**SETIT 2005**
3rd International Conference: **S**ciences of **E**lectronic,
**T**echnologies of **I**nformation and **T**elecommunications
March 27-31, 2005 – TUNISIA

# Etude de la sécurité dans la technologie Bluetooth

Nada Chendeb * et Bachar El Hassan *

** Université Libanaise,*
*Faculté de Génie, Branche 1,*
*Rue Al Arz,EL Kobbeh Tripoli Liban*
**elhassan@ul.edu.lb**
**nadachendeb@hotmail.com**

**Résumé:** Le but de cet article est de présenter une vue d'ensemble de l'architecture de sécurité de la technologie Bluetooth, comme elle est appliquée à sa pile protocolaire. Nous commençons tout d'abord par une étude rapide de cette technologie, puis nous détaillons les mécanismes de sécurité mises en place et examiner également vers la fin de l'article certaines des failles de l'architecture de sécurité proposée.

**Mots clés**: Authentification, Bluetooth, code et clés de sécurité, mécanisme de sécurité, vulnérabilité.

## 1 Introduction

Bluetooth est une norme proposée pour la communication locale sans fil qui permettra aux dispositifs physiquement dispersés tels que les téléphones cellulaires, les imprimantes, les écouteurs sans fil, les assistants numériques personnels (PDA) etc. de communiquer et échanger l'information l'un avec l'autre.

Parmi les modèles d'utilisation prioritaire ou les applications pratiques de la technologie Bluetooth on a le transfert des dossiers et d'autres objets tels que les cartes électroniques entre les dispositifs physiquement dispersés et relativement proches. Une autre utilisation potentiellement populaire devrait permettre aux téléphones mobiles en tant que " modems sans fil " de relier des ordinateurs à l'Internet sans employer n'importe quel câble les reliant ensembles.

Cependant, les soucis de sécurité ralentissent l'adoption de toutes les technologies sans fil et Bluetooth n'est aucune exception. Avant d'entrer dans les détails des mécanismes de sécurité qui font l'objet de notre étude, nous trouvons indispensable d'introduire au lecteur cette technologie.

## 2 Une vue d'ensemble de la technologie Bluetooth

### 2.1 Concept de base : le Piconet [7]

Les liaisons physiques se font sur le principe Maître/Esclaves, fonctionnant selon le type point à multipoint. Un maître pouvant contrôler jusqu'à sept esclaves dans sa zone. Ceux-ci forment alors un petit réseau appelé Piconet.

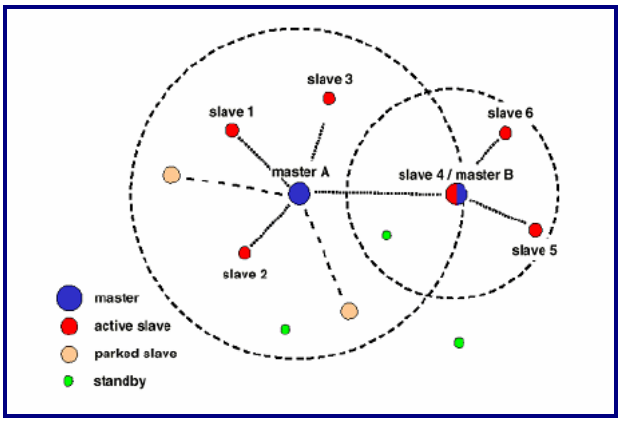


**Figure 1 : Maître/Esclaves dans un Piconet**

Le maître est tout simplement le premier appareil connecté et c'est lui qui fixe l'horloge, la séquence de saut de fréquences et le code d'accès de la liaison. Tous les modules Bluetooth d'un même Piconet utilisent la même séquence de saut de fréquence et sont synchronisés sur l'horloge du maître.

Quoiqu'il arrive, le rôle de la machine (maître ou esclave) est invisible pour l'utilisateur. Un même appareil peut d'ailleurs participer à plusieurs piconets, esclave dans l'un, maître dans un autre. L'imbrication de plusieurs piconets forme alors ce que l'on appelle un Scatternet.

