

Ce chapitre est divisé en deux sections: la section 1 consiste à définir un système RFID ainsi que ses fonctionnements et ses applications. La section 2 consiste à décrire les protocoles étudiés dans ce mémoire.

I. Les systèmes RFID :

1. Définitions :

Les systèmes RFID sont très proches des cartes à puce (smart cards). Comme sur les cartes à puce, les données sont stockées sur une puce électronique (tag). Cette puce peut être de type « machine à états » ou contenir un microprocesseur, elle peut avoir différents types de mémoire. Par contre, à la différence des smart cards, il n'y a pas de contact physique entre la puce et le lecteur ; l'alimentation électrique de la puce se fait par induction électromagnétique. Les données sont aussi transmises selon ce principe, ainsi que par réflexion des ondes radio. C'est bien de là que vient le nom de cette technologie : *Radio Frequency Identification* [NSer 05].

La **radio-identification** plus souvent désignée par le sigle **RFID** (de l'anglais *radio frequency identification*) est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« *RFID tag* » ou « *RFID transponder* » en anglais). Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collés ou incorporés dans des objets ou produits et même implantés dans des organismes vivants (animaux, corps humain). Les radio-étiquettes comprennent une antenne associée à une puce électronique qui leur permet de recevoir et de répondre aux requêtes radio émises depuis l'émetteur-récepteur. Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires [Rid].

2. Historique

Le RFID, résulte de la combinaison de deux technologies: la technologie radio et celle de l'électronique à laquelle s'est substitué aujourd'hui celle de la microélectronique. On cite brièvement un historique de l'évolution de la technologie RFID.

1948 : Le concept du système RFID a son origine dans les années 40 dans le but de différencier les avions amis des avions ennemis. D'imposant tags ou transpondeurs furent placés dans les avions amis afin de répondre comme amical à l'interrogation des radars. Ce système IFF (Identify: Friend or Foe) fut la première utilisation de la RFID.

Aujourd'hui encore, le contrôle du trafic aérien est basé sur ce principe.

1970 : Durant les années 70, les systèmes RFID restèrent une technologie protégée à usage militaire supportée par les états pour la sécurité de sites sensibles notamment dans le secteur du nucléaire.

1980 : L'invention des microsystèmes et l'avancée de la technologie conduit à l'utilisation de tag passif. L'absence de source d'énergie embarquée rend le tag moins coûteux mais l'oblige à obtenir de l'énergie au travers du signal du lecteur. Les distances de lecture obtenues sont alors de quelques centimètres. A la fin des années 70, la technologie est transférée vers le secteur privé. Une des toutes premières applications commerciales est l'identification de bétail en Europe. Le début des années 80 marque la fabrication et la commercialisation de tags par de nombreuses firmes européennes et américaines.

1990 : Début de la standardisation pour une interopérabilité des équipements RFID à commencer par les cartes à puces puis les systèmes tags lecteurs de manière générale[RFp].

3. Fonctionnement :

Dans tout système RFID, on retrouve les mêmes constituants de base (Figure II.1) :

- **un lecteur**, ou scanner, est un appareil qui communique sans fil avec des tags pour identifier l'élément connecté. Le lecteur est en général fait d'un émetteur récepteur radiofréquence, d'un module de commande et d'un élément de couplage qui permet d'interroger les tags électroniques au moyen d'une communication par radiofréquence. Cette communication permet au lecteur de lire un tag passif à petits ou moyens distances et une étiquette active à petites ou grandes distances.
- **une étiquette**, ou transpondeurs (de l'anglais transponder, contraction des mots transmitter et responder), et appelée également tag, fixée sur ces objets, qui réagit à la réception du signal envoyé par le lecteur en renvoyant vers ce dernier

l'information demandée. Un tag comporte un microprocesseur, plus ou moins puissant, dotée d'une mémoire et connecté à une antenne bobinée.

- **un ordinateur** de stockage et de traitement des informations recueillies par le lecteur. Cet ordinateur peut travailler en boucle fermée (cas des systèmes locaux) ou en
- **boucle ouverte** (connexion à un système de gestion de niveau supérieur).

