REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud MAMMERI de Tizi-Ouzou
Faculté du Génie Electrique et d'Informatique
Département d'Informatique

Mémoire présenté pour l'obtention du diplôme Master Recherche en Informatique
Option : conduite de projets informatiques

Par Kahina CHELLI

Sujet :

Protocole matériel d'échange de clés dans les réseaux de capteurs sans fil

Devant le Jury composé de :

M^{r} LALAM Mustapha	Président
M^{r} DAOUI Mehammed	Promoteur
M^{me} AOUDJIT Rachida	Examinatrice
M^{me} BELKADI Malika	Examinateur

Promotion 2011 - 2012

Remerciements :

J'exprime ma profonde gratitude et mes vifs remerciements à mon promoteur, M[r] Mehammed DAOUI, Maître de conférence au département d'Informatique de l'UMMTO, pour l'opportunité qu'il m'a offert pour travailler sur ce projet fort intéressant, pour son encadrement, sa disponibilité, ses conseils généreux. Soyez pleinement remercié.

Je tiens aussi à exprimer l'honneur qui m'est fait par les membres de jury en acceptant d'évaluer mon travail. Qu'il trouve ici ma reconnaissance et mon respect.

Tout particulièrement, je tiens à adresser ma profonde reconnaissance à ma très chère mère Aldjia et mon très cher frère Nourddine, qui m'ont soutenu tout au long de mes études.

Dédicace :

A ma très chère mère, Aldjia

Dont ton mérite, tes sacrifices m'ont permis de vivre ce jour :

Que je te porte pour les sacrifices que tu as consenti pour ma réussite, que tu trouves ici le témoignage de mon attachement, ma reconnaissance, gratitude et respect, que dieu te préserve bonne santé et longue vie. Tous mes sentiments de reconnaissance pour toi.

A la mémoire de mon très cher père, Amar

Ton amour inconditionnel m'a racheté d'une mort prématurée certaine et a auréolé ma vie entière. Reçois à titre posthume tous égards. Tu me manqueras à jamais.

A mon très cher frère Nourddine

Recevez alors tout l'honneur que j'espérais depuis toujours vous faire à travers ce modeste travail.

A ma très chère sœur Drifa, à son mari et ses deux enfants.

A la mémoire de mes grands parents

A toutes les personnes qui me sont chères

Résumé :

Les réseaux de capteurs sans fil constituent un domaine de recherche émergeant en développement très rapide. Ils détiennent un potentiel qui révolutionne de nombreux domaines d'applications. Dans la majorité de ces applications, les nœuds capteurs sont vulnérables aux différents types d'attaques, dus à leurs différentes spécificités. Par conséquent la sécurité des réseaux de capteurs sans fil est extrêmement importante. Pour atteindre un niveau de sécurité appréciable, un protocole d'échange de clés cryptographiques est crucial, afin d'établir une communication sécurisée. Cependant, les nœuds capteurs sont dotés de ressources trop limitées en termes d'énergie, de mémoire et de calcul. Ces dernières posent des contraintes majeures pour leur sécurité, en excluant la possibilité d'appliquer les protocoles d'échange de clés classiques. Donc, le problème est comment établir des clés cryptographiques entre les différents nœuds capteurs, en prenant en compte ces contraintes inhérentes. Dans ce mémoire nous proposons un protocole matériel simple d'échange de clés adapté au contexte spécifique des réseaux de capteurs sans fil.

Table des matières :

Tables des figures :

Liste des tableaux :

Liste des algorithmes :

Introduction générale :

La convergence des avancées récentes en MEMS (Micro ElectroMechanical system), et en réseaux sans fil a favorisée l'émergence des réseaux de capteurs sans fil qui sont basé sur un effort collaboratif d'un nombre potentiellement important de nœuds capteurs, varie entre une centaine à plusieurs milliers. Chaque nœud capteur est doté de ressources très limitées (énergie, mémoire, et puissance de calcul) et d'une certaine intelligence lui permet d'observer et de contrôler certains phénomènes physiques se produisant dans leur environnement ambiant.

Cette technologie révolutionnaire connait un fort essor au sein des communautés scientifiques et industrielles, et présente de nombreuses perspectives d'applications dans des domaines très variés, tels que : la détection et la surveillance des désastres, le contrôle de l'environnement, le bâtiment intelligent, la santé, l'industrie, etc.

Cependant, l'énergie limitée des nœuds capteurs, leur déploiement aléatoire dans des environnements hostiles, la communication radio incertaine, l'absence d'une sécurité physique, rendent les réseaux de capteurs sans fil très vulnérables à divers menaces de sécurité qui peuvent compromettre l'activité réseau. Le problème sera plus critique si le réseau est déployé pour une mission sensible dont les données doivent être prouvées intègres et confidentielle, telles que le secret médical d'un patient, ou la surveillance de champ de batailles dans le domaine militaire.

Assurer les services de sécurité pour ces applications des réseaux de capteurs sans fil nécessite l'utilisation des protocoles cryptographiques. Cependant, les réseaux de capteurs sans fil se heurtent à de nombreuses contraintes sévères rendant ainsi la cryptographie asymétrique est inapplicable pour ces systèmes en raison de leur gourmandise en ressources.
La recherche en sécurité dans les réseaux de capteurs s'est alors tendu vers la cryptographie symétrique. Cette forme de cryptographie se confronte au problème d'échange de clé entre les nœuds voulant communiquer.

Par conséquent, de nouveaux schémas d'échange de clés dédiés et judicieux doivent être mises en place afin de prendre en considération les différentes contraintes imposées par ce type de réseaux.