Le schéma d'émission au sein d'un même Piconet est basé sur le principe de duplexage temporel

(TDD : Time Division Duplex). C'est d'abord le maître qui envoie un paquet à une fréquence f(k), puis l'esclave auquel ce paquet est destiné a seul le droit d'y répondre pendant l'intervalle de temps suivant l'arrivée du paquet maître. La réponse de l'esclave se fait alors sur le canal de fréquence f(k+1).

## 3. Architecture protocolaire de Bluetooth

L'architecture protocolaire de Bluetooth est essentiellement une amalgamation des protocoles spécifiques Bluetooth et d'autres protocoles déjà adoptés tels que WAP, WAE, TCP/UDP/IP, PPA, vCard, vCal et IrMC.

Elle soutient également des protocoles de remplacement de câble tels que RFCOMM et des protocoles d'adaptation de téléphonie tels que AT-commands. Ces protocoles ont été adoptés pour convenir à des applications Bluetooth mais ils ne sont pas spécifiques à Bluetooth.

Un avantage de cette structure amalgamée est qu'elle permet au contrôle de sécurité spécifique aux applications d'être mis en place de façon transparente au contrôle de sécurité des couches inférieures auxquelles Bluetooth fonctionne (Bluetooth fonctionne à la couche liaison de données).

La pile protocolaire de Bluetooth est montrée dans le diagramme montré ci-dessous. Dans la partie propre Bluetooth, on parle des 3 composants : la partie radio (Bluetooth Radio), la bande de base (BaseBand) et le directeur de lien (Link Manager)

### 3.1. Bluetooth Radio

Bluetooth emploie la gamme radio de 2,45 GHz et une largeur de bande théorique maximale de 1 Mb/s, qui est légèrement ralenti par les effets de correction d'erreurs dus à la méthode FEC qui est une méthode efficace pour améliorer le taux d'erreurs sur les bits sans sacrifier trop de largeur de bande.

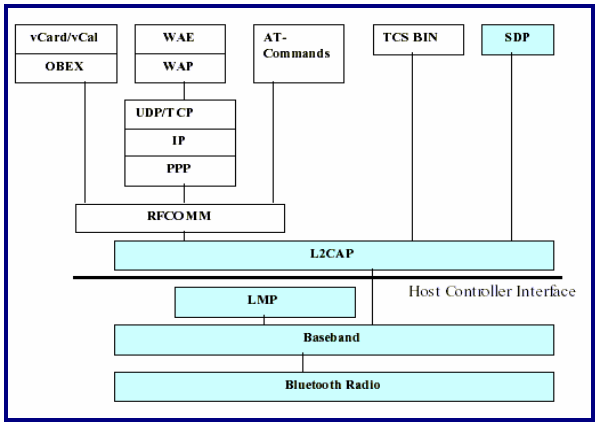


**Figure 2 : Architecture protocolaire de Bluetooth**

Les spécifications de Bluetooth utilisent la méthode du saut de fréquence avec la modulation GFSK - ce système de sélection et de saut entre les fréquences pendant les transmissions s'adapte pour n'importe quel environnement bruité entourant l'emplacement du transfert.

### 3.2. Base Band

C'est la couche qui permet le raccordement physique radio entre les dispositifs Bluetooth. Cette partie de l'architecture Bluetooth emploie une combinaison des technologies de commutation de circuits et de paquets:

- Un canal asynchrone de données et jusqu'à trois canaux synchrones simultanés de voix.
- Un canal qui transfère des données asynchrones et la voix synchrone employant simultanément des combinaisons des technologies de commutation.