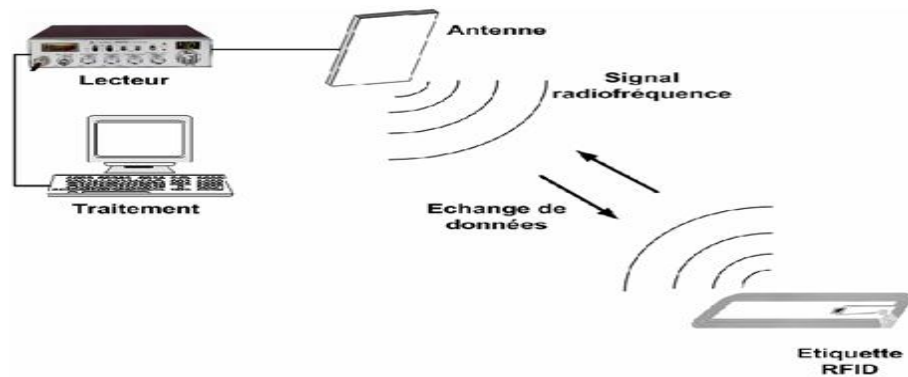


Figure N°II.1 : Schéma général d'un système RFID [RRe]

Quand le transpondeur, qui ne possède généralement pas d'alimentation propre, n'est pas dans le champ d'action d'un lecteur, il est totalement passif. L'énergie, les données et les pulsations d'horloge nécessaires à l'activation et au fonctionnement du transpondeur lui sont fournies par le lecteur. On distingue deux cas, qui peuvent se recouvrir : la communication par champs électromagnétiques et la communication par ondes radio.

4. Le format des tags

On trouve des tags RFID de toutes formes et de toutes tailles. En voici quelques uns, présentés aux figures ci-dessous :

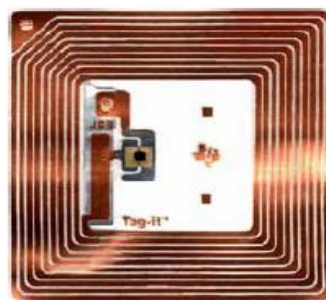


Figure N°II.2 : formats de tags

La(figure II.2) (gauche), désigne le transpondeur et l'antenne sont fins et souples, collés sur un autocollant. [NSer05]

Dans même figure à droite, on distingue bien le transpondeur au centre, entouré d'une antenne de cuivre bobinée. [Nser05]

5. La sécurité

Les enjeux relatifs à la sécurité des tags RFID sont nombreux et importants. Le concepteur de systèmes RFID rencontre les mêmes problèmes que celui qui conçoit des cartes à puces: comment empêcher qu'un attaquant puisse lire, modifier ou fabriquer, voire dupliquer les données d'un tag, de manière à perturber le système et éventuellement obtenir frauduleusement un accès à un bâtiment ou un service ?. Il s'agit d'un problème complexe qui ne connaît pas de réponses parfaitement satisfaisantes.

Dans le cas des systèmes RFID, le fait que les échanges de données se font par ondes radio, ou champs électromagnétiques, ajoute une dimension supplémentaire au problème. D'une part, les menaces qui pèsent sur les cartes à puce avec contact physique sont renforcées par le fait qu'un attaquant peut interagir avec un tag RFID à distance, sans même que son propriétaire légitime ne s'en rende compte. D'autre part, il existe une nouvelle menace, qui pose un défi de taille aux concepteurs : comment empêcher un attaquant d'intercepter la communication radio, pour ensuite « rejouer » la transaction en imitant le tag original, un peu `a la manière d'Ali Baba devant la grotte des voleurs ?

Il est facile d'imaginer des scénarios catastrophiques pour les acteurs qui utiliseraient des systèmes de paiement électroniques mal sécurisés. Lors de la conférence de sécurité informatique Blackhat 2004, un consultant allemand, Lukas Grunwald, a présenté le logiciel libre RFDump4, qui permet de lire et de modifier différents types de tags RFID. Il existe également une bibliothèque5 de fonctions en langage C écrite par le français Loic Dachary, libre elle aussi, pour dialoguer avec les tags RFID [NSer05].

6. Les Applications de RFID:

Les applications de la RFID peuvent être utilisées dans les entreprises, par les individus ainsi que par les états. Ce système est exploité dans plusieurs domaines : le

transport, la sécurité, la santé, la bibliothèque, et la logistique qui sont autant des domaines dans lesquels cette technologie existe déjà et apparaîtra dans le futur [SS07].

6.1. Le paiement : le paiement est un des défis importants de la RFID. Parmi les applications de la RFID dans ce domaine, le modèle Pidion BIP-1300 se présente comme un PDA durci, qui accepte des techniques de paiement diverses, comme les cartes bancaires à puce ou à bande.