Plusieurs protocoles d'échange de clés ont été proposés dans la littérature ces dernières années permettant de remédier aux vulnérabilités qui touchent considérablement les réseaux de capteurs sans fil, et assurant ainsi les services de sécurité. Généralement, basé sur une

approche logicielle et souffrent souvent des problèmes de scalabilité, connaissance à priori de la phase de déploiement, ou bien faiblesse face à la capture des nœuds.

Dans le contexte d'un réseau de capteurs sans fil, assurer une communication sécurisée entre des nœuds fortement contraints en ressources et déployés aléatoirement dans des environnements hostiles est un défi majeur.

Dans ce cadre, nous proposons un nouveau protocole d'échange de clés basé sur une approche matérielle adapté au contexte spécifique des réseaux de capteurs sans fil.

Organisation du mémoire :

Ce mémoire est organisé comme suit :

Chapitre 1, nous présentons l'opportunité de la sécurité dans les réseaux de capteurs sans fil.

Nous abordons ensuite dans le chapitre 2, les différentes contraintes des réseaux de capteurs sans fil influençant les protocoles d'échange de clés dans ces systemes.

Dans le chapitre 3, nous présentons notre protocole matériel d'échange de clés.

Enfin, nous terminons ce mémoire avec des résultats de simulations qui seront présentés au chapitre 4.

1

L’opportunité de la sécurité dans les réseaux de capteurs sans fil

Introduction:

Les réseaux de capteurs sans fil sont un type particulier des réseaux AdHoc, détiennent un potentiel qui révolutionne de nombreux domaines d’applications, aussi variés que militaire, industrie, environnement, ou médecine, etc. Cet engouement est principalement dû à leurs spécificités (notamment l’autonomie, le faible coût, la flexibilité, etc.), et à la disponibilité d’une large gamme de types de plateformes matérielles : thermique, optique, radiation, mouvements, vibrations, etc.

Dans la plupart des applications, les réseaux de capteurs sans fil se basent sur l’effort collaboratif des centaines voire des milliers de nœuds capteurs matériellement très contraints, souvent déployés aléatoirement dans des environnements hostiles et non contrôlés. Ces caractéristiques les rendent très vulnérables à divers type d’attaques intentionnelles ou accidentelles. De même, la nature vulnérable des communications radios sont des facteurs qui augmentent les risques d'attaques contre ce type de réseau.

La divulgation des informations échangées entre les différents nœuds peut être sans impacts dans certaines applications, telles que les applications environnementales. Cependant, la confidentialité et l’intégrité des informations recueillies sont cruciales dans d’autres applications, et l’existence de failles de sécurité représente un risque non toléré. A titre d’exemple, le secret médical d’un patient, ou la sécurité du territoire dans le domaine militaire.

Ce présent chapitre, vise essentiellement à présenter l'opportunité de la sécurité dans les réseaux de capteurs sans fil, et la nécessité d'établir des liens sécurisés entres les différents nœuds de réseaux. Nous commençons d'abord, par une description générale de cette technologie, et quelques domaines d'applications. Ensuite, nous passons à leurs spécificités. Puis, nous listons les principales vulnérabilités de ces systèmes. Ainsi, nous décrivons les principaux objectifs de la sécurité.

I. Description des réseaux de capteurs sans fil :

Comme beaucoup d'autres technologies de l'information, les réseaux de capteurs sans fil sont originalement motivés par la recherche militaire. L'agence américaine DARPA (Defense Advanced Research Projects Agency) a débuté les recherches sur ces réseaux pour des besoins militaires. Par la suite, d'autres travaux ont vu le jour où les participants étaient essentiellement les milieux universitaire dont on trouve l'université Berkeley de Californie, avec les projets SmartDust et PicoRadio [3] [8].

Un réseau de capteurs sans fil [1] [9] est un hybride des systèmes embarqués et distribués, mettant en communication ad hoc une pléthore de nœuds capteurs autonomes, matériellement très petits, dotés de ressources très limitées (énergie, mémoire, et calcul), et de diverses capacités de détections.

Suivant une architecture sans infrastructure et déploiement souvent aléatoire, les nœuds capteurs coordonnent et collaborent entre eux afin de traquer, d'observer, et de contrôler des phénomènes physiques se produisant dans leur environnement ambiants.

Les données remontées par les différents nœuds capteurs seront ensuite acheminées via les ondes radio, suivant un routage multi-sauts vers un point de collecte (éventuellement plusieurs) baptisé station de base ou puits, moyennant ainsi des protocoles dédiés. Le puits récupère les informations remontées par les différents nœuds, et les transmet à son tour par satellite ou internet au centre de traitement final.