### 3.3. Link Manager

Le directeur de lien emploie, comme son nom l'indique, le protocole LMP, Link Manager Protocol, pour configurer, authentifier et manipuler les connexions entre les dispositifs Bluetooth. Ce protocole fonctionne parallèlement à L2CAP. Tandis que L2CAP est responsable de commander les protocoles des couches supérieures, LMP est responsable d'installer le lien entre deux dispositifs Bluetooth. Il inclut la décision et la commande de la taille de paquet dans BaseBand, des services de sécurité tels que l'authentification et le chiffrage à l'aide des clés du lien et des clés de chiffrage. Il gère également le schéma de puissance, qui est divisé en trois modes : Sniff, Hold et Park.

Une courte description des autres protocoles est donnée ci-dessous :

Host Controller Interface HCI : Il est employé pour fournir une interface de commande aux contrôleurs BaseBand, Link Manager et à d'autres contrôleurs de matériel.

L2CAP (Logical Link Control and Adaptation Protocol) : Ce protocole adapte les protocoles des couches supérieures sur la couche BaseBand.

SDP (Service Discovery Protocol) : Ce protocole est nécessaire pour que les dispositifs Bluetooth puissent recueillir des informations sur les types de dispositif, les services et les caractéristiques de service de sorte qu'un raccordement entre les dispositifs puisse être installé.

RFCOMM : C'est un protocole de remplacement de câble. Comme c'est vu dans la figure, un certain nombre de protocoles des couches supérieures s'interfacent avec la couche RFCOMM qui se connecte à son tour aux protocoles propres à Bluetooth. Ainsi aucun standard séparé ne doit être conçu pour que les protocoles des couches supérieures travaillent avec Bluetooth.

TCS BINARY et AT Commands : ce sont des protocoles de commande de téléphonie qui permettront à des services tels que les modems et le fax de fonctionner au-dessus de Bluetooth. RFCOMM, TCS BIN et AT commands ensembles et d'autres protocoles adoptés tels que OBEX, TCP/UDP/IP, PPA et WAE/WAP forment les

protocoles orientés application qui fonctionnent au-dessus des protocoles Bluetooth spécifiques.

## 4. La Sécurité dans Bluetooth

La sécurité est une priorité dans un réseau normal, mais l'est encore plus dans un réseau sans fil, en permettant aux utilisateurs une connexion permanente et un accès facile, ce type de réseau se voit très vulnérable. Les concepteurs de Bluetooth, en essayant de faire de ce protocole une référence, ont implémenté un certain nombre de fonctionnalités liées à la sécurité.

Nous allons détailler ici les caractéristiques génériques et les niveaux de sécurité qui ont été incorporés dans les spécifications Bluetooth.

### 4.1. Les mécanismes de sécurité [4]

- Les dispositifs Bluetooth transmettent sur la bande fortement utilisée de 2.45GHz. Pour sécuriser les transmissions au niveau de la couche physique, Bluetooth utilise la méthode du saut de fréquence, une technique de saut autour de la bande radio 1600 fois par seconde. Ceci améliore la clarté et réduit également ce qu'on appelle "écoute clandestine occasionnelle" en permettant seulement aux dispositifs synchronisés de pouvoir communiquer.

- La spécification Bluetooth inclut des mécanismes de sécurité au niveau liaison des données. Elle soutient l'authentification (unidirectionnelle ou mutuelle) et le chiffrage. Ces mécanismes sont basés sur une clé secrète de lien partagée par les deux dispositifs en communication. Pour générer cette clé un procédé appelé "pairing procedure" est employé quand les deux dispositifs se communiquent pour la première fois.

### 4.2. Les paramètres de base pour la sécurité

La sécurité du protocole Bluetooth (niveau liaison de données) est basée sur l'exploitation des trois paramètres suivants.

Un nombre aléatoire RAND : permettant de simuler le hasard sur 128 bits. Il change fréquemment et il est produit par le dispositif Bluetooth.

Une adresse dépendante du dispositif physique BD-ADDR (Bluetooth Device ADDResse) : Chaque carte Bluetooth se voit assigner une adresse permanente et unique de 48 bits lors de sa construction. Cette adresse permet aux autres utilisateurs d'avoir de la confiance en la personne à l'autre extrémité de la communication.

