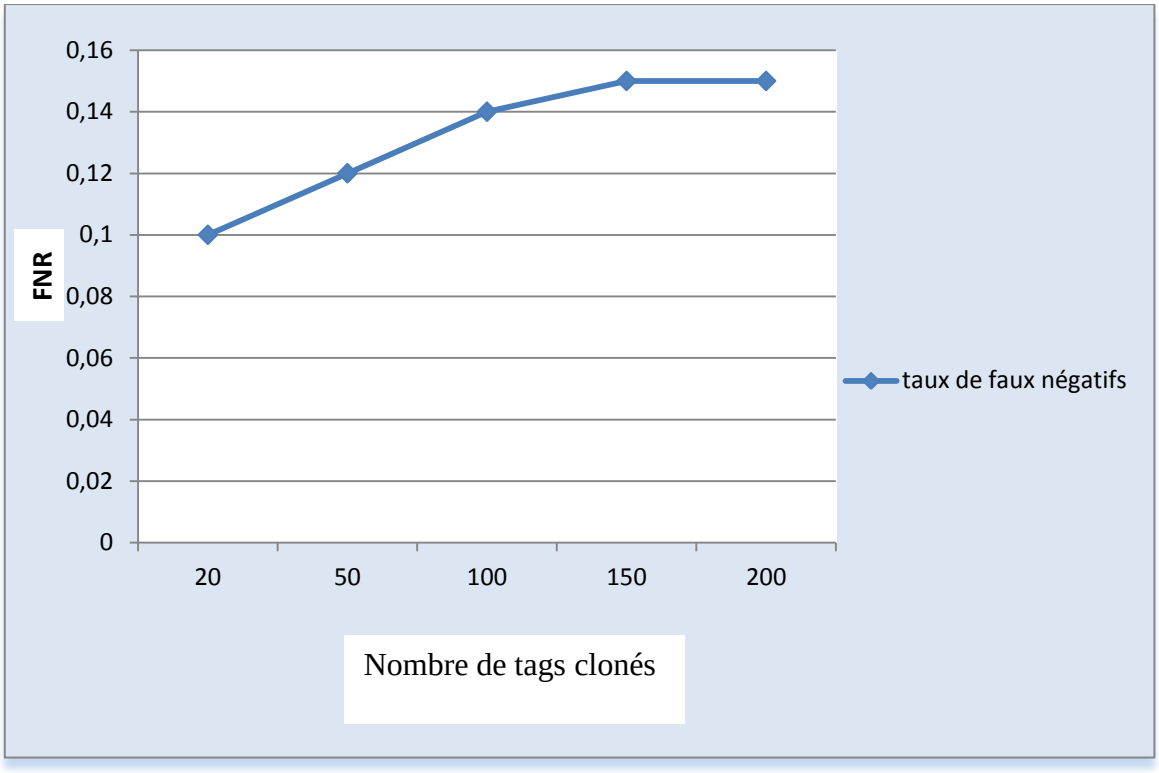


Figure V.9: Le taux de faux négatifs.

La figure ci-dessus montre la variation du taux de faux négatif en fonction du nombre de tags clonés (intrus) dans le système. Cette figure montre que le taux de faux négatif (FNR) ; ie le nombre d'attaques non détectées augmente avec l'augmentation du nombre d'intrus. Mais, ce taux reste acceptable malgré le grand nombre d'intrus (pour 200 intrus juste 15 % ne sont pas détectés). Donc, d'après ces résultats, nous pouvons constater que notre système a un taux de détection élevé (sur 200 intrus on a 85% d'intrus détectés). Même si le taux de détection diminue avec l'augmentation du nombre d'attaques, nous sommes toujours en mesure d'atteindre un taux de détection considérable.

5. Conclusion :

La première partie de ce chapitre a été consacrée à la présentation des outils de développement dont l'émulateur Rifidi, le serveur RifidiEdge, Workbench, puis nous avons présenté l'implémentation du système de détection d'intrusions proposé ainsi que l'attaque du clonage d'étiquettes RFID au quelle le SDI doit faire face.

Dans la deuxième partie nous avons présenté et discuté les résultats des simulations effectuées.

Par ailleurs, nous avons constaté que les tests de performances effectués sur la sécurité offerte par le système ont montré que ce dernier répond aux critères de performances souhaités.

Conclusion générale

Conclusion générale

La technologie RFID est parvenue à un stade de développement où la sécurité de l'information et la protection de la vie privée ont été reconnues comme des obstacles à la généralisation de son utilisation. En effet, leurs applications sont de plus en plus nombreuses et diversifiées. La problématique majeure de cette technologie est la sécurité.

Les RFIDs sont très vulnérables à de multiples attaques vu leurs contraintes critiques. Beaucoup de mécanismes ont été proposés pour assurer la sécurité dans les RFIDs tels que : la cryptographie, l'authentification, la détection d'intrusions.

Dans ce travail nous nous sommes focalisés sur la sécurité dans les systèmes RFID. Pour cette raison nous avons étudié différents travaux proposés pour la détection d'intrusion, puis nous avons exposé un système de détection d'intrusions qui détecte le clonage d'étiquettes dans les systèmes RFIDs.

Vu que le clonage d'étiquettes est l'une des menaces les plus graves pour la sécurité des systèmes RFID, nous avons proposé un système de détection d'intrusion qui se base sur la technique basée connaissances pour la détection du clonage afin d'atteindre un taux élevé de détection. L'objectif de ce système est d'offrir un niveau de sécurité acceptable et réduire le taux de fausses alertes.

Les résultats de simulation ont montré que notre SDI peut découvrir l'intrusion de clonage dans les RFIDs de manière efficace, ce dernier assure un taux de détection élevé, ce qui a montré que notre système répond aux objectifs souhaités.

Cela dit, plusieurs perspectives sont envisagées pour notre projet tel l'utilisation de la cryptographie ainsi que l'utilisation de la force du signal reçu RSSI pour localiser les étiquettes légitimes et réduire le taux de fausses alertes produites par notre système tout en prenant compte du type d'étiquettes utilisées.

Bibliographies

Bibliographie :

[1] : Dat-Son NGUYEN, « Développement de Capteurs sans fil basés sur les Tags RFID UHF passifs pour la détection de la Qualité des aliments». Thèse de doctorat, Université de GRENOBLE, Septembre 2013

[2] : Loïc Schmidt, « Passage à l'échelle des intergiciels RFID pour l'informatique diffuse », Thèse de doctorat (spécialité Informatique), Université Lille 1, décembre 2010.

