Sécurité des PAN (Personal Area Networks, ex. ZigBee...)

Jie Chen, Chenxi Du

L'introduction de zigbee:

1. Origin

ZigBee est un protocole de haut niveau permettant la communication de petites radios, à consommation réduite, basée sur la norme IEEE 802.15.4 pour les réseaux à dimension personnelle avec faible consommation énergétique (Low-Power Wireless Personal Area Networks : LP-WPAN). Ratifiées le 14 décembre 2004, les spécifications de ZigBee 1.0 sont disponibles auprès des membres de la communauté industrielle ZigBee Alliance.

2. Caractéristiques

Cette technologie a pour but la communication de courte distance telle que le propose déjà la technologie Bluetooth, tout en étant moins chère et plus simple. À titre d'exemple, les nœuds ZigBee classiques nécessitent environ 10% du code nécessaire à la mise en œuvre de nœuds Bluetooth ou de réseaux sans fil, et les nœuds ZigBee les plus élémentaires peuvent ainsi descendre jusqu'à 2%.

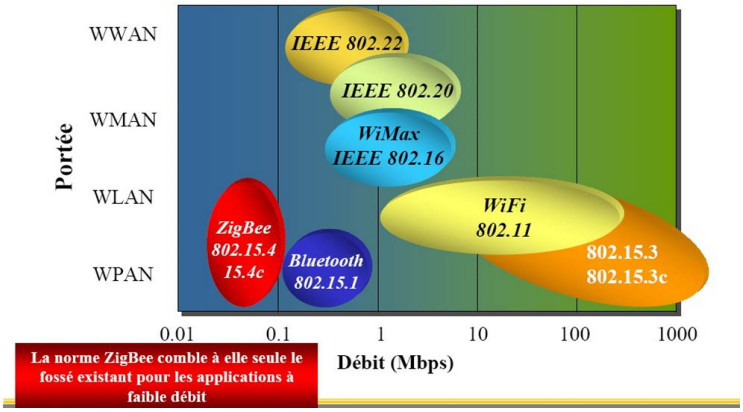


Figure 1. Graphique comparatif de différents protocoles sans fil

La figure 1 nous présente les deux caractéristiques clairement et compare les différentes technologies sans fil actuelles. On peut aussi voir que le ZigBee a un débit faible (moins de 0.1 Mbps). Ainsi, si nous voulons l'utiliser pour transférer des données comme vidéo en haut débit, c'est pas possible. D'ailleurs, le zigbee est utilisé dans les domaines des contrôles industriels, des applications médicales, des détecteurs de fumée et d'intrusion et de la télécommande de la freebox v6.

Tableau 1 Comparaison des protocoles Zigbee, Bluetooth et Wi-Fi

Caractéristique	Zigbee	Bluetooth	Wi-Fi
IEEE	802.15.4	802.15.1	802.11a/b/g/n/ac
Besoins mémoire	4-32 ko	250 ko +	1 Mo +
Autonomie avec pile	Années	Mois	Jours
Nombre de nœuds	65 000+	255	256+
Vitesse de transfert	20-250 kb/s	1 Mb/s	11-54-108-320-1000 Mb/s
Portée (environ)	100 m	10 m	300 m

3. Architecture

Comme le montre la figure 2, l'architecture ZigBee est composée de 4 couches sur les 7 du modèle OSI : Physique (PHY), Liaison (MAC), Réseau (NWK) et Application (APL). Entre ces couches se trouve les points d'accès aux services (SAP), ces SAP offrent les API pour permettre aux couches de communiquer tout en isolant le travail interne à chacune des couches. ZigBee utilise deux types de SAP par couches : un pour les données (Data Entity), et un pour le management (Management Entity).

Les deux couches inférieures (PHY et MAC) sont définies par les spécifications de l'IEEE 802.15.4, et les couches supérieures sont proposées directement par l'Alliance de Zigbee. Dans la couche APL, on peut voir quelques parties différentes, notamment la sous-couche ZigBee Device Object (ZDO) qui est responsable de la gestion du réseau en local et via le médium d'accès. Il offre des services pour la découverte d'autres noeuds et services dans le réseau, et est définit l'état courant et le rôle de l'objet dans le réseau.