6.2. Transport : Une des applications les plus connues et les plus démocratisées de la technologie RFID reste la carte de transport sans contact. L'utilisateur du métro passe sa carte sur une base (généralement apposée à des tourniquets d'accès), qui l'authentifie, valide son titre de transport, et lui donne accès au réseau. 3,4 millions de titres de transport sans contact circulaient en juin 2008 sur le réseau de transport en commun parisien de la RATP. Ce système fonctionne également dans des villes telles que Londres, Helsinki ou encore Tokyo.

6.3. Bibliothèques : Certaines bibliothèques ont mis en place un système d'IRF pour faciliter l'emprunt de livres, contrôler les stocks et réduire les traumatismes répétés chez les bibliothécaires. Cependant, les préoccupations au sujet de la surveillance des livres choisis ont mis au jour les problèmes de protection de la vie privée relatifs à l'IRF.

6.4. Contrôle d'accès : L'identification des individus passe aussi par l'authentification des papiers d'identités. Le RFID est alors un moyen qui d'une part, s'assure de la validité des documents, mais aussi, il s'assure que les informations contenues dans le passeport le sont également d'un point de vue numérique. Il est à noter que des questions de sécurité importantes se posent quant à la l'intégrité des données contenues dans les tags RFID des passeports.

6.5. La santé : Le suivi et le contrôle des patients peuvent également s'effectuer à travers de puces RFID implantées dans le corps humain de manière sous cutanée. Par exemple, la société Verichip [Ver], produit et commercialise une puce implantable pour identifier les patients en situation d'urgence.

6.6. Le RFID et la logistique : Un des secteurs d'activité dans lequel la technologie RFID est utilisée depuis plus longtemps est celui de la logistique. Les codes à barre ont été remplacées par les tags RFID, et ce dans des domaines aussi divers que la fabrication de médicaments, ou encore ici dans celui de la gestion de containers maritimes. L'avantage de la RFID est ici déterminant, puisque la fréquence d'onde permet de repérer des tags à plusieurs centaines de mètres. Cela permet par exemple d'effectuer des inventaires et de surveiller les containers en temps réel.

II. Protocoles d'authentification RFID :

Le protocole d'authentification permet au lecteur d'être sûr de l'identité de tag. Inversement, il peut permettre à un tag pour être sûr de l'identité d'un lecteur. Si les deux propriétés sont assurées, nous parlons de l'authentification mutuelle. On étudie des protocoles qui utilisent la primitive cryptographique qui s'appelle la fonction du hachage « MD-5 ,SHA-1... ».

1. Protocole RHLS :

Le protocole RHLS (*Randomized Hash Lock scheme*) proposé par Weis et al [WSRE03]. Dans ce protocole (voir Figure II.3), les informations transmises par le tag à chaque fois qu'elle est interrogée se compose d'une valeur aléatoire nt et la valeur $H1 =$ valeur du hachage $h(ID, nt)$ où ID qui est l'identifiant statique du tag. Afin de calculer cette information, le tag a besoin d'un générateur pseudo-aléatoire et un objet incorporé une fonction du hachage irréversible mais seulement stocke son identifiant.

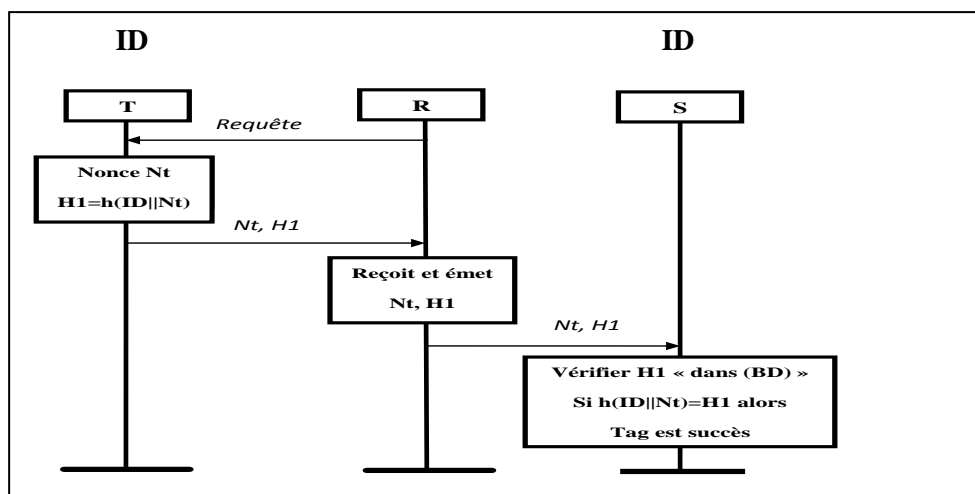


Figure N°II.3: le protocole RHLS

La notation TAG-READER-SERVER proposée est la suivante :