[3]: S. Tedjini, E.Perret, «Radio-Frequency Identification Systems and Advances in Tag Design», Invited paper, Radio Science Bulletin No 331, pp. 9-20, December 2009.

[4] : Pisaneschi Thomas, « Mise en place d'un système RFID pour une entreprise de panneaux laqués haute finition **».**Rapport de fin d'études, université Henri Poincaré, 2011

[5]EPCGlobal. Class 1 generation 2 UHF air interface protocol standard version 1.0.9. http://www.epcglobalinc.org, January 2005.

[6] : BACHOTI Youssef, « Principe fondamental de la RFID » Projet de fin d'étude, Télécom SudParis, janvier 2011.

[7] : Frédéric LETIENT, « Etat de l'art et applications des RFID », Epreuve TEST Travail d'Etude et de Synthèse Technique en ELECTRONIQUE, Grenoble, Juin 2008.

[8] : Laurent Coutelier, Bruno Le-Roux, « Annexe La technologie RFID », 2013.

[9] : Gildas Avoine, « RFID et sécurité font-elles bon ménage ? », Massachusetts Institute of Technology Cambridge, MA 02139, USA

[10] : Gildas Avoine. « Cryptography in Radio Frequency Identification and Fair Exchange Protocols », PhD thesis, EPFL, Lausanne, Switzerland, December 2005.

[11] : Gildas Avoine, «sécurité de la RFID : le cas du passeport biométrique » ,UCL, Louvain-la-Neuve, Paris, novembre 2007.

[12] : LABED Ines,Proposition d'un système immunitaire artificiel pour la détection d'intrusions, magister en informatique,Université de Constantine, 2005/2006

[13]: Syed Ahson, Mohammad Ilyas, « Applications, Technology, Security, and Privacy » ,RFID HANDBOOK,1953

[14] : Torstein Haver , « Security and Privacy in RFID Applications », Master of Science in Communication Technology,Norwegian University of Science and Technology Department of Telematics, juin 2006

[15] :Coulton, P., Rashid, O., and Bamford, W., « Experiencing 'touch' in mobile mixed reality games,Proceedings of The Fourth Annual International Conference in Computer Game Design and Technology », Liverpool, November 2006.

[16]: NFC Forum, NFC Data Exchange Format (NDEF) Technical Specification NDEF 1.0, NFCForum-TS-NDEF_1.0, 24th July 2006.

[17] :Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo, « Security Analysis of a Cryptographically-Enabled RFID Device » The John Hopkins University Information Security Institute and RSA Laboratories, 28 January 2005.

[18] : Léonard Gross, « Sécurité RFID et préservation de la sphère privée », Institute for Information and Communication Technologies, Travail de diplôme, Suisse, janvier 2007

[19] : Monty L. , « Vulnérabilités des RFID », article,2010.

[20] : S. Brands et D.Chaum, « Distance-BoundingProtocols », rapport,1993

[21]: Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, « Is Your Cat Infected with a Computer Virus » in PerCom 2006. Pisa, Italy, 2006.

[22]: SYED AHSON, MOHAMMAD LYAS, «RFID HANDBOOK, application, technology, security, and privacy», CRC Press, 2008.

[23]: Annalee Newitz, «The RFID Hacking Underground», article, Wired Magazine, 14 May 2006 http://www.wired.com/wired/archive/14.05/rfid.html?pg=1&topic=rfid&topic_s .

[24]: Geethapriya Thamilarasu, Ramalinga Sridhar, « Intrusion Detection in RFID Systems », University at Buffalo, Buffalo, USA.

[25]: T. Karygiannis, B. Eydt, G. Barber, L.Bunn, and T. Phillips, « Guidelines for securing radio frequency identification (RFID) systems », NIST Special Publication 800-98, April 2007.

[26] : OCDE, « Sécurité de l'information et protection de la vie privée, Application Impacts et initiatives nationales », rapports de l'OCDE sur l'identification par radiofréquence (RFID), juin 2008.

[27]: Nathalie Dagorn, « Détection et prévention d'intrusion : présentation et limites », rapport de recherche, Université de Nancy1, France, 2006.

[28]: Guillaume Hiet, « Détection d'intrusions paramétrée par la politique de sécurité grâce au contrôle collaboratif des flux d'informations au sein du système d'exploitation et des applications : mise en oeuvre sous Linux pour les programmes Java », thèse de doctorat, Université de Rennes 1, France, 2008.

[29]:http://www.cisco.com;http://www.nfr.net;http://www.snort.org;http://all.net/dtk/dtk.html; http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php

[30] : Klaus Müller, « IDS-système de détection d'intrusion », 2005, http://www.linuxfocus.org/Francais/July2003/article294.shtml.

[31]: LABED Ines, « Proposition d'un système immunitaire artificiel pour la détection d'intrusions », magister en informatique, Université de Constantine, 2005/2006

[32]: Stephen E. Smaha, « Haystack : An Intrusion Detection System », In Fourth Aerospace Computer Security Applications Conference, Tracor Applied Science Inc., Austin, TX, 1988.

[33]: M. M. Sebring, E. Shellhouse, M. E. Hanna, and R. A. Whitehurst, « Expert system in intrusion detection: A case study », In Proceedings of the 11th National Computer Security Conference, 1988

[34] : Teresa F.Lunt, R Jagannathan, Rosanna Lee, Sherry Listgarten, David L. Edwards, Peter G. Neumann, Harold S. Javitz, and Al Valdes, « Ides : The enhanced prototype, a real-time intrusion detection system », Technical report, CSL SRI Internationnal, Computer Science Laboratory, Menlo Park, USA, Octobre 1998.

[35]: Teresa F. Lunt, « IDES : An Intelligent System for Detecting Intruders », In Proceedings of the symposium : Computer Security, Threat and Countermeasures, Rome, Italy, 1990

[36] : Teresa F. Lunt, Ann Tamaru, Fred Gilham, R. Jagannathan, Caveh Jalali, and Peter G Neuman, « A real-time intrusion detection expert system (ides) », Technical report, , SRI Internationnal, Computer Science Laboratory, USA, Février 1992.

[37]: Geethapriya Thamilarasu and Ramalingam Sridhar, « Intrusion Detection in RFID Systems », Article, University at Buffalo, Buffalo, USA.