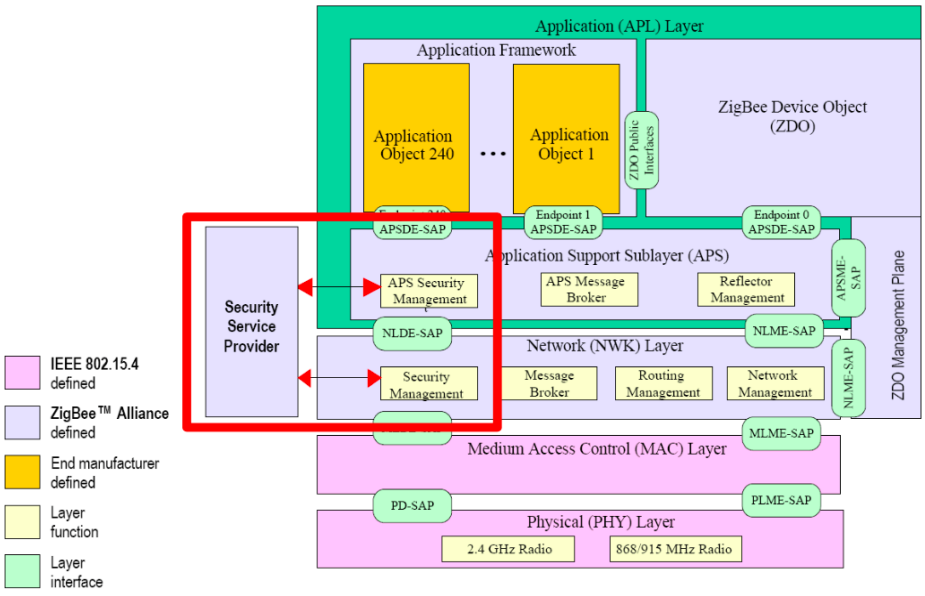


Figure 2. Architecture principale de Zigbee

4. La topologie

Figure 3 nous montre que la topologie de Zigbee. La pointe verte signifie un coordinateur et parfois le il sert comme un 'Centre de confiance'. Normalement, il n'y a qu'un coordinateur dans un réseau de Zigbee qui est responsable pour stocker les clés pour le réseau, mettre en œuvre le service de sécurité pour configurer un appareil avec sa clé et autoriser un appareil dans le réseau.

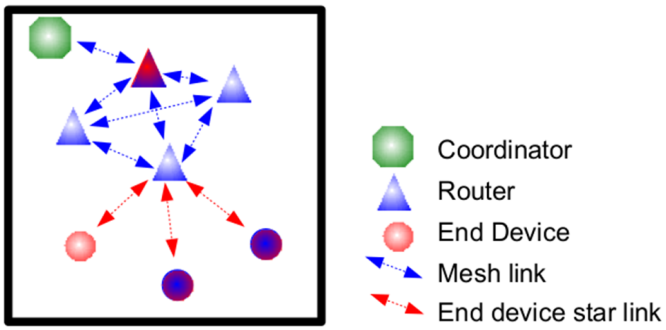


Figure 3. Topologie de Zigbee

La sécurité de Zigbee

La protection cryptographique existe justement entres deux équipements en assumant que chaque couche de la pile de protocoles se fait mutuellement confiance. Comme l'architecture indiquée dans le figure 2, Chaque couche prend en charge le mécanisme de sécurité (*PHY*, *MAC*, *NWK* et *APL)*. ZigBee est basé sur la norme IEEE 802.15.4 pour sa gestion des couches physique et liaison, la sécurité pour ces couches est donc aussi assurée par cette norme. D'autre part, le "Security Service Provider" fournit la sécurité pour les couches NWK et APL.

Les services de sécurité mis en place pour ZigBee se chargent de l'établissement et du transport des clés, de la protection des frames et du management des équipements.

1. L'établissement et le transport des clés

Le Centre de Confiance :

Les spécifications ZigBee introduisent le rôle de centre de confiance qui est un équipement auquel les autres équipements du réseau peuvent avoir confiance. C'est celui-ci qui distribue les clés et contrôle les accès. Il y en a un seul par réseau et il s'agit le plus souvent du coordinateur ZigBee.

Trois types de clés:

- LK (les "clés de liaison" ou "link keys") . Les communications de pair à pair sont protégées par des clés 128 bits partagées par les 2 équipements pour la sécurité de la couche APS. Le plus souvent, un des deux équipements est le centre de confiance et c'est lui qui s'occupe de la création et l'établissement de la clé.
- NK (les "clés de réseau" ou "network keys"). Les communications broadcast sont protégées par des clés 128 bits partagées par tous les équipements du réseau. Un jeu de clés est tenu par le centre de confiance du réseau et la clé de réseau courante est identifiée par un numéro de séquence de clé. Cette clé est généralement transportée par le Centre de confiance, mais peut aussi être préinstallée. La mise à jour se fait en deux étapes: mise à jour de la nouvelle clé et du numéro clé de séquence associé et passer à nouveau numéro de la séquence de la clé.
- MK (une "clé maître" ou "master key"). Elle est utilisée pour la génération des clés.