Un code personnel d'identification PIN : C'est un code personnel qui est attribué à l'utilisateur. Ce code PIN peut être stocké sur 1 à 16 octets. Le PIN peut être stocké dans la mémoire non-volatile du dispositif.

Ces paramètres permettent de créer des clés pour authentifier et chiffrer les transferts de données afin de les sécuriser.

### 4.3 Les modes de sécurité

Selon les caractéristiques de Bluetooth, les dispositifs peuvent fonctionner dans un des trois modes de sécurité :

Le mode 1 : C'est le mode de sécurité le moins sûr dans lequel le dispositif Bluetooth ne lance aucun procédé de sécurité. Un dispositif Bluetooth dans ce mode est dans un mode de découverte du réseau.

Le mode 2 : Ce mode impose la sécurité après l'établissement du lien entre les dispositifs au niveau L2CAP. Ce mode permet l'établissement des politiques flexibles de sécurité comportant des commandes des couches application fonctionnant parallèlement aux protocoles des couches inférieurs.

Le mode 3 : Ce mode impose des commandes de sécurité telles que l'authentification et le chiffrage au niveau de la couche Baseband, il est identique au mode 2 mais y ajoute des fonctions d'authentification et de chiffrement avant que la connexion ne soit établie.

### 4.4. Les niveaux de sécurité des dispositifs et des services

Bluetooth définit des niveaux de sécurité pour les dispositifs et les services. [5]

- Pour des dispositifs il y a deux niveaux possibles de sécurité. Un dispositif distant peut être:

1- Un dispositif fiable : Il aurait accès à tous les services pour lesquels la relation de confiance a été placée.

2- Un dispositif non fiable : Il aurait un accès limité aux services.

- Pour les services, trois niveaux de sécurité ont été définis.

1- Les services qui exigent l'autorisation et l'authentification : On accorde seulement l'accès automatique aux dispositifs de confiance. D'autres dispositifs ont besoin d'une autorisation manuelle.

2- Les services qui exigent l'authentification seulement : L'autorisation n'est pas nécessaire. C.-à-d. le dispositif devrait être authentifié avant de pouvoir utiliser ces services.

3- Les services ouverts : L'authentification n'est pas exigée, aucune approbation d'accès n'est exigée avant qu'on accorde l'accès de service.

Note : L'architecture Bluetooth tient compte de définir les politiques de sécurité qui peuvent placer des relations de confiance de telle manière que même les dispositifs fiables puissent seulement obtenir l'accès aux services spécifiques et pas à d'autres.

Il est important de comprendre ici que les protocoles spécifiques Bluetooth peuvent seulement authentifier des dispositifs et pas des utilisateurs. Ceci ne doit pas dire que le contrôle d'accès basé sur l'utilisateur n'est pas possible. L'architecture de sécurité Bluetooth permet à des applications d'imposer leurs propres politiques de sécurité. La couche liaison, sur laquelle les mécanismes de sécurité spécifiques de Bluetooth fonctionnent, est transparente aux mécanismes de sécurité imposés par les couches supérieures. Ainsi il est possible d'imposer le contrôle d'accès granuleux basé sur l'authentification de l'utilisateur dans le cadre de sécurité de Bluetooth.

**4.5 Le contrôleur de sécurité**

Les mécanismes et les politiques de sécurité qui peuvent être soutenues par Bluetooth comme mentionné ci-dessus sont possibles grâce à un composant appelé le contrôleur de sécurité (Security Manager). Le contrôleur de sécurité est l'entité qui décide quelles politiques sont à appliquer quand une demande de connexion est faite. Basé sur le service, le type de dispositif et son niveau de fiabilité, le contrôleur de sécurité peut imposer l'authentification du niveau application, le chiffrage de la session et toutes les autres politiques spécifiques d'accès.

Le contrôleur de sécurité a besoin de l'information concernant des dispositifs comme des services avant qu'elle puisse prendre une décision. Cette information est stockée dans deux bases de données notamment, la base de données de dispositif et la base de données de service.