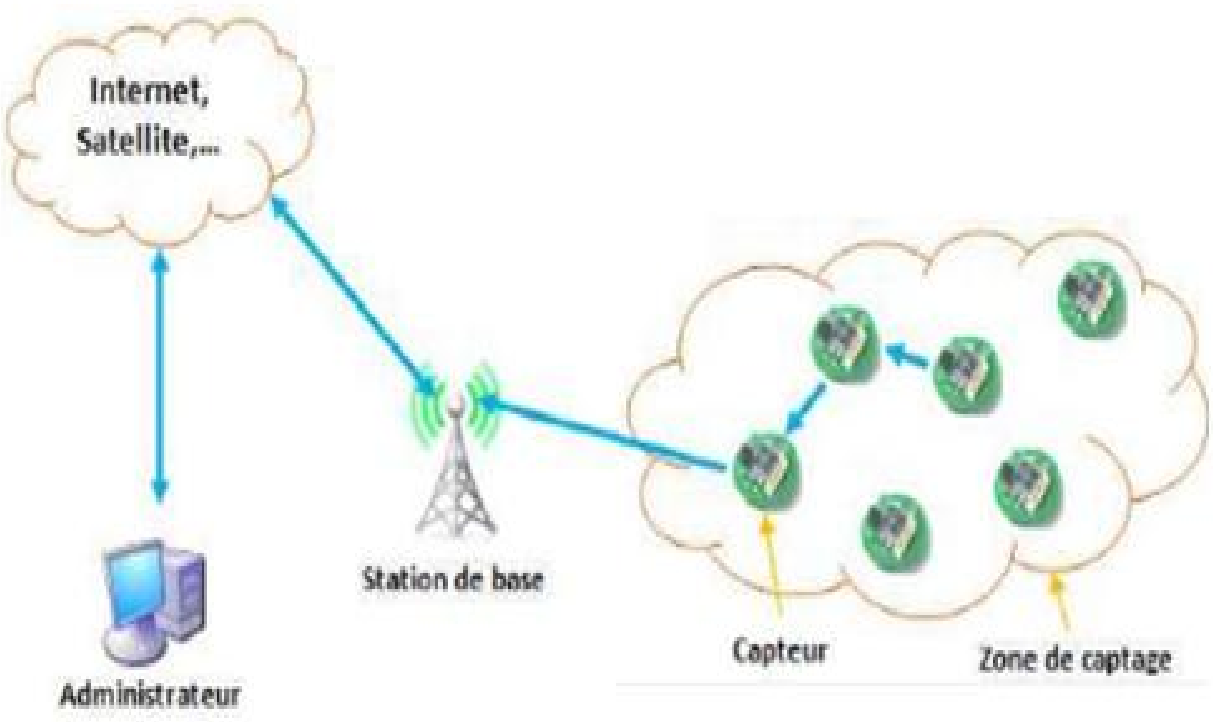


Figure.1.1. L'architecture de communication d'un réseau de capteurs sans fil.

II. Les domaines d'applications des réseaux de capteurs sans fil :

Les réseaux de capteurs sans fil servent comme une interface du monde physique réel, et leurs domaines d'applications ne cessent d'accroitre avec des impacts importants, dont les principales [1] [2] :

1. Le monitoring d'habitat :

Le monitoring d'habitat est l'une des premières applications des réseaux de capteurs sans fil. A titre indicatif, le projet dans Great Duck Island. Les chercheurs surveillent le comportement des pétrels (oiseaux palmipèdes vivent en haut mer).

Pareillement, le projet ZebraNet, qui permet la surveillance de comportement des zèbres dans les réserves Africaines au Kenya ; y compris leur migration à longue distance, leurs interactions inter-espèce, et leur comportement nocturne, en moyennant des colliers de pistage.

2. Le monitoring d'environnement :

Le monitoring d'environnement est une autre application fréquente des réseaux de capteurs sans fil. A titre d'exemple, le projet GlacesWeb vise à comprendre le mouvement glaciaire, les changements climatiques et leurs effets sur le niveau de la mer, etc.

Les réseaux de capteurs sans fil sont également déployés pour la surveillance des processus hydrologiques, météorologiques, la surveillance des changements environnementaux des forets, et la surveillance des sites industriels (ex. déploiement des capteurs sur les centrales nucléaires, ou dans les raffineries de pétrole pour détecter des fuites de produits toxique, etc.).

3. Le monitoring intelligent et permanant de la santé :

Grâce à la miniaturisation des nœuds capteurs, il est concevable d'intégrer sur et à l'intérieur de corps humain des capteurs pour la surveillance intelligente et permanente des patients. Par exemple, des nœuds capteurs peuvent mesurer la température, la pression sanguine, la glycémie, le rythme cardiaque d'un individu, ou transmettre des images en temps réel de l'intérieur d'un cops humain, etc. ce réseau est baptisé un BAN (Body Area Networks).

4. Les applications de suivi de la cible :

Parallèlement aux applications évoquées au dessus, il existe d'autres applications dites applications de suivi de la cible (target-tracking). Le concept de base, est de localiser une cible par la trilateration et d'autres techniques, moyennant de multiples capteurs capables de mesurer la distance, ou un angle d'incidence de la cible. Ce type d'application particulier de réseaux de capteurs sans fil, nécessite intrinsèquement le traitement d'informations collaboratif entre les senseurs et un niveau de sécurité adéquat.

5. Les applications militaires :

Les applications militaires sont une instance d'applications de suivi de la cible. Les réseaux de capteurs sans fil peuvent être déployés dans des endroits stratégiques, afin de surveiller toutes les activités des forces ennemis pour détecter et acquérir autant d'informations possibles sur leurs mouvements, reconnaissances des attaques nucléaires ou chimiques, et d'autres phénomènes d'intérêts.

Les réseaux de capteurs sans fil sont utilisés également pour la surveillance des champs de batailles, les systèmes de guidage pour les missiles intelligents, etc. Des exemples

typiques de ces applications sont: Les projets VigilNet, qui est une application de surveillance, et CounterSniper System qui vise à localiser les tireurs en estimant la source de l'explosion.

6. Autres applications :

Les réseaux de capteurs sans fil peuvent offrir des meilleures contributions dans des domaines assez variés. A titre d'exemple, le bâtiment intelligent. Suite à un séisme ou au vieillissement des failles pourraient être détectées par des capteurs intégrés dans les murs ou dans le béton.

Les réseaux de capteurs peuvent également être utilisés dans l'agriculture ; des capteurs sont incorporés dans la terre pour donner des informations sur l'état du champ. Ainsi, la protection des barrages pourrait être accomplie en y introduisant des capteurs.