Trois méthodes de distribuer les clés aux équipements:

-La préinstallation : Il s'agit de placer les clés dans l'équipement grâce à une méthode hors bande, via un équipement spécial comme un clavier par exemple.

- Le transport : C'est le centre de confiance qui envoie la clé, de la façon la plus sécu- risée possible, aux deux équipements
- L'établissement : Il s'agit d'une méthode où les équipements négocient séparément avec le centre de confiance pour établir les clés sans qu'elles soient transportées en utilisant une de ces trois techniques :

Tableau 2. Méthode d'acquisition et type de clé utilisé

Méthode d'acquisition/Type de clé	NK	MK	LK
Transport de clé (via le centre de confiance)	Oui	Oui	Oui
Etablissement d'une clé (via MK)	Non	Non	Oui
Pré-installation (avant de rejoindre le réseau)	Oui	Oui	Oui

2. La protection des trames

La norme IEEE 802.15.4 utilise l'algorithme de cryptage standard Advanced Encryption Standard (AES) avec une clé de 128bits. Cette clé peut être préinstallée sur les nœuds ou partagée hors bande. Le cryptage permet de garantir la confidentialité et l'intégrité des données.

Le champ " Auxiliary Security Header" est utilisé uniquement dans le cas lorsque l'on active le bit "Security Enabled" contenu dans la "Frame Control". Il est composé de 3 champs principaux : "Security Control" (protection utilisée), "Frame Counter" (identifiant de compteur unique protégeant la duplication du message) et "Key Identifier" (informations indiquant la clé).

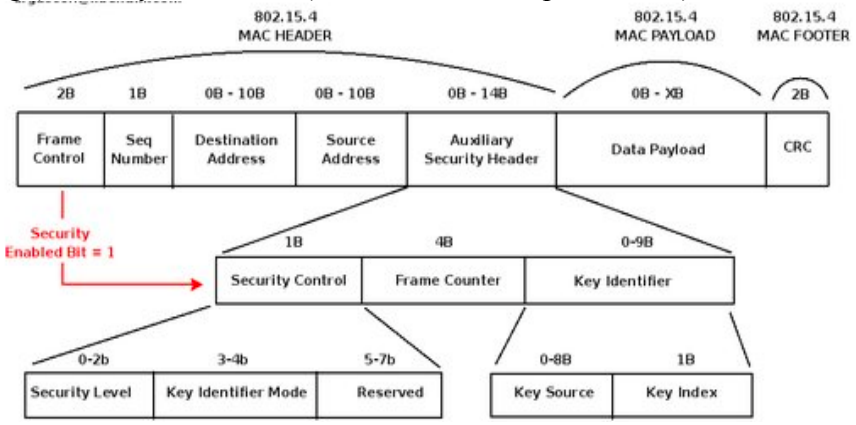


Figure 4. Le champ " Auxiliary Security Header"

Le champ " Security Level " dans le champ "Security Control" indique parmi 8 niveaux de politique de sécurité laquelle est déterminée pour cryptographier des données.

Tableau 3. 8 niveaux de politique de sécurité

Valeurs bits	Police de sécurité	Signification
000 (0x00)	Pas de sécurité	Pas de cryptage ni d'authentification des données
001 (0x01) 010 (0x02) 011 (0x03)	AES-CBC-MAC-32 AES-CBC-MAC-64 AES-CBC-MAC-128	Pas de cryptage mais l'authentification des données est garantie
100 (0x04)	AES-CTR	Cryptage mais pas d'authentification des données
101 (0x05) 110 (0x06) 111 (0x07)	AES-CCM-32 AES-CCM-64 AES-CCM-128	Cryptage et authentification des données