1- La base de données de dispositif stocke des informations sur le type de dispositif, son niveau de fiabilité et sur la longueur de clé de lien utilisée pour le chiffrage.

2- la base de données de service stocke l'information concernant les conditions d'authentification, d'autorisation et de chiffrage pour les services.

Le processus typique suivi par le contrôleur de sécurité en accordant l'accès à un dispositif pour un service particulier est comme suit :

1- Le dispositif distant demande l'accès

2- La demande de connexion vient à L2CAP

3- L2CAP demande au contrôleur de sécurité d'accorder l'accès

4- Le contrôleur questionne les bases de données de dispositif et de service

5- Si le dispositif est fiable, donc le contrôleur de sécurité peut ou ne peut pas demander l'authentification ou l'autorisation

6- Si le dispositif est non fiable, le contrôleur de sécurité peut terminer la connexion ou imposer l'autorisation. L'authentification au niveau de Bluetooth se produira quand des clés de lien sont échangées. Selon l'accès régissant la politique de sécurité, le contrôleur de sécurité pourrait inviter un protocole d'application pour imposer la sécurité de niveau d'application telle qu'un arrangement d'username/password pour l'authentification. L'appui est également incorporé pour d'autres arrangements d'authentification par l'interface de contrôleur de sécurité.

7- Le contrôleur de sécurité décidera alors si l'accès de service exige le chiffrage de lien. Si oui, des clés sont négociées et échangées au niveau du protocole L2CAP et la connexion continuera à être établie.

Alternativement, si le dispositif est en mode de sécurité 3, le contrôleur de sécurité demande au LMP pour authentifier et chiffrer la communication avant que la connexion soit établie.L'architecture générale de sécurité dans Bluetooth est présentée dans la figure suivante :

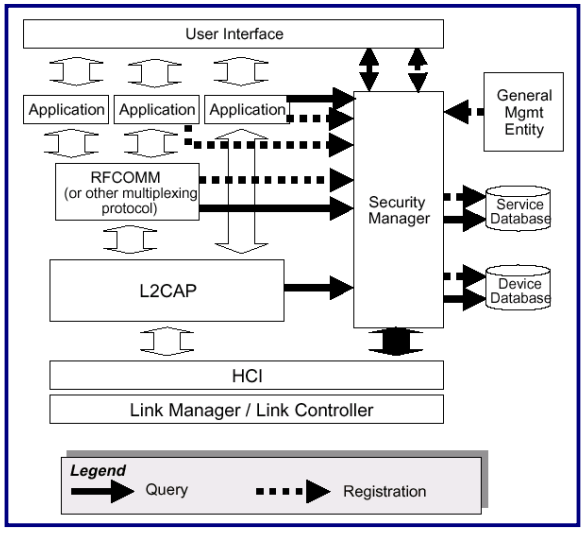


**Figure 3 : Architecture générale de sécurité dans Bluetooth**

Nous voyons ainsi que le contrôleur de sécurité est l'entité centrale qui contrôle et impose la politique de sécurité dans l'architecture de sécurité de Bluetooth.

### 4.6. La gestion des clés dans Bluetooth

Assurer une transmission sécurisée avec le protocole Bluetooth, implique l'utilisation de plusieurs genres de clés et de contrôles. [6]

#### 4.6.1. Le code PIN

En soi, le code PIN joue son rôle dans l'authentification pour identifier uniquement les dispositifs. Il est utilisé pour accéder au dispositif Bluetooth tout comme le code utilisé pour accéder à la carte SIM d'un appareil cellulaire.

Le PIN est ou bien un nombre fixe inscrit au dispositif ou bien un code défini par l'utilisateur. Pour les codes PIN définis par l'utilisateur, il peut les changer quand il veut, de ce fait on ajoute de la sécurité d'authentification au système. Un PIN est normalement de 4 digits de longueur, mais il peut être entre 1 et 16 octets.