De plus, les réseaux de capteurs sans fil jouent un rôle essentiel dans les grandes structures comme les usines, et les immeubles administratifs. Ou encore, ils ont des intérêts pour la surveillance des infrastructures, telles que les ponts (ex. Golden Gate), afin de détecter et de signaler les faiblesses structurelles, etc.

Figure.1.2. Quelques applications des réseaux de capteurs sans fil.

III. les spécificités des réseaux de capteurs sans fil :

Les réseaux de capteurs sans fil ont des spécificités exclusives qui les rendent efficaces et attrayants, dont les principales [1] [7] [8]:

1. Ressources très limitées :

Les ressources de calcul et de mémoire des nœuds sont relativement faibles. Cela, est engendré par le faible coût de fabrication des nœuds capteurs, et leur taille extrêmement miniaturisée. A titre d'exemple, le nœud capteur TelosB, qui est caractérisé par une CPU RISC sur 16 bits, avec une fréquence d'horloge de 8 Mhz, pour seulement 10 K de RAM, 48 K de mémoire pour les programmes, et une mémoire flash de 1024 K.

Non seulement les capacités des nœuds sont faibles, mais en plus ils opèrent sur des batteries, et par conséquent, ils ont une durée de vie limitée. L'énergie limitée des nœuds capteurs est leur caractéristique la plus critique.

2. Effort collaboratif et déploiement hautement massif des capteurs:

Un nœud capteur est un dispositif électronique intelligent d'une taille extrêmement miniaturisée, obtenue au détriment de ses capacités de calcul, stockage et énergétique. Ses caractéristiques rendent son déploiement tout seul inefficace. Cependant, sa collaboration, et sa coordination avec des centaines, voire des milliers de ses pairs, peuvent parvenir à atteindre un objectif bien précis.

3. Communication radio multi-sauts :

Les ressources limitées des nœuds capteurs leurs imposent des portées de transmission réduites, où chaque nœud accepte de relayer les informations récoltées à travers le réseau (un nœud capteur joue les rôles de hôte et de routeur) pour atteindre le nœud-puits. En plus, cette communication, n'est pas coûteuse en énergie, par rapport à la communication à un seul saut.

4. Capacité d'auto-organisation et topologie dynamique :

Le déploiement des nœuds capteurs est souvent aléatoire, et dans des endroits hostiles sans protection physique. Ces nœuds tombent en panne (destruction physique, épuisés en énergie, etc.), et de nouveaux nœuds rejoignent le réseau. Donc, le réseau doit être en mesure de s'auto-organiser pour continuer à remplir sa fonction.

5. Scalabilité :

La surveillance d'un phénomène peut nécessiter le déploiement d'un nombre conséquent de nœuds capteurs, varie entre plusieurs centaines à des milliers (selon l'application). Les protocoles dédiés aux réseaux de capteurs sans fil doivent pouvoir fonctionner et s'adapter selon le nombre de nœuds.

Dans la plupart des applications des réseaux de capteurs sans fil, les nœuds capteurs ont pour mission de remonter, et de router des informations souvent sensibles et cruciales. Cependant, leurs spécificités inhérentes, les rendent extrêmement vulnérables et fragiles à un certain nombre d'attaques préjudiciables. De plus, l'absence d'une sécurité physique pour ce type de réseau (déploiement aléatoire, souvent dans des environnements hostiles), et la nature vulnérables des liens radio, sont des facteurs qui augmentent les risques d'attaques [6] [7] [9].

IV. Les vulnérabilités des réseaux de capteurs sans fil :

Nous décrivons ici, les principales vulnérabilités des réseaux de capteurs sans fil, qui sont exploitées par l'attaquant afin de gagner des privilèges [6] [9].

1. Communication radio et effort collaboratif des nœuds :

Un réseau capteurs sans fil est basé sur une collaboration de plusieurs milliers de nœuds ; ce nombre conséquent implique une communication radio broadcast. Cette dernière, est due en fait, à l'inaptitude d'avoir une connaissance globale sur la topologie et d'appliquer le protocole IP. Ceci, est ajouté à la nature versatile des ondes radio.

Ces facteurs rendent les réseaux de capteurs sans fil très vulnerables à plusieurs types d'attaques intensionnelles et préjudiciables simple à réaliser, comme les interférences. Ou encore, quiconque possédant un récepteur adéquat peut potentiellement écouter clandestinement les différentes communications, etc.

2. Transmission à distance :

Le pilotage direct des nœuds peut s'avérer difficile (téléchargement de code) en raison des environnements hostiles. Il est donc, judicieux de les commander à distance. Cependant, ce mode de transmission à distance entraine une augmentation du temps de communication ; et cela est favorable pour un attaquant, qui peut provoquer des collisions. Ou encore, il peut injecter son propre code malveillant.

3. Couplage avec l’environnement de déploiement :

Dans la plupart des applications des réseaux de capteurs sans fil, les nœuds capteurs sont déployés à l'intérieur ou à proximité des phénomènes à observer. Ce couplage étroit avec l'environnement conduit à de fréquentes compromissions intentionnelles, ou accidentelles des nœuds. Car les environnements de déploiements des réseaux de capteurs sans fil sont souvent non contrôlés, dont l’accès n’est nullement restreint.

4. Faible coût :

Comme le succès des applications des réseaux de capteurs sans fil dépendent également de leur faible coût ; les nœuds ne peuvent pas se permettre une protection physique inviolable.