$$T \rightarrow R: N_t, H(ID.N_t)$$

$$R \rightarrow S: N_t, H(ID.N_t)$$

2. Protocole HMNB :

La référence [HMNB07] représente le protocole HMNB, ce protocole est lancé par le lecteur, tel que le lecteur génère un nonce N_r et l'envoie à tag. Le tag génère un nonce N_t , la réponse du tag dépend de la valeur de S . Dans le cas où le processus se termine avec succès et aucun des messages n'est bloqué ou perdu, la valeur de S est égale à 0. Dans le cas contraire, la valeur de S vaut 1, ce cas devrait se produire rarement. (La figure II.4) décrit ce protocole.

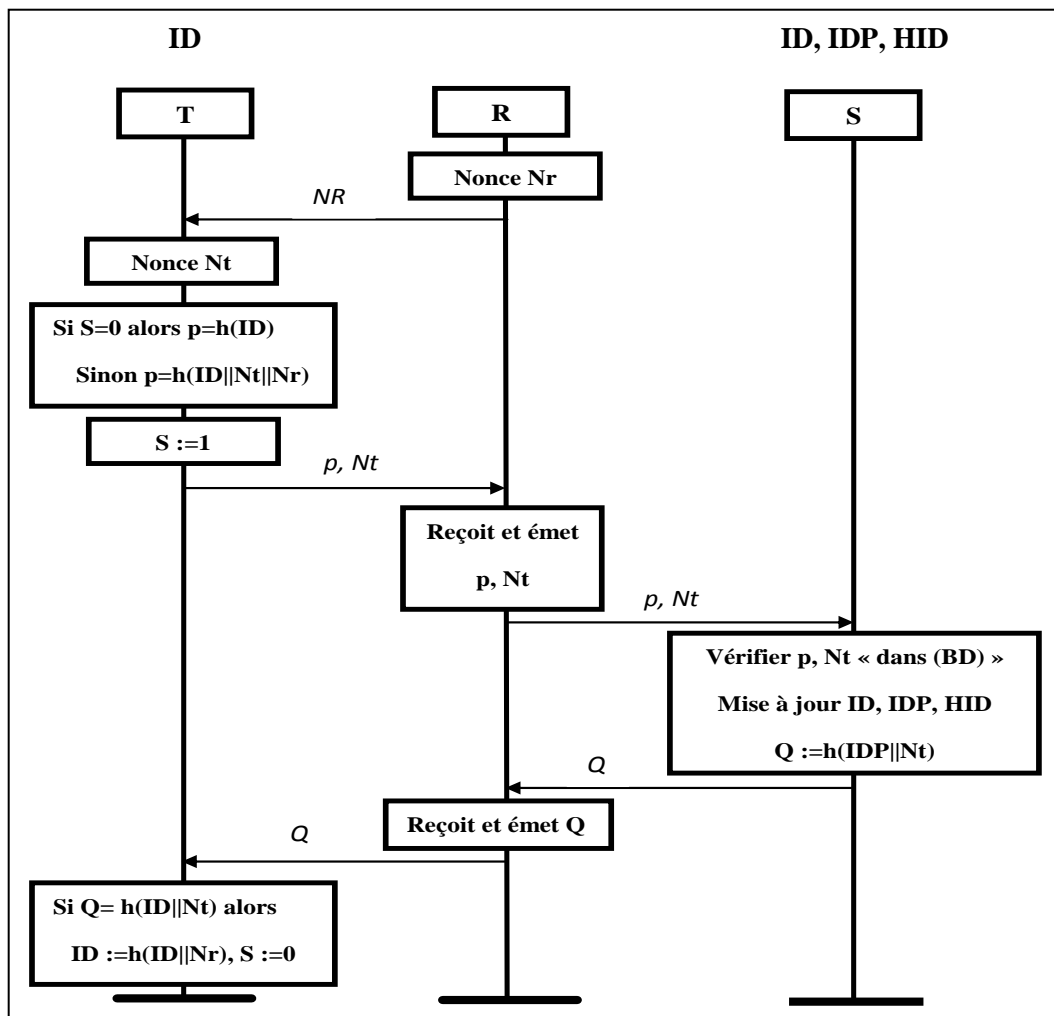


Figure N°II.4:Le protocole HMNB

La notation TAG-READER-SERVER, proposée est la suivante :