#### 4.6.2. Les clés de lien

Les clés de lien sont utilisées dans le procédé d'authentification ainsi comme paramètre dans la dérivation de la clé de chiffrage. Elles peuvent être temporaires ou semi-permanentes.

- Une clé temporaire dure seulement jusqu'à ce que la session courante soit terminée et ne puisse pas être réutilisée.

- Une clé semi-permanente peut être utilisée après que la session courante termine. Elle authentifie habituellement les unités Bluetooth qui partagent la session.

Il y a également quatre types principaux de clés de lien, qui sont tous des nombres aléatoires de 128-bits.

- La clé d'unité : Unit Key KA

KA est la clé d'unité du dispositif Bluetooth A, dérivé à l'installation du dispositif.

- La clé d'initialisation : Initialisation Key Kinit

Kinit, comme son nom le suggère, est employé dans le processus d'initialisation.

- La clé de combinaison : Combination Key KAB

KAB est dérivée de deux dispositifs Bluetooth, A et B. Elle est produite pour chaque paire de dispositifs et est utilisée quand plus de sécurité est nécessaire.

- La clé maître Master Key Kmaster

Kmaster est employée quand le dispositif maître, impliqué dans le piconet, veut transmettre à plusieurs dispositifs une fois pour toute. Elle dépasse la clé de lien courante seulement pour cette session maîtrisée.

#### 4.6.3. La clé de chiffrement

La clé de chiffrage peut changer de 8 à 128 bits, elle assure le passage sécurisé pour chaque paquet transmis entre les dispositifs pendant la session du transfert. Cette clé est dérivée de la clé courante de lien, et chaque fois que le chiffrage est exigé, elle est régénérée à nouveau.

#### 4.6.4. Initialisation et génération des clés

Chacun des dispositifs Bluetooth impliqués, après que l'utilisateur avait été authentifié par le système de contrôle par PIN, exige l'échange des clés. Cet échange des clés se produit pendant une phase d'initialisation que les deux dispositifs sont exigés à accomplir.

Note: les algorithmes E22 et E21 sont combinés dans l'algorithme dénoté simplement E2 et déterminant la clé de lien.

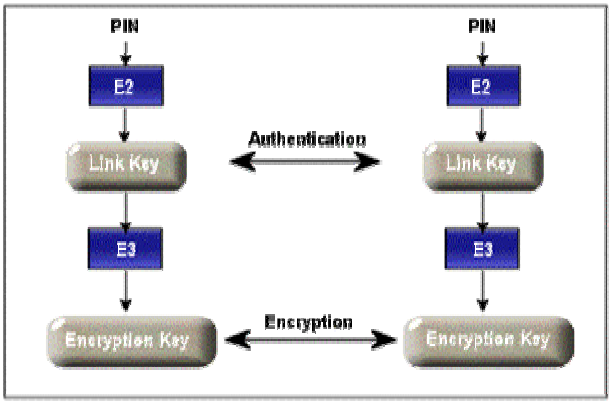


**Figure 4 : Processus général d'authentification et de chiffrement**

Toutes les procédures d'initialisation comprennent les étapes suivantes :

1- Génération d'une clé d'initialisation à l'aide de l'algorithme E22 en utilisant le code PIN du dispositif.

2- Génération de la clé de lien en utilisant l'algorithme E21.

3- L'authentification se produit, (voir le paragraphe suivant) pendant cette opération une valeur excentrée de chiffrage d'authentification (ACO : Authentication Ciphering Offset) est produite.

4- Echange des clés de lien.

5- Génération de la clé de chiffrage dans chaque unité par l'algorithme E3. Cette clé est calculée sur la base de la clé de lien, d'un nombre aléatoire et d'une valeur excentrée de chiffrage (COF : Ciphering OFfset) basée sur la valeur ACO du processus d'authentification.

Après ce procédé le lien est établi ou avorté, avec un temps d'attente et une période de re-essais des tentatives d'initialisation échouées.

### 4.7. Procédures d'authentification

Le schéma d'authentification dans Bluetooth est essentiellement une stratégie de défi-réponse, où un protocole de 2 passes est employé pour vérifier si l'autre partie connaît une certaine clé secrète.