[38]: Luke Mirowski and Jacky Hartnett, **«** Deckard: A System to Detect Change of RFID Tag Ownership**» ,** IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7, University of Tasmania, Hobart, Australia, July 2007

[39]: M. Esposito and G. Della Vecchia, « An Ontology-based Intrusion Detection for RFID Systems », Article, University of Naples "Parthenope", Centro Direzionale , Naples, Italy.

[40]: Nathalie Dagorn, « Détection et prévention d'intrusion : présentation et limites », Research Report, 2006.

[41]: F. Meunier, « Détection d'intrusions: notions avancées de NIDS axées sur le logiciel ManHunt (Recourse Technologies) », Rapport, Watch4net, Août 2002

[42]: Herve Schauer Consultants, « La détection d'intrusion», Présentation : extrait du cours sécurité TCP/IP du Cabinet HSC, Mars 2000.

[43]: Luke Thomas Mirowski, « Detecting Clone Radio Frequency Identification Tags », University of Tasmania, November, 2006.

Annexes

Annexe A : Rifidi Edge server

1. Description du Rifidi Edge server :

Le serveur Rifidi Edge est une plate-forme d'application qui fournit aux développeurs un moyen de développer et déployer des applications RFID. Les caractéristiques et les outils disponibles pour les développeurs d'applications RFIDs sont dans le Kit de développement standard Rifidi Edge server (SDK).

Ce qui suit aide à se familiariser avec la SDK du serveur Rifidi Edge. Il décrit la structure de la SDK, comment mettre en place un environnement de développement, et comment créer votre premier projet d'application Rifidi, comment l'exporter et le déployer.

Vue de l'ensemble de la SDK :

La SDK contient les fichiers et les dossiers suivants:

 exemples - Contient des exemples d'applications Rifidi y compris un modèle pour vous aider à démarrer

 lib - Contient tout le code nécessaire pour exécuter le serveur Rifidi Edge.

 docs - Contient tous les documents

 launch file- La configuration d'exécution par défaut pour exécuter le serveur Rifidi Edge à partir d'Eclipse

 target file- Le fichier qui indique à Eclipse où trouver les dépendances nécessaires pour exécuter le serveur edge.

2. Mise en place d'un environnement de développement :

L'environnement qui permet de développer une application Rfid en utilisant le serveur Rifidi Edge est Eclipse. Pour cela il faut suivre les instructions sur la page wiki pour importer la SDK dans l'espace de travail Eclipse.

2.1. Importation du projet Template :

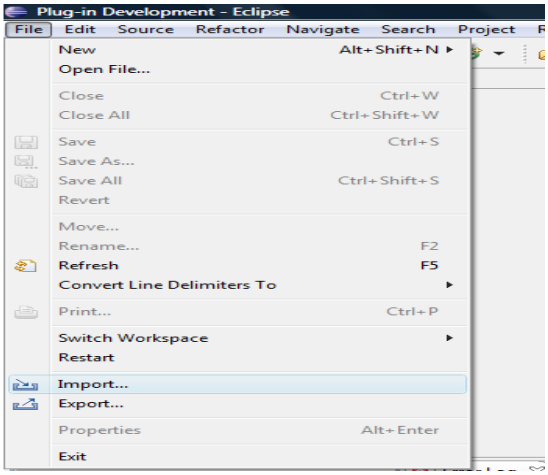
Maintenant que l'environnement de développement est mis en place, il y a l'envie de créer un projet d'application Rifidi. Au lieu de suivre les instructions étape par étape sur la façon de mettre en place une application, il est recommandé d'importer le **projet Template** à partir du répertoire des exemples dans la SDK. Pour cela il faut :

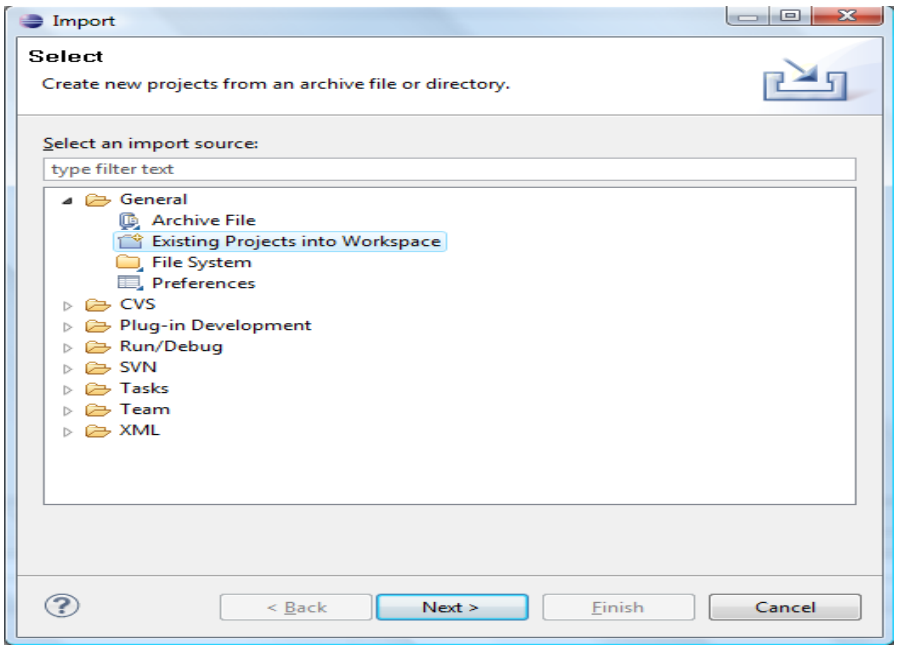
1. File->Import
2. Choisir dans General-> Existing Projects into Workspace
3. Cliquer sur le bouton Parcourir à côté de "Select root directory"
4. Accéder au répertoire de SDK dans le dossier workspace.