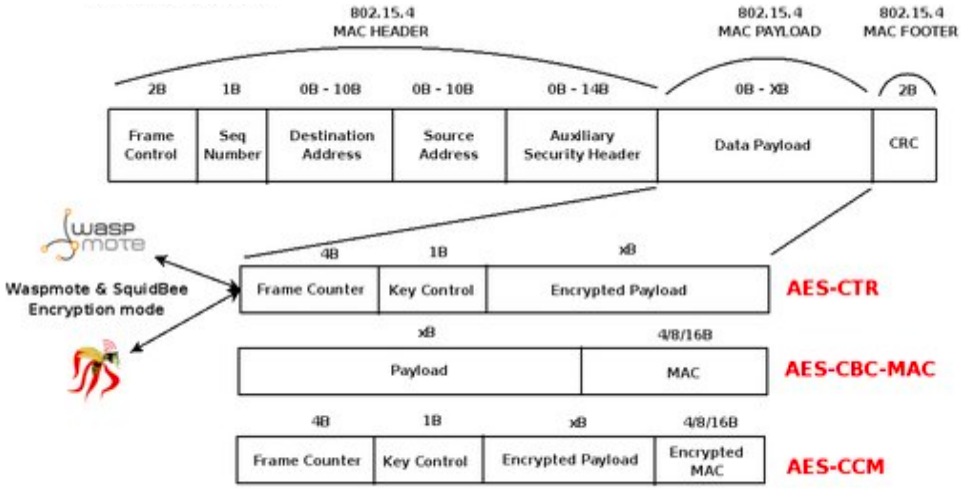


Figure 5. Le champ "Data Payload"

Comme le mécanisme appliqué sur la couche MAC, la protection de frames peut être utilisée sur la couche NWK ou la couche APS ou tous les deux couches en fonction du niveau de sécurité demandée, les implications sont montrées dans le graphique dessous.

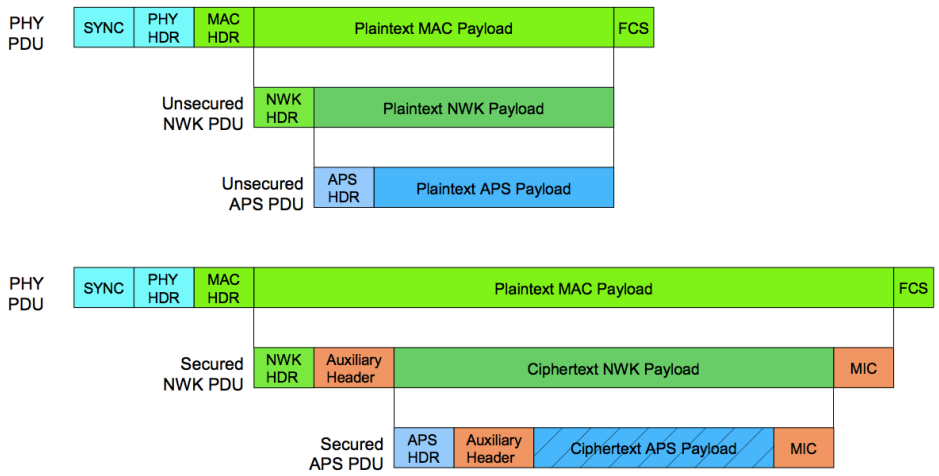
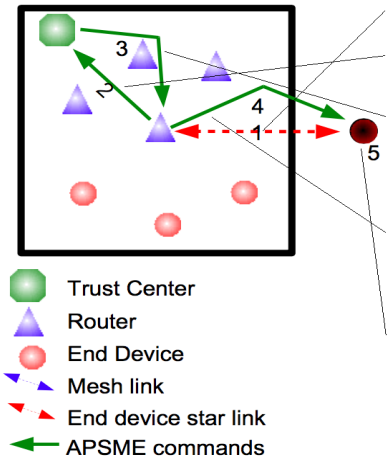


Figure 6. La protection de frames sur les couche NWK et APS

3. Le management des équipements

Même si que les messages sont sécurisés, plusieurs clés sont mises en place, des algorithmes complets peuvent être instanciés, il faut manager le moyen de rejoindre un réseau ZigBee pour éviter la faille dans les équipements d'un réseau. Généralement c'est le Centre de Confiance dans tout le réseau qui est responsable du management des équipements, la décision d'inclure un équipement au réseau est prise par lui.

Pour présenter les échanges, un exemple où un équipement procédant à une préconfigurée link-key mais sans network-key veut rejoindre le réseau est donné:



1. L'équipement fait une jointure non-sécurisée.
2. Le routeur demande d'autorisation au Centre de confiance (crypte entre routeur et TC).
3. Le TC envois la network-key (cryptée entre TC et l'équipement) via un connexion cryptée entre le routeur et TC.
4. Le routeur envois de la network-key (cryptée entre TC et l' équipement).
5. Authentification mutuelle.