L'authentification est réussie si le protocole vérifie que les deux dispositifs ont la même clé. Pendant le procédé d'authentification, une valeur ACO est produite et stockée dans des les deux dispositifs. La valeur ACO est employée pour déterminer un nombre de 96 bits COF qui est employé dans la génération de la clé de chiffrage, il constitue un des paramètres de l'algorithme E3 mentionné ci-dessus dans la phase d'initialisation.

Le schéma d'authentification se produit comme suit (voir figure 5) :

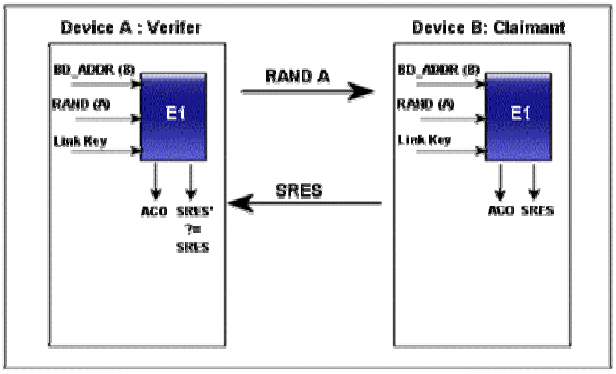


**Figure 5 : Processus d'authentification**

Etape 1 : Le vérificateur (A) envoie au claimant (B) un nombre aléatoire (RAND A) à authentifier.

Etape 2 : Le vérificateur et le claimant emploient la fonction E1 d'authentification avec le nombre aléatoire (RAND A), l'adresse BD_ADDR du claimant et la clé courante de lien pour obtenir une réponse.

Etape 3 : Le claimant envoie la réponse au vérificateur, qui s'assure alors de la validité de la réponse. De même, tous les deux calculent la valeur ACO qui est employée plus tard dans la détermination de la valeur de COF employée pour produire la clé de chiffrage comme cité ci-dessus.

### 4.8. Procédures de chiffrement et de confidentialité

Après que la clé de lien avait été établie et l'authentification a été couronnée de succès, la clé de chiffrage est produite par l'algorithme E3 et le système de chiffrage de Bluetooth est prêt à chiffrer systématiquement la charge utile pour la transmission. Le procédé de chiffrage 6 implique une graine binaire E0 qui est employée pour le chiffrage des données.

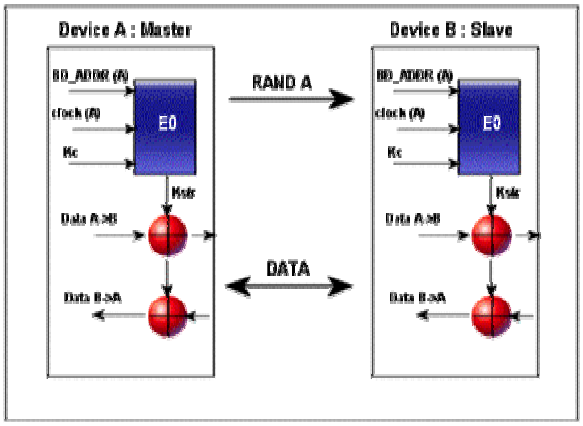


**Figure 6 : Processus de chiffrement**

La graine binaire E0 se compose de 3 éléments ; le générateur principal de clé, le générateur de clé de charge utile, et le composant de chiffrage/déchiffrage. Le registre principal de la suite binaire contient quatre registres, connus sous le nom de registres à décalage linéaires de rétroaction (LSFR : Linear Feedback Shift Register). Ces registres sont de longueurs 25, 31, 33, et 39 donnant une longueur totale de 128. Le générateur de clé de charge utile combine les bits d'entrée dans les divisions appropriées et les décale aux quatre registres du générateur principal de la clé binaire.