5. Sélectionner 'org.rifidi.app.template'

6. Sélectionner ‘Copy projects into workspace’

7. Cliquer sur finish.



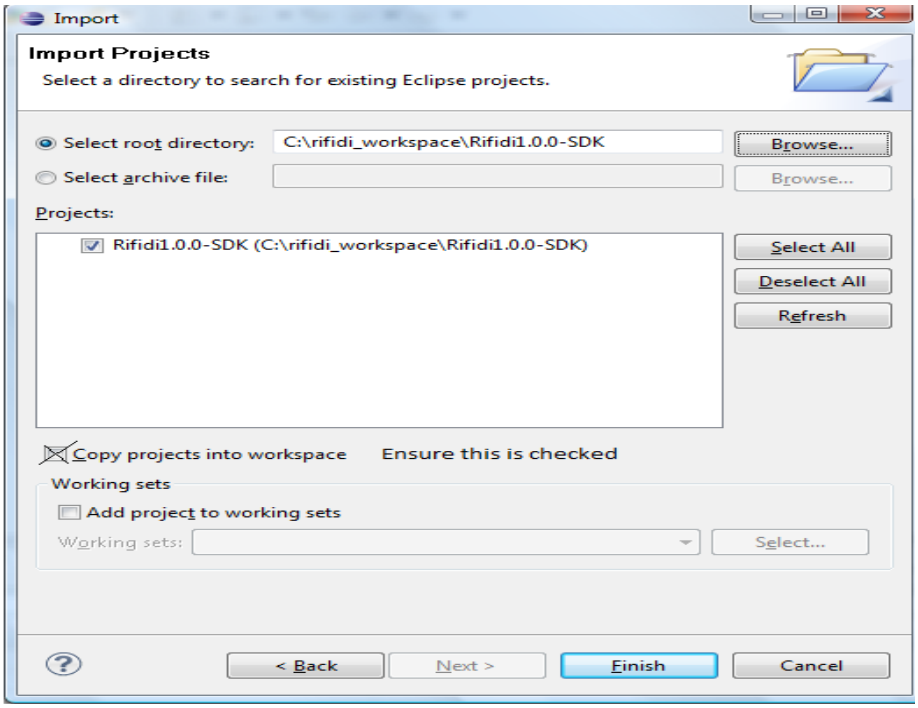


2.2. Exécution du projet

Une fois le **Template** importé, il est modifié en mettant une ligne d'impression dans la méthode **start** de sorte à voir si le projet est en cours d'exécution ou a commencé. Maintenant, le serveur Edge peut s’exécuter à partir d'Eclipse.

1. Ouvrir le run configuration (Run-> Run Configurations).
2. Sélectionner le projet 'org.rifidi.app.template' dans run configuration.

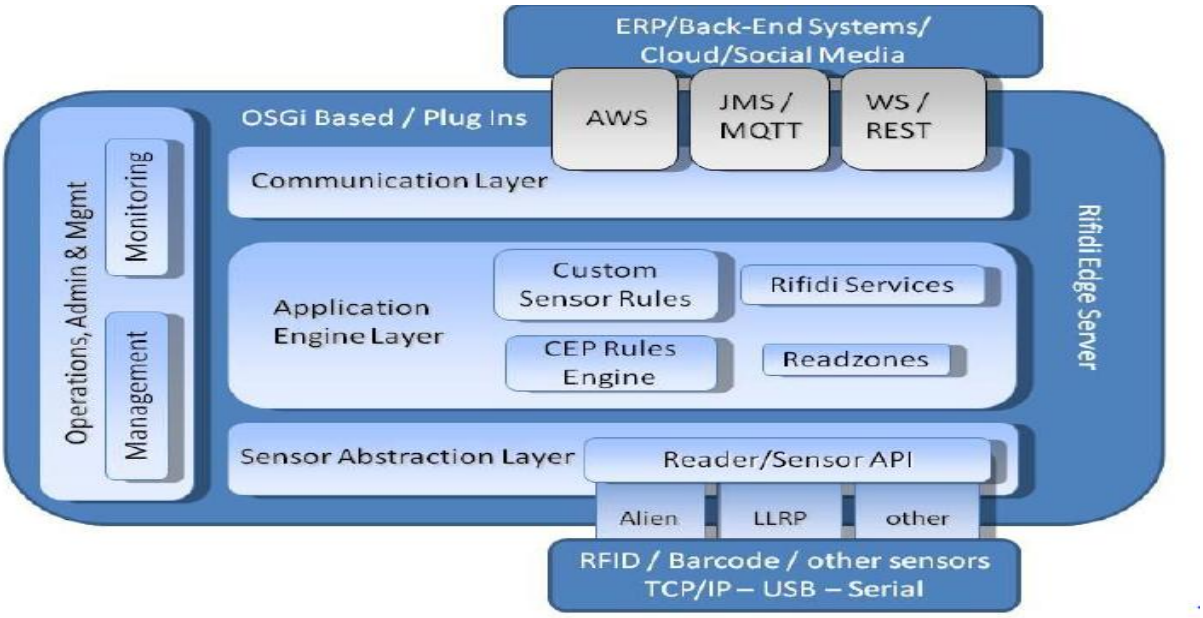
3. Cliquer sur Apply et Run.



À ce stade, la sortie de journalisation dans la console devrait se voir pour indiquer que le serveur Edge a été lancé.

3. Architecture du serveur Rifidi Edge

L'architecture du serveur Rifidi Edge à un niveau élevé. Le serveur Edge est divisé en trois couches conceptuelles. La couche capteur d'abstraction fournit une API commune pour intégrer des capteurs pour recueillir divers types de données à partir d'eux. La couche Application Engine effectue des règles de traitement sur les données. La couche de communication (parfois appelée la couche d'intégration) fournit un moyen pour intégrer les événements recueillis dans la couche d'application avec d'autres systèmes (tels que des bases de données ou des systèmes ERP). En outre, à partir de la version 3.1, le serveur Rifidi Edge offre une couche Operation, Administration & Management qui expose de nombreuses fonctions internes via une interface de services.



Architecture du Rifidi Edge Server

- **Sensor Abstraction Layer**

Le but du serveur Edge est de se connecter à tout type de senseurs (capteurs) (par exemple, les lecteurs RFID, lecteurs de codes à barres, périphériques mobiles) et de recueillir des informations de leur part. Dans de nombreux scénarios, cela consiste à se connecter à un lecteur (comme Alien 9800, Motorola LLRP, etc.), et de collecter des informations de l'EPC. Toutefois, le serveur Edge est conçu de façon à pouvoir collecter toutes sortes de données (actives, passives, etc.) à partir de nombreux types de dispositifs. Cette couche permet aux utilisateurs de se connecter aux appareils pour recueillir les données requises pour l'application.