$$R \rightarrow T: Nr$$

$$T \rightarrow R: Nt, H(ID)$$

$$R \rightarrow S: Nr, Nt, H(ID.Nt)$$

$$S \rightarrow R: H(IDP, Nt) \% \text{ tel que } IDP' := ID$$

$$R \rightarrow T: H(IDP, Nt)$$

3. Protocole CRAP:

Le protocole CRAP (*Challenge-Response based Authentication Protocol*) [RKKW05] est proposé par Rhee et al. Ce protocole basé sur l'authentification mutuelle entre le tag et le lecteur à l'aide d'une fonction de hachage et les nombres aléatoires. Un tag répond au lecteur en lui envoyant une fonction de hachage qui contient le nombre Nr reçu du lecteur et son propre nombre aléatoire Nt ainsi que l'identificateur ID.

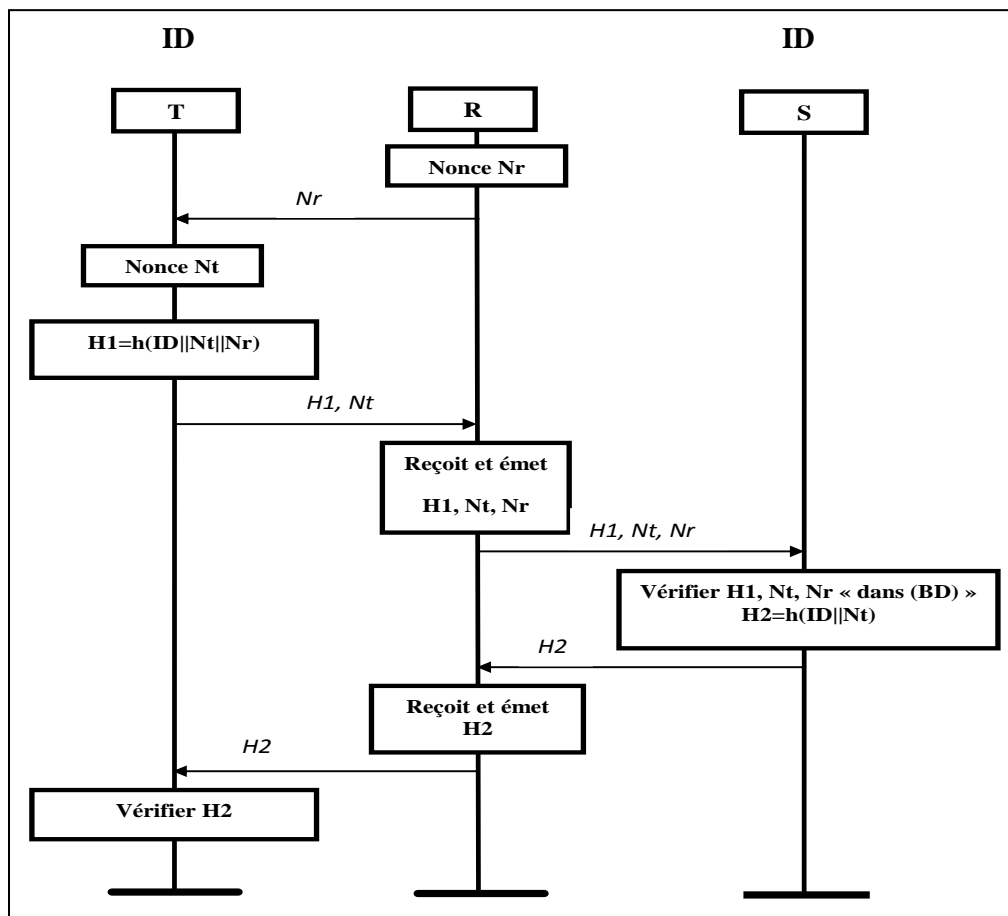


Figure N°II.5 : Le protocole CRAP

La notation TAG-READER-SERVER, de ce protocole est la suivante :

$R \rightarrow T : Nr$

$T \rightarrow R : H(ID, Nr, Nt), Nt$

$R \rightarrow S : H(ID, Nr, Nt), Nt, Nr$

$S \rightarrow R : H(ID, Nt)$

$R \rightarrow T : H(ID, Nt)$

4. Protocole LAK:

Ce protocole est proposé par Lee et al. [LAK06], Ce protocole est partagé en deux phases : phase d'authentification et la phase de mise à jour de la clé. (La figure II.6) décrit ce protocole.