Figure 7. La jointure d'un équipement

Les algorithmes

Zigbee utilise l'algorithme CCM* basé sur AES-128 pour la confidentialité, l'authentification et l'intégrité.

AES est un chiffrement par bloc dont la taille est de 128 bits. Sont clé peut varier parmi 128, 192 et 256 bits. AES contient 4 fonctions principales, c'est SubBytes, ShiftRows, MixColumns et AddRoundKey. Il a aussi des tours. Mais dans le premier tour, il a que la fonction AddRoundKey. Dans le dernier tour, il a que les autres trois fonctions sauf AddRoundkey.

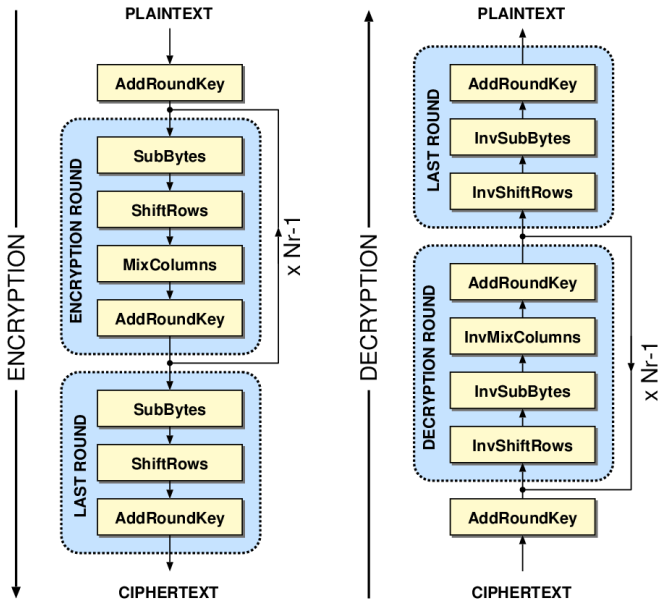


Figure 8. Chiffrement et déchiffrement de AES

Le mode CCM (Counter with CBC-MAC) est un mode d'opération pour le chiffrement par blocs. Il est un algorithme de chiffrement conçu pour fournir à la fois l'authentification et la confidentialité. Mode CCM est défini uniquement pour le chiffrement par blocs avec une longueur de bloc de 128 bits . Dans la RFC 3610, il est défini pour une utilisation avec AES.

Zigbee utilise le mode CCM* qui contient CCM mais il peut utiliser CTR et CBC-MAC seul en même temps. Il utilise CTR et CBC-MAC pour assurer la confidentialité et l'intégrité respectivement. Ainsi, une combinaison des deux façons peut fournir différent niveau de sécurité. On peut aussi choisir la longueur de MIC (Meessage Integrity Check) de 32, 64 ou 128 selon l'exigence de niveau de sécurité.

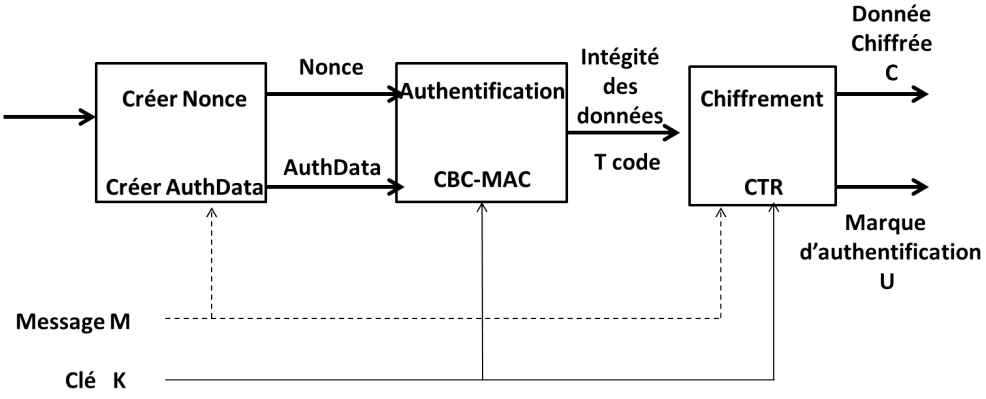


Figure 9. CCM* mode

La figure 10 et la figure11 montre que les étape de réaliser le mode CTR et CBC-MAC. Il utilise les paramètres au-dessous :