- **Application Engine Layer**

Pour la plupart des applications, il est préférable de ne pas sauvegarder tous les cas produits par les capteurs. De nombreux capteurs peuvent envoyer 1000 événements par seconde, un grand nombre de ce qui pourrait être des doublons. Il y a des applications qui s'intéressent aux événements de niveau supérieur plus qu'aux premiers événements.

Complex Event Processing (CEP) est un paradigme de visualisation des données comme des événements éphémères (ie un courant constitué d'événements non-persistant). Rifidi Edge server utilise un processeur Complex Event appelé Esper qui permet d'écrire des requêtes en utilisant une syntaxe de type SQL. Un exemple de requête pour obtenir des étiquettes à partir d'un lecteur particulier pourrait ressembler à ceci:

```
select * from ReadCycle where ReaderID='gate_1'
```

La couche application permet aux développeurs d'écrire la logique qui utilise Esper pour filtrer les événements globaux produits par le capteur. Les applications de cette couche peuvent effectuer la logique d'entreprise personnalisée basée sur les étiquettes qui sont vues. Par exemple, une application peut alerter un responsable de l'entrepôt via un e-mail si une étiquette qui correspond à un certain modèle est vue dans un domaine particulier.

- **Communication Layer :**

Après avoir traité les données, il a probablement besoin de les remettre à une sorte de système de fonction de l'application. Par exemple, certains utilisateurs voudraient que les données soient stockées dans une base de données, d'autres voudraient qu'elles soient remises à une interface utilisateur riche de quelque sorte. Le Rifidi Edge est construit en plusieurs connecteurs, à savoir JMS et des services Web. Cependant, comme il dépend de l'application, il est possible d'écrire votre propre connecteur (comme une connexion TCP / IP socket) si l'application en a besoin.

- **Application Layer :**

Le but de la couche capteur (sensor) est de recueillir des données provenant des capteurs et les mettre dans Esper. Le but de la couche d'application est de réaliser la logique de gestion sur les données que les capteurs recueillent. La couche application est destinée à être suffisante pour supporter une grande variété d'applications générales, mais fournissent des outils qui sont communs à de nombreuses applications.

4. Rifidi API Application :

Les Applications Rifidi sont au cœur de la couche application, leurs classes sont utilisées pour ajouter des déclarations personnalisées à Esper. Pour regarder des événements, il faut voir les services Rifidi les intégrer avec les infrastructures existantes, telles que les bases de données et les files d'attente JMS.

Afin de fournir un développement cohérent, le déploiement et la gestion des applications Rifidi, toutes les applications doivent hériter d'AbstractRifidiApp. Cette classe fournit un ensemble de services aux applications Rifidi, y compris:

 Life cycle management (démarrage et arrêt de l'application)

 Configuration management (Utilisation de fichiers de propriétés pour fournir des paramètres d'entrée à l'application)

 Esper management (Veiller à ce qu'Esper soit utilisé correctement)

 Plugging into the OSGi console (Permet à votre application d'être contrôlée par la ligne de commande OSGi).

Il ya deux pièces à chaque application. La première est la classe d'application elle même.

```
Public class MyApp extends AbstractRifidiApp{
```

```
Public MyApp(){

super (“group”, “app”);
}
@Override
public void _start(){
//insert code here to create esper statements or subscribe // to rifidi services
}
@Override
public void _stop(){
//insert any clean up code here
} }
```

La deuxième partie est le spring XML qui crée l’application, l’injecte avec toutes les dépendances dont il a besoin (tels que les services rifidi ou des connexions de base de données, etc.) et enregistre l’application dans le registre de service OSGi. Ce fichier xml va dans le dossier "/ META-INF spring" dans le bundle. Les espaces de noms XML nécessaires ont été retirés de l'exemple suivant pour le souci de concision.

```
<! -- Create the application object -->
<bean id=”app1” class=”com.mycompany.MyApp”/>
<! -- register the app in the OSGi service registry -->
<osgi:service ref=”app1” interface=”org.rifidi.edge.api.RifidiApp”/>
```

La meilleure façon de commencer avec notre propre application est d'importer les modèles d'application à partir de la SDK et les modifier. En outre, il ya plusieurs exemples d'applications bien documentées dans la SDK qui démontrent de nombreuses fonctionnalités de l'application API. Explorer ces exemples est la meilleure façon d'avoir une idée de la façon de coder en utilisant l'API.

4.1.Les exemples d’application :

Pour les développeurs qui sont nouveaux dans le serveur Rifidi Edge il ya plusieurs développements documentés sur le **wiki**. Certains d'entre eux sont présentés dans les sections suivantes. Voici la liste complète d’eux:

- HelloWorld App Jumpstart
- Database application Jumpstart
- MQTT Jumpstart
- AWS / Cloud Jumpstart
- Rifidi Management API Jumpstart
- Dynamic Reader configuration Jumpstart
- Rifidi services Jumpstart
- Northwind application

- **HelloWorld application**

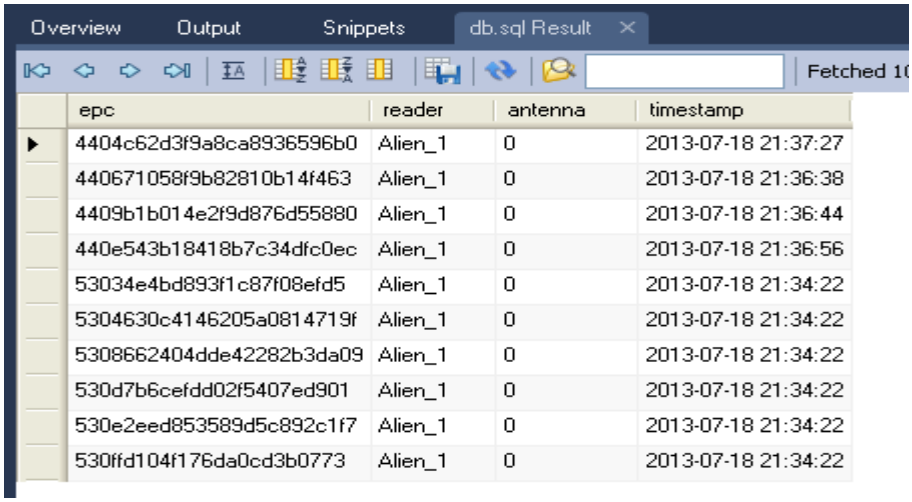
L'application HelloWorld est une application Rifidi très simple. Elle utilise le **ReadZoneMonitoringService** pour créer un abonné (subscriber), et graver les tags EPC id à la norme quand une étiquette arrive dans la zone de lecture. Voir la description sur le wiki pour plus de détails.