Ces deux derniers facteurs fragilisent le réseau d’une manière non négligeable, et le rendent vulnérable à diverse attaques potentielles. A titre indicatif, la capture physique des nœuds par un adversaire. Ce dernier peut extraire toutes les informations confidentielles et sensibles stockées sur ces nœuds, et télécharge son code malveillant puis les remet au réseau. Dans ce cas, les nœuds eux-mêmes sont des points de vulnérabilité. Par conséquent, ces nœuds malicieux peuvent relayer les différents paquets qui circulent à travers le réseau, du fait que le routage est multi-saut et chaque nœud participe à l’acheminement des paquets.

V. les objectifs et les exigences de la sécurité [5] [7] [9]:

1. La confidentialité :

La confidentialité est la primitive clé de la sécurité des réseaux de capteurs sans fil. L’objectif requis de la confidentialité, est d’entretenir le secret des messages échangés à travers le réseau, contre les attaques passives (ex. l’analyse de trafic). Particulièrement, dans les applications militaires et médicales, où des informations sensibles sont remontées, et communiquées entre les nœuds.

Une approche standard pour garantir la confidentialité et de protéger contre la divulgation des informations critiques est la cryptographie. Sans les clés de décryptage correspondantes, les attaquants sont incapables d'accéder à l'information critique.

2. L'intégrité :

La garantie de la confidentialité n'implique pas que les données soient intactes. Les attaquants peuvent introduire des interférences sur quelques morceaux d'un paquet transmis, afin de changer sa destination, son contenu, etc. Donc, l'intégrité des données est une composante de sécurité potentiellement significative, qui fait référence à l'habilité de certifier que les données n'ont pas été falsifiées pendant la transmission, intentionnellement (par un attaquant), ou accidentellement (due au canal radio peu fiable).

3. L'authenticité :

L'authenticité permet à chaque nœud capteurs d'avoir l'habilité de vérifier l'identité des nœuds pairs avec lesquels il communique. Sans l'authenticité, un attaquant peut se faire passer pour un nœud légitime et obtenir l'accès aux ressources et aux informations critiques, et perturbe ainsi le fonctionnement des nœuds légitimes. Donc l'authenticité a un impact considérable sur la vie de réseau.

4. La disponibilité :

La disponibilité est un aspect important dans les réseaux de capteurs sans fil. Elle permet de s'assurer que chaque nœud peut toujours communiquer avec ses voisins dans le réseau, et que leurs données soient accessibles. En d'autres mots, le réseau est en mesure d'être toujours apte à fournir des services quand ils sont requis.

5. La fraicheur des données :

Même si la confidentialité et l'intégrité des informations sont assurées, nous avons besoin de certifier que chaque message est récent, et aucun attaquant peut retransmet des anciens messages. Ce requis, est considérablement important lorsque des stratégies d'échanges de clés cryptographiques, sont élaborées dans la conception des réseaux de capteurs sans fil.

Une solution clé, pour les réseaux de capteurs sans fil en vue d'éliminer la plupart des vulnérabilités liées à leur sécurité, est la cryptographie. Pour que les schémas cryptographiques soient applicables et sécurisés, ils doivent avoir une méthode efficace et fiable d'échange de clés.

Autrement dit, pour établir une communication sécurisée entre les différents nœuds du réseau et empêcher qu’il soit compromis par un adversaire, un mécanisme d’échange de clés fiable doit être mis en place.

VI. L’échange de clés dans les réseaux de capteurs sans fil:

Les protocoles d’échange de clés est l’une des mesures fondamentale, et l’un des aspects les plus difficiles pour la configuration d'un système cryptographique de sécurité. Car, la sécurité de tout système cryptographique est basée sur la fiabilité de son mécanisme d’échange de clés. Ce dernier, est défini comme le processus qui permet la production, la distribution, le renouvellement, et la destruction des clés cryptographiques. En fait, il représente une nécessité pour tout système de communication [5].

L’échange des clés cryptographiques, lors du déploiement d’un réseau de capteurs sans fil est l’une des exigences primaires, pour prohiber plusieurs types d’attaques contre ce type de réseau. Le problème sera trivial à résoudre si l’application de protocoles d’échanges de clés traditionnel, comme Diffie-Hellman était possible.

Malheureusement, ces protocoles sont très gourmands en temps d’exécution, en mémoire, et en énergie. Cette dernière représente l’handicape majeur pour les réseaux de capteurs sans fil.

Depuis quelques années, plusieurs recherches sont axées sur ce problème d’échange de clés dans les réseaux de capteurs sans fil. En fait, les réseaux de capteurs sans fil possèdent plusieurs contraintes strictes et inhérentes. Certaines liées à la technologie sous-jacente des nœuds capteurs et d’autres au réseau. Encore d’autres sont liées à l’environnement de déploiement [7].

Ces différentes contraintes, imposent de se focaliser sur une sécurité mieux adaptée répondant aux exigences de mission à accomplir et dans des conditions satisfaisantes.

Conclusion:

Les réseaux de capteurs sans fil présentent des intérêts considérables et croissants, et leurs domaines d’applications ne cessent d’accroître.

Dans beaucoup d’applications, les informations circulant à travers le réseau sont vulnérables à de nombreuses menaces. Ces vulnérabilités exposent ces réseaux à de nombreuses attaques qui peuvent porter atteinte à la sécurité de ces données échangées, ainsi qu'au bon fonctionnement du réseau.

Dans ce chapitre nous avons présenté les réseaux de capteurs sans fil, leurs principaux domaines d’applications, ainsi leurs spécificités exclusives. Nous avons aussi, abordé l’aspect sécurité et son opportunité pour ces réseaux. Ainsi que le besoin d’établir une communication sécurisée entres les différents nœuds du réseau.