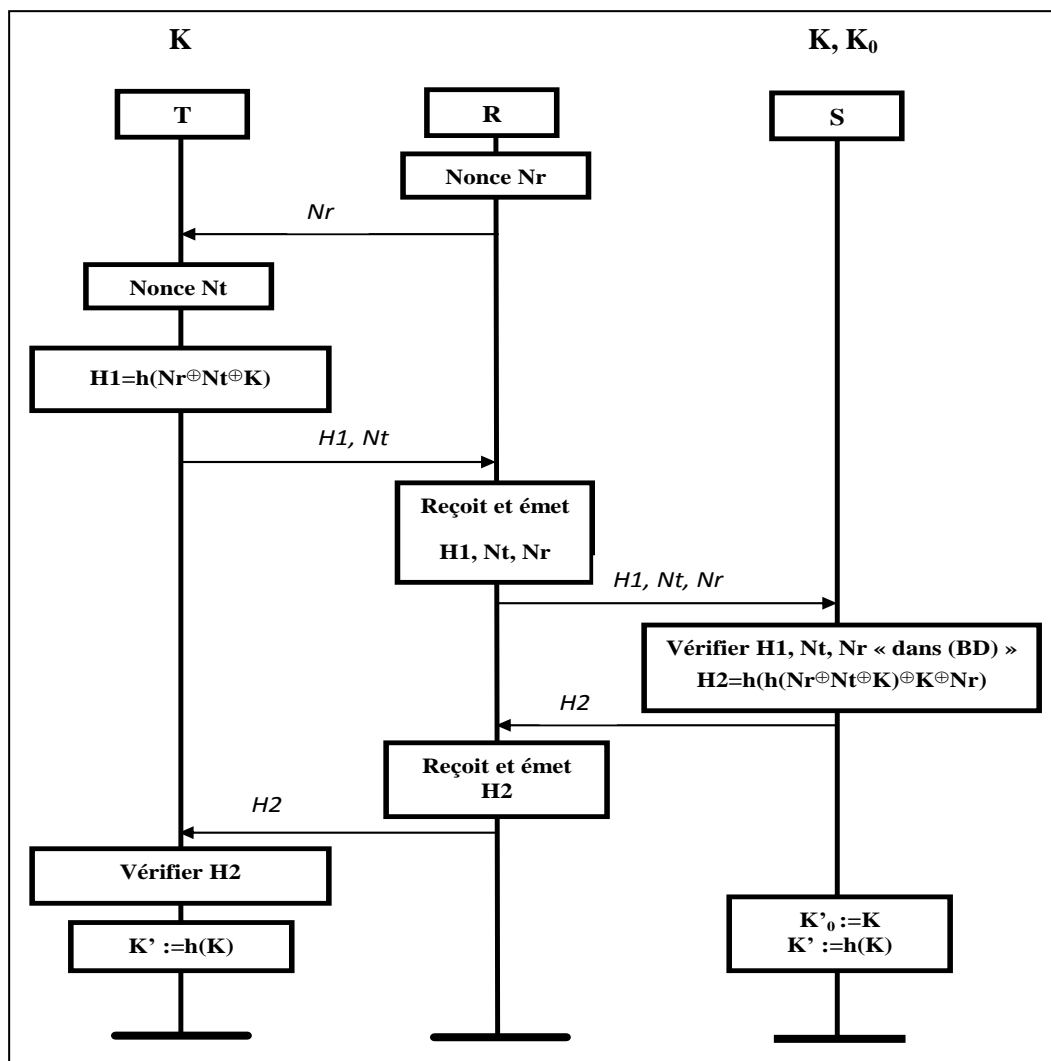


Figure N°II.6: Protocole LAK.