- **Database Application**

Un lecteur RFID et quelques étiquettes aident à faire usage du nouveau matériel. Une utilisation courante des cas développeurs veut enregistrer quand une étiquette se présente, et ce que le lecteur ou antenne a vu, et enregistrer cela dans une base de données. C'est ce que l'exemple **DB App** fait. Il génère exactement une entrée à chaque fois qu'une étiquette pénètre dans la zone de lecture d'un lecteur et enregistre l'horodatage (timestamp) et le lecteur ID.

Afin d'essayer l'application DB, il faut simplement télécharger l'application et le fichier sql, puis installer l'application et exécuter le fichier sql pour créer la table dans la base de données.S'il est souhaité de modifier l'application DB, la télécharger, et l'importer dans l'environnement de développement Rifidi. Toutes les étapes requises sont dans le wiki.

La structure de la table ressemblera à:



epc	reader	antenna	timestamp
4404c62d3f9a8ca8936596b0	Alien_1	0	2013-07-18 21:37:27
440671058f9b82810b14f463	Alien_1	0	2013-07-18 21:36:38
4409b1b014e2f9d876d55880	Alien_1	0	2013-07-18 21:36:44
440e543b18418b7c34dfc0ec	Alien_1	0	2013-07-18 21:36:56
53034e4bd893f1c87f08efd5	Alien_1	0	2013-07-18 21:34:22
5304630c4146205a0814719f	Alien_1	0	2013-07-18 21:34:22
5308662404dde42282b3da09	Alien_1	0	2013-07-18 21:34:22
530d7b6cefdd02f5407ed901	Alien_1	0	2013-07-18 21:34:22
530e2eed853589d5c892c1f7	Alien_1	0	2013-07-18 21:34:22
530ffd104f176da0cd3b0773	Alien_1	0	2013-07-18 21:34:22

Pour résumer, voici les composants dont il ya besoin:

 Le serveur Rifidi Edge, avec l'application DBApp et le fichier de DBApp.properties.

 La base de données MySQL, avec le schéma db installé. Utiliser db.sql fichier à générer.

- **Northwind application**

Après que l'application de DB soit en cours d'exécution, envisager une application plus sophistiquée, mais aussi complexe. L'exemple d'application Northwind vous fera découvrir

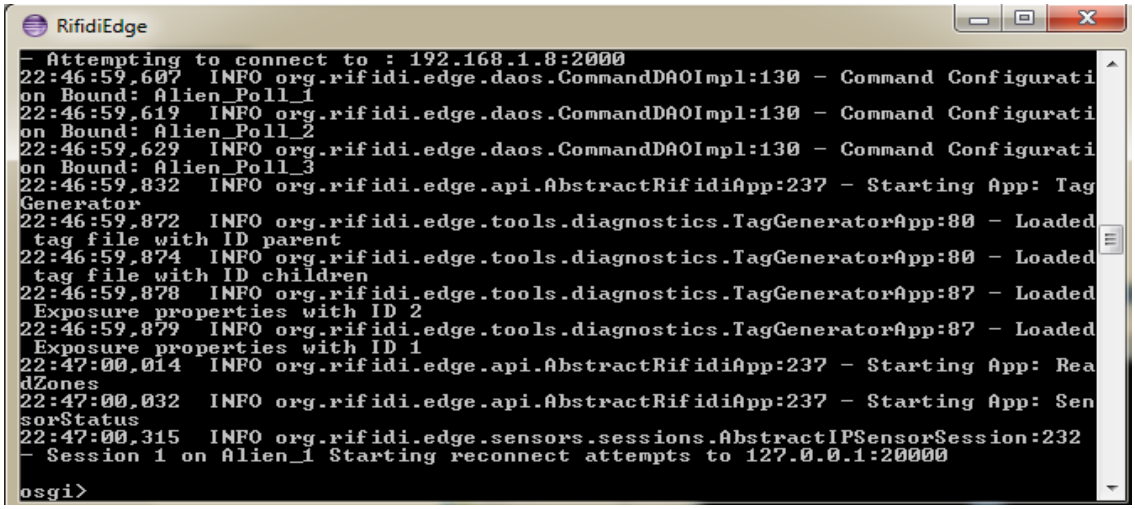
l'écriture de règles d'esper personnalisées. Aller dans l'exemple Northwind sur wiki pour trouver des détails sur cette application. Cependant, il est recommandé de construire les règles d'esper dans le cadre d'un service comme indiqué dans les services de Rifidi.

- **Dynamic Reader Configuration Jumpstart :**

Dans certaines situations, la mise à jour la configuration du lecteur dynamiquement, se fera pendant l'exécution, sur la base des événements ou d'infrastructure. Cet exemple d'application spécifique met à jour la configuration **LLRP ROSPEC** d'un lecteur existant en temps de fonctionnement. Ce pourrait être étendu à d'autres propriétés ou mettre à jour les configurations du lecteur dynamiquement. L'exemple de l'application peut être trouvé sur le wiki.

5. Utilisation de la console Rifidi Edge :

La console du serveur Rifidi Edge permet aux utilisateurs d'accéder à leurs applications et de trouver des informations utiles et détaillées sur l'état actuel du serveur Edge par l'intermédiaire d'une ligne de commande, elle est souvent utile à des fins de gestion et de test.



Une fois connecté, l'utilisation de la commande «help» permet de lister toutes les commandes disponibles.

```
osgi> help
```

Les commandes au sommet sont toutes les commandes prévues par le cadre OSGI lui même pour le contrôle et l'affichage des informations. Les commandes en bas (dans la section Rifidi Edge Server) sont toutes les commandes fournies par le serveur.