Malheureusement, les protocoles d’échange de clés appliqués aux réseaux classiques sont inapplicables pour les réseaux de capteurs sans fil en raison de leurs contraintes, qui rendent l’échange de clés dans ces systèmes un défi majeur.

Le chapitre suivant sera une étude des diverses contraintes des réseaux de capteurs sans fil qui influencent les protocoles d’échanges de clés.

2

Les contraintes des réseaux de capteurs sans fil relatives aux stratégies de sécurité

Introduction :

Les réseaux de capteurs sans fil constituent un domaine de recherche en développement très rapide, avec une large utilisation dans différents domaines d'applications, exigeant une grande sécurité.

Cependant, ces réseaux se heurtent à de nouveaux problèmes fondamentaux, provenant principalement des capacités réduites des nœuds capteurs individuels : basse puissance, énergie limitée, et faible capacité de stockage. Ainsi, de leurs caractéristiques réseau : déploiement fortement dense et aléatoire, souvent dans des environnements hostiles et sans protection physique, couplage avec l'environnement, etc. Ces problèmes forts s'ajoutent à ceux hérités des réseaux Ad Hoc, tels que la communication radio incertaine et sans infrastructure, la nature distribuée des applications, etc.

Ces contraintes sévères restreignent voire excluent la possibilité d'appliquer les mesures de sécurité existantes, et imposent la conception de nouvelles solutions efficaces, prenant en compte les différentes contraintes imposées, afin de pouvoir sécuriser les réseaux de capteurs sans fil sans consommer leur énergie, qui est la métrique primaire de performance de ces réseaux.

Dans ce chapitre, nous commençons par une description technologique et architecturale des nœuds capteurs. Ensuite, nous abordons les différentes contraintes qui

influencent les protocoles d'échange de clés dans réseaux de capteurs sans fil. A la fin, nous présentons une brève description des solutions proposées dédiées au contexte de ces réseaux.

I. Description d'un nœud capteur sans fil:

Dérivés de la technologie MEMS (**M**icro **E**lectro**M**echanical **S**ystem), les nœuds capteurs sont des dispositifs électroniques embarqués, autonomes, extrêmement miniaturisés, et à faible coût. Ces dispositifs intelligents qui sont dotés de ressources très limitées en termes de calcul, de mémoire, et d'énergie ; servent à la surveillance et au contrôle des phénomènes physiques se produisant dans leur environnement ambiant. Les mesures remontées peuvent tant concerner la température, la pression, les radiations, le mouvement, la lumière, le son, etc. Leur rôle est également de transformer l'état de ces grandeurs physiques observées en un signal numérique, afin qu'elles soient plus aisément manipulables, et de les communiquer si nécessaire à leurs voisins distants de quelques mètres tout au plus, via les ondes hertziennes [1] [9].

1. Aspect technologique :

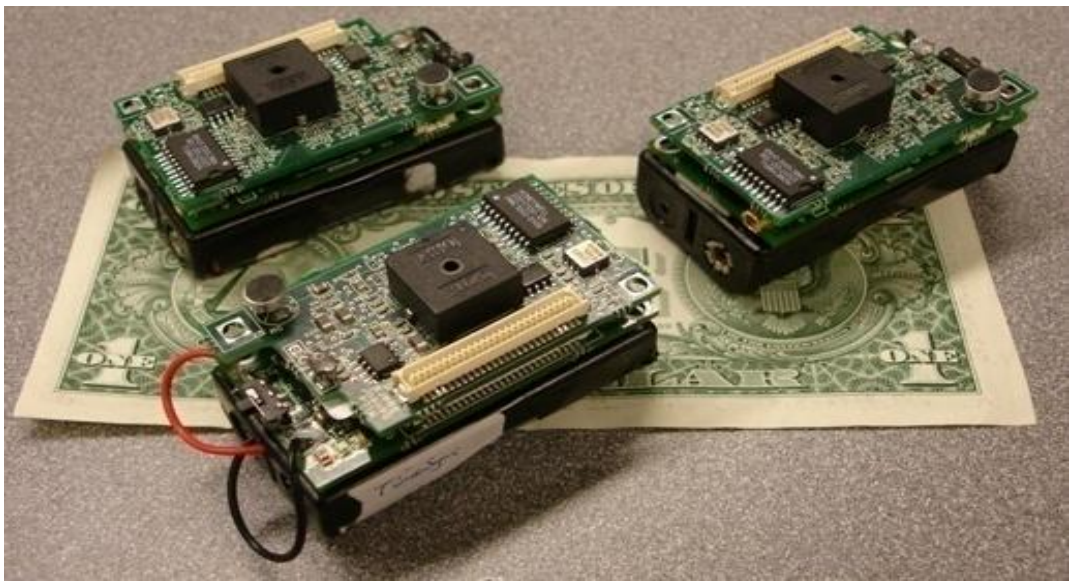


Figure.2.1. Aspect technologique des nœuds capteurs sans fil.

2. Détails d'une architecture matérielle typique d'un nœud capteur sans fil:

De nombreuse plateformes matérielles de nœuds capteurs sans fil sont disponibles, incluent par exemple TelosB, RatMote, MICAZ, et bien d'autres. Tous ces nœuds partagent des propriétés matérielles souvent limitées, avec parfois quelques spécificités liées aux applications pour lesquels ils sont conçus.