K(clé) de 128 bits ;

L (la longueur du domaine de message) integer de 2 - 8 ;

M(la longueur du domaine d'authentification) de (0, 4, 6, 10, 14, 16) ;

Nombre aléatoire N(Nonce) de longueur de (15-L) ;

Donnée d'authentification 'a' de longueur l(a), $0 <= l(a) < 2^{64}$;

Message 'm' de longueur de l(m), $0 <= l(m) < 2^{8L}$;

Transformation d'entrée : L'objective de transformation d'entrée est pour créer AuthData et PlaineText-Data utilisé par authentification et chiffrement à partir de 'a' et 'm', où AuthData = AddAuthData || PlaintextData.

Transformation d'authentification : L'objective est pour créer le code d'intégrité T en utilisant le mode CBC-MAC. Les entrés sont le nombre aléatoire Nonce N et AuthData.

Transformation de chiffrement : L'objective est pour assurer la confidentialité en utilisant le mode CRT. Les entrés sont l'intégrité T, le nombre aléatoire Nonce N et AuthData.

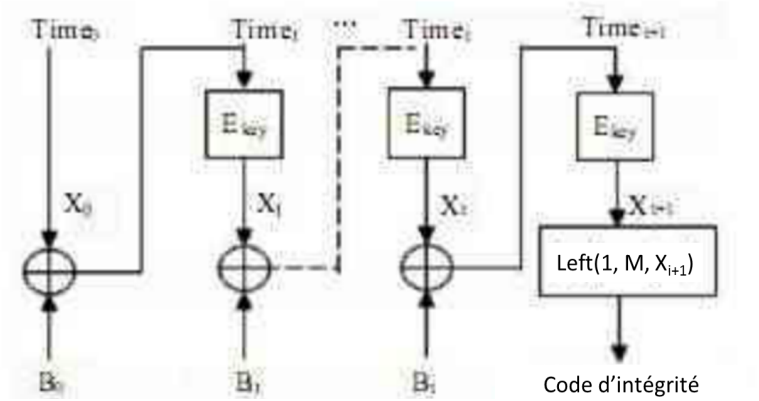


Figure 10. CBC-MAC

B0 = Reserved(1bit) ||Adata(1bit) || M || L || **Nonce N** || l(m).

$X_0 = 0128$, $X_{i+1} = E(\mathbf{K}, X_i \oplus B_i)$, for i = 0, ..., t.

Le code d'intégrité T = Left (1, **M**, X_{i+1}) // le premier M octets de X_{i+1}.

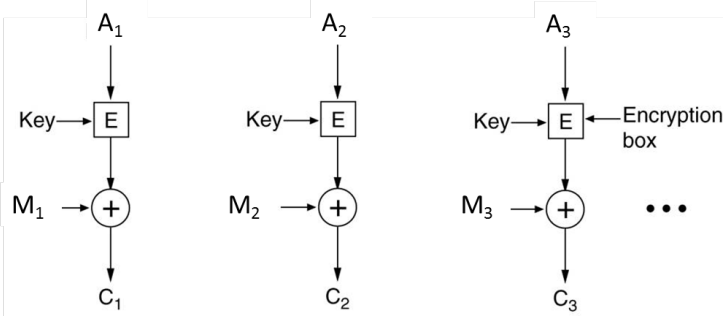


Figure 11. CTR

Le bloc chiffré $C_i = E(\mathbf{K}, A_i)$;

Le domaine de compteur A_i = Re-served || Reserved || 0 || L || Nonce **N** || Counter **i**, for i=0, 1, 2,...

Le bloc de message M_i est toujours de 128 bits.

Le bloc de chiffrement $S_0 = E(K, A_0)$

Le marque d'authentification $\mathbf{U} = \mathbf{T} \oplus left(1, M, S_0)$

Le message chiffré C = left(1, l(m), C_1 || C_2 || ... || C_t) || **U**

Références :

[1] http://en.wikipedia.org/wiki/ZigBee

[2] https://docs.zigbee.org/zigbee-docs/dcn/09/docs-09-5378-00-0mwg-zigbee-security.pdf

[3] http://www.libelium.com/security-802-15-4-zigbee/

[4] Etude du protocole, de la securite et creation d'une application ZigBee, Anthony AMBROGI, Jeremy THIMONT

[5] http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4

[6] http://www.docin.com/p-667613843.html

[7] http://www.docin.com/p-274974407.html

[8] http://www.doc88.com/p-7072010253981.html