Le principe de ce protocole est constitué par la notation suivante :

$R \rightarrow T : Nr$

$T \rightarrow R : Nt, H(Nr \oplus Nt \oplus K)$

$R \rightarrow S : Nt, Nr, H(Nr \oplus Nt \oplus K)$

$S \rightarrow R : H(H(Nr \oplus Nt \oplus K) \oplus K \oplus Nr)$

$R \rightarrow T : H(H(Nr \oplus Nt \oplus K) \oplus K \oplus Nr)$

Ce protocole découvre une attaque de type attaque par rejeu algébrique [C10]. La trace d'attaque est comme le suivant : pour personifier le tag, l'intrus peut renvoie la fonction $h(nr \oplus nt \oplus K)$ pour vu que $nr \oplus nt = nr' \oplus nt'$, autrement dit $h(nr \oplus nt \oplus K) = h(nr' \oplus nt' \oplus K)$. Pour satisfaire à cette condition l'intrus créer nt' , tel que : $nt' = nr(nr'(nt$ et avec d'utilisation les propriétés de l'opérateur Xor (voir : le chapitre II, page 31) alors l'attaque est succès.

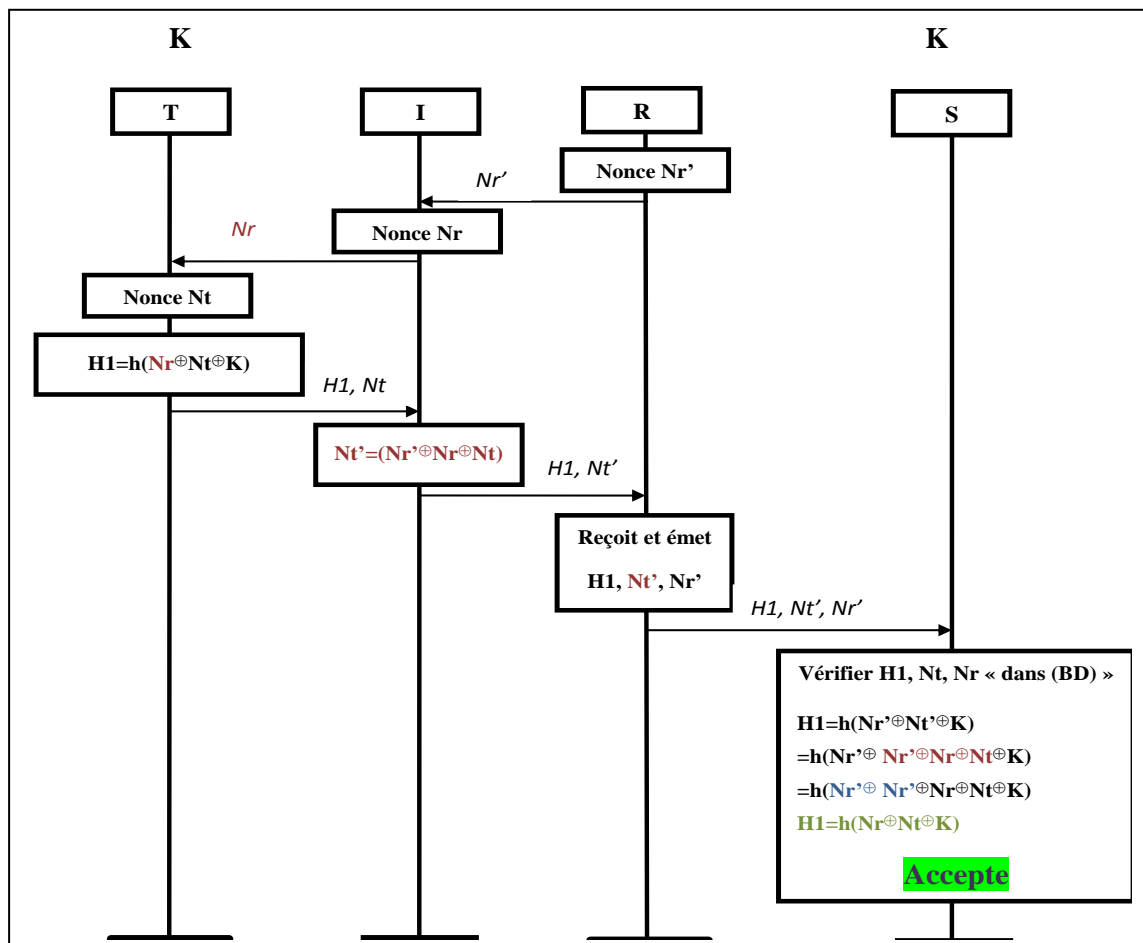


Figure N°II.7 : Trace d'attaque sur protocole de LAK [C10]

5. Protocole PAP :

Ce protocole est proposé par Liu et Bailey [LB09]. Le protocole PAP est basé sur quatre locations différentes: à l'intérieur d'un magasin, à un comptoir de contrôle, à un comptoir de retour, et à l'extérieur d'un magasin. Notre travail s'intéresse par le protocole dans location de *comptoir de contrôle*.