On peut démarrer, arrêter et contrôler les applications en utilisant le RifidiAppManager. En tapant dans la console OSGi la commande 'apps' une liste des applications s'affiche :

```
osgi> apps
0:Rifidi App: AppService:ReadZones (STARTED)
1:Rifidi App: AppService:SensorStatus (STARTED)
2:Rifidi App: AppService:UniqueTagInterval (STARTED)
3:Rifidi App: AppService:StableSet (STARTED)
```

```
4:Rifidi App: AppService:LimitStableSet (STARTED)
5:Rifidi App: AppService:UniqueTagBatchInterval (STARTED)
6:Rifidi App: AppService:RSSI (STARTED)
7:Rifidi App: Templates:TemplateApp (STOPPED)
8:Rifidi App: Diagnostic:GPIO (STARTED)
9:Rifidi App: Diagnostic:Serial (STARTED)
10:Rifidi App: Diagnostic:Tags (STARTED)
11:Rifidi App: Diagnostic:TagGenerator (STARTED)
12:Rifidi App: Monitoring:ReadZones (STARTED)
13:Rifidi App: Monitoring:Tags (STARTED)
14:Rifidi App: Monitoring:SensorStatus (STARTED)
```

Chaque ligne contient: L'ID d'application (un identifiant numérique), le groupe d'application, le nom de l'application et l'état de l'application (démarré ou arrêté).

Le démarrage d'une application arrêtée se fait en utilisant la commande **startapp**. De même, l'arrêt d'une application démarrée se fait en utilisant la commande **stopapp**.

Une commande utile est la commande 'readers' qui répertorie tous les lecteurs disponibles et leurs états.

```
osgi> readers
ID: Awid2010_1
session (1): IPSession: 192.168.1.91:4000 (CREATED),
[GPIO Session IPSession: 192.168.1.91:4001 (CREATED)]
Recurring Command(0): Awid2010_Push_Start_1
ID: Alien_1
session (1): IPSession: 192.168.1.120:23 (PROCESSING),
[Autonomous Session IPServerSession: 54321 (PROCESSING)],
[GPIO Session IPServerSession: 54322 (PROCESSING)]
```

Dans ce cas, il ya deux configurations de lecteur. Le premier est appelé Awid2010_1. Il dispose de deux sessions interactives qui sont à la fois liées à des ID de session 1. Une pour la lecture d'étiquettes (au 192.168.1.91:4000), et l'autre pour interagir avec les événements GPI /O (au 192.168.1.91:4001

La seconde configuration possède un ID de Alien_1. Il dispose de trois sessions, toutes liées à l'ID de session 1. La session interactive (au 192.168.1.120:23) est utilisée pour émettre des commandes pour le lecteur. La session autonomous (sur le port 54321) écoute tout simplement les étiquettes du lecteur Alien. La session GPIO (sur le port 54322) est une autre session qui écoute le lecteur Alien pour pousser les événements GPI / O à elle.

5.1.Création de configuration de lecteurs :

Il est possible d'utiliser la console OSGI pour créer et contrôler les configurations des lecteurs. La commande qui permet de répertorier les types de lecteurs disponibles est 'readertypes' :

```
osgi> readertypes
ThingMagic
LLRP
Alien
Awid3014
Awid2010
Alien-Autonomous
```

Pour créer une configuration pour se connecter à un lecteur Alien, il faut utiliser la commande 'CreateReader' :

```
osgi> createreader Alien IpAddress 192.168.1.8 Port 23
Reader Created with ID Alien_1
```

Chaque lecteur adaptateur a son propre ensemble de propriétés (par exemple IpAddress, Port) qui permettent aux utilisateurs de spécifier les informations de connexion. Pour plus de détails voir le wiki.

Ensuite, créer une session:

```
osgi>createsession Alien_1
Session created: Alien_1:1
```

Pour répertorier les types de commande disponibles, il faut utiliser la commande 'commandtypes':

```
osgi> commandtypes
ID: Awid-Read-Block-Data
ID: Awid-Mask-Push-Start
ID: Awid3014-Push-Stop
ID: LLRP-Configure
ID: Awid3014-Push-Start
ID: LLRP-Push-Stop
ID: LLRP-Poll
ID: Awid2010-Push-Stop
ID: ThingMagic-Poll
ID: Awid2010-Push-Start
ID: Alien-Push-Stop
ID: Alien-Push-Start
ID: Alien-Poll
```

Il faut créer une nouvelle commande Alien-Poll et la soumettre à la session :

```
osgi>createcommand Alien-Poll
Command Configuration Created with ID Alien_Poll_1
osgi>executecommand Alien_1 1 Alien_Poll_1 1000

command submitted
```

Enfin, démarrer la session et enregistrer la configuration de sorte qu'elle démarre automatiquement si le serveur Edge est arrêté et redémarré.

```
osgi> startsession Alien_1 1

Session Alien_1:1 started
osgi> save
Configuration Saved!
```

6. Propriétés

Ce sont les propriétés du lecteur Alien qui peuvent étre ajustées (sauf pour les propriétés en lecture seule) par la commande "setProperties".

6.1. Propriétés de connexion:

- MaxNumConnectionAttempts: Le nombre de connexions que le serveur Edge tente de se connecter au lecteur avant d'abandonner. -1 est équivalente à l'infini.
- Username: Le nom d'utilisateur utilisé pour se connecter au lecteur.
- Password: Le mot de passe utilisé pour se connecter à un lecteur.
- IpAddress: L'adresse IP du lecteur physique.
- Port: Le port que le lecteur physique utilise pour se connecter au serveur Edge.
- ReconnectionInterval: La quantité de temps en millisecondes que le serveur Edge va attendre après avoir échoué à se connecter avant de tenter de se reconnecter à un lecteur.

6.2. Propriétés générales:

- Uptime: Le temps en millisecondes que le lecteur a été activé. (Lecture seulement)
- MACAddress: L'adresse MAC du lecteur. (Lecture seulement)
- readertype: Le type de lecteur connecté (9800, 9900, etc). (Lecture seulement)
- PersistTime: La quantité de temps qu'une étiquette reste en mémoire une fois qu'elle est lue. Si cette valeur est définie à -1 les étiquettes y resterons jusqu'à ce qu'elles soient retournées par le biais d'une commande.
- ExternalOutput: Le masque de bit représentant la sortie courante du lecteur. (Lecture seulement)
- DisplayName: Le nom qui sera affiché pour ce lecteur.
- IOStreamPort: Le port à ouvrir pour écouter IOEvents du lecteur.
- MaxAntennas: Le nombre maximum d'antennes que le lecteur peut supporter. (Lecture seulement)
- ReaderVersion: la version de firmware que le lecteur a. (Lecture seulement)
- NotifyPort: le port que le serveur Edge va utiliser pour recevoir des connexions autonomous.
- InvertExternalOutput: donne les valeurs de la sortie externe.
- ExternalInput: le masque de bit représentant l'entrée courante du lecteur. (Lecture seulement)
- InvertExternalInput: donne les valeurs de l'entrée externe.