Une architecture matérielle typique d'un nœud capteur sans fil intègre les unités suivantes [1] [9]:

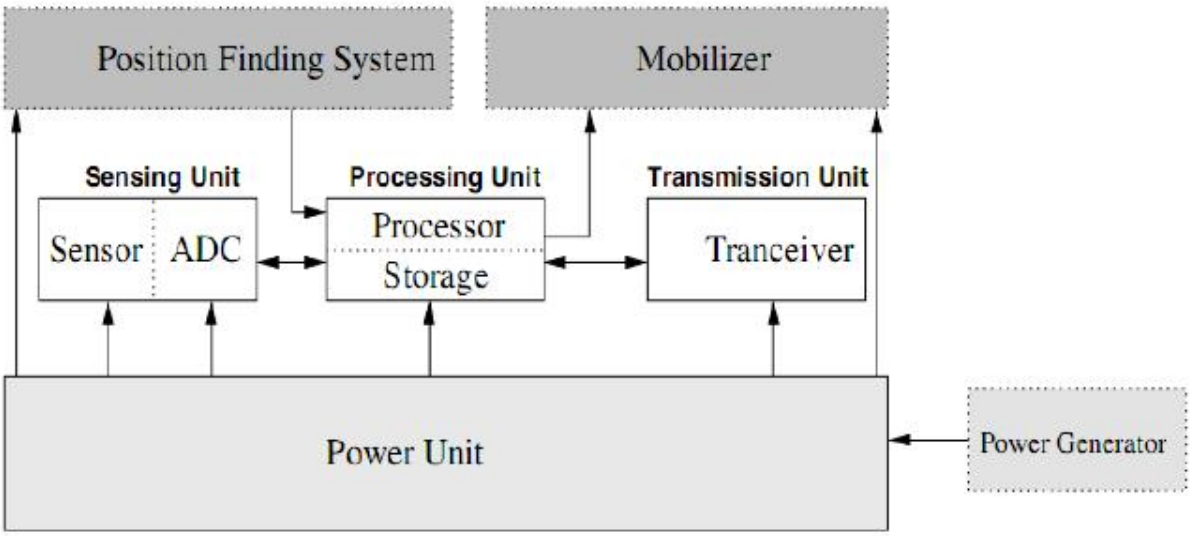


Figure.2.2. l'architecture typique d'un nœud capteur sans fil.

1. Unité de d'acquisition :

Elle consiste en deux composants, un dispositif qui intercepte les données du monde physique et les transforme en signaux analogiques, et un convertisseur analogique/numérique qui transforme ces signaux analogiques en un signal numérique compréhensible par l'unité de traitement ;

2. Unité de traitement :

Cette unité est composée d'un microprocesseur ou d'un microcontrôleur, associé généralement à une unité de stockage. Ces deux composants permettent le fonctionnement global du nœud capteur en assurant son démarrage, son fonctionnement, le traitement des données, etc. ils dépendent bien sûr de type de nœuds capteurs utilisés. Mais globalement ces ressources sont limitées.

3. Unité de communication :

Elle est responsable des émissions et des réceptions des données sur un medium sans fil. Elle se base sur les technologies sans fil à faible portée de communication, Zigbee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1), ou WiFi (IEEE 802.11);

4. Unité d'alimentation énergétique :

C'est l'unité la plus critique d'un nœud capteur. Elle est responsable de la gestion de l'énergie et de l'alimentation de tous les composants du nœud capteur. Elle consiste généralement en une batterie avec une quantité d'énergie limitée, souvent ni rechargeable, ni remplaçable.

II. Contraintes des réseaux de capteurs sans fil relatives à la sécurité:

L'une des spécificités particulières des nœuds capteurs est leur taille extrêmement miniaturisée. Certaines applications requièrent parfois des nœuds d'une taille très petite, pouvant être d'ordre d'une poussière (par exemple, les nœuds capteurs Smart Dust, ou la poussière intelligente) restants en suspension dans l'air.

Cette spécificité ajoutée au faible coût de fabrication et aux caractéristiques héritées des réseaux Ad Hoc créent de nombreuses contraintes sévères influencent d'une façon considérable les mécanismes d'échange de clés dans les réseaux de capteurs sans fil.

II.1. Contraintes matérielles [5] [7] [9]:

Le besoin de déployer les nœuds capteurs dans des environnements stratégiques, a poussé les concepteurs de plus en plus à miniaturiser leur taille. L'architecture physique des nœuds capteurs se retrouve alors impactée par l'adoption de capacités de calcul, et de mémoire très limitées.

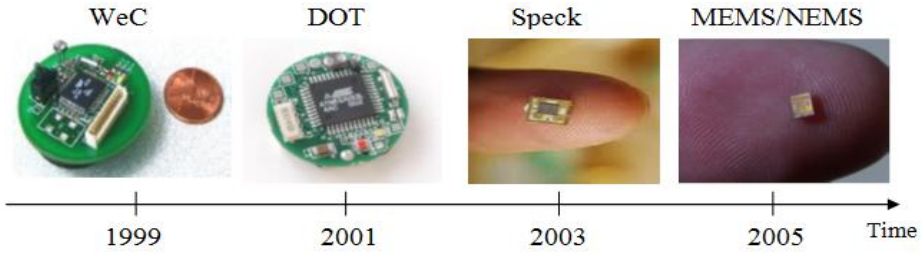


Figure.2.1. Progression des technologies des nœuds capteurs à travers le temps.