Le tag envoie d'abord son identificateur ID et un nonce aléatoires au lecteur. Le lecteur utilise cette information pour déterminer la clé secrète k du tag et lui applique une fonction de hachage en envoyant à la fois le résultat haché et un autre nonce aléatoire au tag. Le tag vérifie le lecteur en réalisant la même fonction de hachage en utilisant sa clé secrète k avec le nonce envoyé au lecteur. Si cette valeur correspond au résultat haché, envoyé par le lecteur, le tag authentifie le lecteur. Le tag alors effectuera une autre fonction de hachage en utilisant sa clé secrète k avec le nonce reçu du lecteur et envoie cette valeur hachée au lecteur. Le lecteur effectue ensuite la même fonction de hachage avec sa clé secrète k . Si le résultat correspond, alors lecteur authentifie le tag.

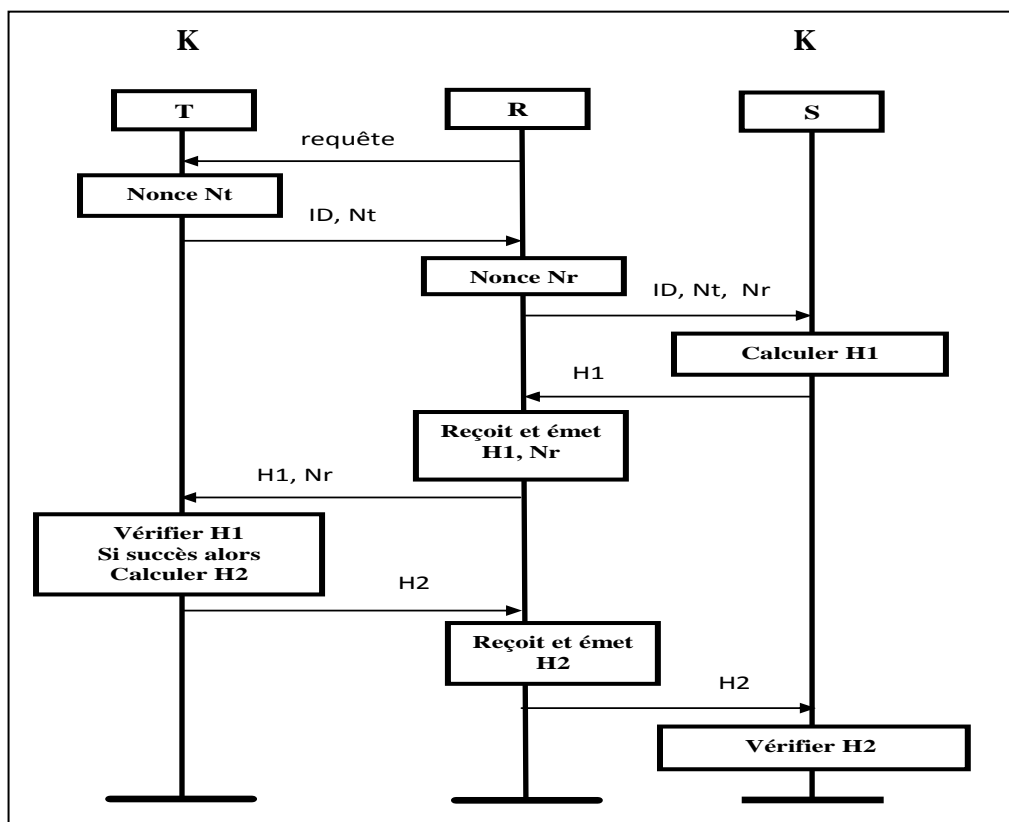


Figure N°II.8 : protocole de PAP (contrôle)

Spécifie en modèle TAG-READER-SERVER, comme suit :

$T \rightarrow R : ID, N_t$
 $R \rightarrow S : ID, N_t, N_r$
 $S \rightarrow R : H(N_t, K)$
 $R \rightarrow T : N_r, H(N_t, K)$
 $T \rightarrow R : H(N_r, K)$
 $R \rightarrow S : H(N_r, K)$