7. Les Commandes :

Ceci est une liste des commandes qui peuvent être utilisées pour communiquer avec le lecteur Alien.

Alien-Poll:

Cette commande interroge le lecteur Alien avec la commande "get taglist" pour une durée déterminée, elle retourne les étiquettes vues par le lecteur. Elle possède une propriété:

TagType: Le type d'étiquette qui sera recherché. "0" recherche uniquement les étiquettes Gen1. "1" recherche seulement des étiquettes Gen2. "2" recherche toutes sortes d'étiquettes.

Alien-Push-Start: Cette commande va démarrer le lecteur Alien en utilisant son adresse IP et son numéro de port.

NotifyAddressPort: C'est la même valeur que « NotifyPort » dans les propriétés du lecteur.

NotifyAddressHost: L'adresse IP de la machine où le serveur Edge est exécuté.

Alien-Push-Stop:

Cette commande permet d'éteindre le mode.

8. Scénarios d'utilisation communs:

Pour un Push:

```
//Create an Alien Push command

> createcommand Alien-Push-Start

//Create the autonomous command
> setproperties Alien_Push_Start_1 NotifyAddressPort 54321 NotifyAddressHost 192.168.1.201
//Executes the stop command
> executecommand Alien_1 1 Alien_Push_Start_1 -1
//Create the stop command
createcommand Alien-Push-Stop
//Execute the stop command once
> executecommand Alien_1 1 Alien_Push_Stop_1 -1
```

Pour un Poll:

```
//Create the Alien Poll command
> createcommand Alien-Poll
//Starts polling the reader every 1000 milliseconds
> executecommand Alien_1 1 Alien_Poll_1 1000
//Stops and deletes the command
> deletecommand Alien_Poll_1
```

Annexe B : Le lecteur Alien

1. Le lecteur Alien : L'Alien 9800 est produit par Alien Technology. C'est un lecteur polyvalent qui peut lire les étiquettes de classe 1 génération 2.

Modèle : ALR 9800

Protocole de réseau : TCP / IP

Communication : LAN TCP / IP (RJ-45), RS-232

Antennes: 4 ports

General Purpose I / O : 4 entrées, 8 sorties.

Le lecteur Alien a été le premier lecteur mis en œuvre dans l'émulateur (comme les informations d'horodatage dans les étiquettes spécifique à Alien)

2. La Communication :

Le lecteur Alien envoie des messages en clair sur une connexion TCP. La connexion peut être facilement testée par telnet dans le lecteur et l'émission de commandes. Ce qui suit est un exemple d'une session Telnet qui montre comment obtenir la liste de tags. Le lecteur est en cours d'exécution à 192.168.2.100:20000.

```
$ telnet 192.168.2.100 20000
Trying 192.168.2.100...
Connected to 192.168.2.100.
Escape character is '^]'.
**********************************************
*
* Alien Technology : RFID Reader
*
**********************************************

Username>alien
alien

Password>password
********
Alien >get taglist
```

```
get taglist
(No tags)

Alien >
```

3. Modèle de mémoire :

Le modèle de la mémoire du lecteur Alien est basé sur le concept de persistTime, qui est la quantité de temps qu'une étiquette reste en mémoire après avoir été vu par une antenne. Il est possible de changer le persistTime en utilisant la commande set persistTime. Par exemple, la commande suivante va paramétrer le persistTime de 500 ms.

```
Alien >set persistTime=500
set persistTime
PersistTime = 500
```

4. Obtention des tags :

Il existe deux modes principaux pour obtenir les étiquettes à partir d'un lecteur Alien. Le plus simple est le mode «on demand», dans lequel l'utilisateur émet simplement une commande et le lecteur renvoie la liste de tags. Le mode Autonomous permet au lecteur d'agir en tant que client et envoyer la liste des tags à un serveur à un certain emplacement.

4.1. On demand : pour obtenir la liste des tags lus, un utilisateur peut envoyer la commande 'gettaglist ' ou tout simplement 't' le lecteur répondra avec sa liste de tags.

4.2. Mode Autonomous : Le Mode autonomous est plus compliqué. L'utilisateur doit mettre en place plusieurs paramètres, tels que notifyAddress (l'adresse du serveur sur laquelle la liste des tags doit être envoyé), notifyTime l'intervalle de temps pour les messages qui seront envoyés), notifyTrigger (la condition sur laquelle tirer un message), et d'autres. Quand le notifytime a expiré, un message qui contient la liste des tags sera envoyé au serveur.Le NotifyTime est une variable qui contrôle la façon dont les messages basés sur le temps sont envoyés, il est en secondes.

5. Identification :

Pour accéder aux données du lecteur Alien l'utilisateur doit s'authentifier avec son nom est son mot de passe. Le nom et le mot de passe par défaut sont "alien/password".

6. Obtention et définition des variables

Le lecteur Alien rifidi permet aux utilisateurs d'obtenir et définir des variables, en utilisant les commandes get et set. Comme mentionné précédemment, il est possible d'obtenir la liste des tags utilisant la commande getTaglist ou t.

7. Les commandes prises en charge:

La liste des commandes prises en charge par Rifidi:

7.1. Les commandes générales:

- Quit (q)
- get/set ReaderName
- get ReaderType
- get ReaderVersion
- get / set ReaderNumber
- get / set Username
- get / set Password

7.2. Commandes TagList

- get Taglist (t)
- get / set PersistTime
- get / set TagListFormat (possible values = text, terse, xml)
- clearTagList
- get / set TagType
- get / set AntennaSequence

7.3.Commandes Autonomous

- get / set AutoMode (possible values = on, off)
- get / set AutoFalseOutput
- get / set AutoFalsePause
- get / set AutoStartPause
- get / set AutoStartTrigger
- get / set AutoStopTimer
- get / set AutoStopTrigger
- get / set AutoStopTimer
- get / set AutoTrueOutput

- get / set AutoTruePause
- get / set NotifyMode
- get / set NotifyAddress
- get / set NotifyFormat (possible values = text, terse, xml)
- get / set NotifyTime
- get / set NotifyTrigger
- get / set NotifyHeader (possible values = on, off)

7.4. Commandes Program Tag

- get / set ProgAntenna
- ProgramTag
- get / set Function

7.5. Commandes GPIO

- get / set ExternalOutput