E0 prend comme paramètres, le Kc qui est la clé de chiffrage produite par E3, un nombre aléatoire, l'adresse de dispositif BD_ADDR, et l'horloge du dispositif A. En utilisant la sortie de l'algorithme E0, Kstr et les données à transmettre, le texte chiffré est formulé dans des paquets de données pour la transmission.

## 5. Les vulnérabilités dans la sécurité de Bluetooth

L'architecture de sécurité de Bluetooth, n'est pas sans faiblesse. Il y a un certain nombre de faiblesses dans cette architecture qui peuvent être exploitées.

L'une des failles du protocole Bluetooth est une faille spécifique aux réseaux sans fils : le déni de service par batterie. Comme les éléments d'un réseau sans fil sont nomades, ils sont dépendants d'une source d'énergie limitée. L'une des principales attaques de DoS est de surcharger de travail la machine à attaquer pour consommer le plus rapidement possible son énergie.

Un autre problème, cependant pas aussi simple à mettre en œuvre, est l'attaque «man in the middle» pour voler des clés d'identification et de chiffrage avant le début d'une session et l'usage de la même chose pour personnifier et/ou écouter des communications. Ce problème est cependant non spécifique à Bluetooth. La plupart des systèmes des échanges principaux sont enclins à ce type d'attaque. La seule méthode pour atténuer ceci est de construire des systèmes d'authentification basés par certificat numérique.

Rendre les intervalles et les modèles de méthode du saut de fréquence raisonnablement imprévisibles, peut aider à empêcher un attaquant de se cloisonner sur le signal de dispositif.

Un problème de vol d'identité est encore possible lors de l'utilisation d'une clé de lien basée sur le « unit key » où il est assez facile de voler l'identité d'un correspondant. En imaginant que A et B communiquent en se basant sur le « unit key » de A, un troisième intervenant C peut venir communiquer avec A et obtenir cette clé. C peut donc utiliser l'adresse Bluetooth de B pour se faire passer pour lui...

L'autre issue traite le code PIN même. La plupart des dispositifs ont extrêmement un PIN très court (habituellement 4 caractères, c.à.d. il y a seulement 10000 possibilités). C'est une faiblesse de sécurité importante, bien que cette faiblesse soit due à l'implémentation non plus à la spécification, les PINs courts peuvent être recherchés exhaustivement par les attaquants.

## 6. Conclusion

Dans ce papier, nous avons décrit la technologie Bluetooth, présenté les mécanismes de sa sécurité pour finir par l'étude de la vulnérabilité de cette sécurité. Nous pouvons dire que même si les concepteurs de ce protocole se sont penchés sur les aspects de sécurité durant la spécification, un certain nombre de vulnérabilités font que son utilisation doit se limiter à de petits réseaux n'échangeant pas de données sensibles.

## Remerciements

Nous tenons à remercier le CNRS libanais qui a financé cette étude dans le cadre d'un projet intitulé :

« Communication sans fil utilisant la technologie Bluetooth ».

## Références

[1] Security comparison : Bluetooth communications vs 802.11 , Thomas G. Xydis, http://www.bluetooth.com/upload/14Bluetooth_Wifi_Security.pdf

[2] Bluetooth security white paper, Bluetooth SIG, http://www.bluetooth.com/upload/24Security_Paper.PDF

[3] Tendances en matière de technologies sans fil et sécurité des appareils sans fil, http://www.cse-cst.gc.ca/fr/documents/knowledge_centre/government_publications/itsb/ITSB-03.pdf

[4] An overview of Bluetooth security, Nikhil Anand, http://www.giac.org/practical/gsec/Nikhil_Anand_GSEC.pdf

[5] Bluetooth security, Juha T. Vainio. http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

[6] Évaluation des vulnérabilités de Bluetooth (ITSPSR-17), rapport sur les produits et systemes de securite TI http://www.cse-cst.gc.ca/fr/services/publications/itspsr/itspsr17.html

[7] Bluetooth, The Bluetooth Specification, v.1.0B http://www.bluetooth.com/developer/specification/specification.asp