1. Capacité énergétique limitée :

L'énergie est la contrainte la plus critique dans réseaux de capteurs sans fil. La taille réduite des nœuds implique des batteries miniaturisées avec des quantités d'énergie limitées. De plus, une fois déployés il est difficile voire impossible de pouvoir changer ou recharger leurs batteries. Il est également plus difficile d'intervenir pour localiser le nœud capteur défaillant, dû au déploiement hautement dense et aléatoire des nœuds, ainsi qu'à leurs environnements hostiles et inaccessibles. Par conséquent, la faible consommation d'énergie est une exigence principale pour les protocoles de sécurité, afin prolonger la durée de vie du réseau ;

2. Espaces de stockage et mémoire limités :

Un nœud capteur a un espace mémoire des programmes et de stockage des données très limité. Par conséquence, pour développer un mécanisme d'échange de clé efficace, il est nécessaire de limiter la taille du code. À la moyenne, la plupart des nœuds capteurs sans fil possèdent une mémoire de programme seulement de 10 à 64 Kilo Octets, et une capacité de stockage flash de 512 Kilo Octets à 4 Miga Octets. Avec une telle contrainte, les logiciels des nœuds doivent également être assez petits. Par exemple, l'espace totale de code TinyOS, un système d'exploitation standard pour les nœuds capteurs, est approximativement 4 K. Son scheduler occupe seulement 178 Octets ;

3. Capacité de calcul limitée :

Malgré les progrès récents dans la fabrication de circuit intégrés de plus en plus puissants, les nœuds capteurs actuels souffrent d'un manque de puissance de calcul. Ils fonctionnent généralement avec des registres de 8 à 16 bits. A titre d'exemple, un nœud capteur TelosB utilise un microcontrôleur MSP430 fabriqué par Texas Instrument, cadencé à 8MHz. Il dispose de 10 Kilo Octets de RAM et de 48 Kilo Octets de mémoire flash. Ce microcontrôleur est optimisé pour répondre aux contraintes d'économie d'énergie des nœuds capteurs, d'où son cadencement faible. De ce fait, il a une capacité de calcul assez limitée. Généralement, il fait un compromis entre le niveau de performance et la consommation d'énergie ;

4. Bande passante limitée et communication radio à faible portée :

Afin de minimiser l'énergie consommée lors de transmission des données (compte tenu que le module radio est le plus gourmant), la bande passante des nœuds capteurs est très restreinte. Typiquement, le débit utilisé ne dépasse pas quelque centaine de Kilo Octets par

seconde. De plus, le module radio a une portée de quelques dizaines de mètres, variable selon l'environnement de déploiement et la fréquence radio.

Capteurs	**MicaZ**	**Telos**	**Inote2**	**WSN430**
Processeur	Atmel AT-Mega 128L	TI MSP430	Intel PXA271 XScale	TI MSP430
Vitesse du processeur	16 MHz	8 MHz	13 - 416 MHz	8 Mhz
RAM	4 Ko	2 Ko / 10 Ko	256 Ko	10 Ko
Espace programme	128 Ko	60 Ko / 48 Ko	32 Mo	48 Ko
Flash	512 Ko	256 Ko	32 Mo	1 Mo
Communication série	UART	DIO,SPI, I2C, UART	UART,GPIO	DS2411
Batterie	2xAA	2/3A	3x AAA	PoLiFlex
Voltage	2.7 V	1.8 - 3.6 V	3.2 - 4.5 V	2.2 V
Radio	TI CC2420 802.15.4	TI CC2420 802.15.4	TI CC2420	TI CC1100
Fréquence (MHz)	2400-2483	2400-2483	2400-2483	315/433/868/915
Débit de données (Kb/s)	250	250	500	250

Tableau.2.1. Différentes caractéristiques matérielles de quelques nœuds capteurs.

5. le faible coût de fabrication :

La taille extrêmement miniaturisée des nœuds capteurs obtenue au détriment de ses ressources en termes d'énergie, de mémoire, et de puissance du calcul, rend ainsi son déploiement tout seul inutile. Mais, sa collaboration avec des milliers voire des millions de nœuds pairs leur permettent d'accomplir leur tâche. Par conséquence, le coût de production d'un seul nœud capteur est crucial pour l'évaluation de coût global du réseau. De même, les contraintes intrinsèques liées aux environnements de déploiement imposent l'utilisation des nœuds capteurs à faible coût.

Akyildiz et al. [1] suggèrent que le coût d'un seul nœud doit être beaucoup moins d'un Dollar pour la faisabilité des solutions des réseaux de capteurs sans fil.

Cependant, ce faible coût des nœuds capteurs restreint énormément leurs capacités de calcul, et de mémoires. Ainsi, l'utilisation de composants d'autodestruction (dits tamper-resistant, qui sont relativement chers) n'est pas possible.

La minimisation du coût de production des nœuds capteurs constitue actuellement un grand défi, vu les fonctionnalités que doivent comporter ces nœuds capteurs et l'objectif désiré pour un coût inférieur à un Dollar ;

Inévitablement, ces contraintes fortes posent de nouveaux challenges considérables pour la sécurité des réseaux de capteurs sans fil. L'énergie, l'espace mémoire limités, et la faible puissance de calcul, excluent la possibilité d'appliquer les mécanismes d'échange de clés existants qui sont gourmands en ressources.

En plus à ces contraintes liées à la technologie sous-jacente des nœuds capteurs, il ya des contraintes liées au réseau qui posent aussi des challenges potentiels généralement hérités des réseaux MANETS.

II.2. Contraintes réseau [7] [9]:

1. Communication sans fil peu fiable :

Les ondes radio permettent aux nœuds capteurs d'être installés facilement dans les zones d'intérêts. Cependant, elles soulèvent plusieurs défis. La limite de la puissance d'émission ainsi que la bande de fréquences non propriétaire (partagée), ajouté à une forte densité de déploiement impliquent de fortes interférences, des phénomènes d'atténuation, de réflexion et de distorsion, affectant la transmission de données des nœuds capteurs. Les nœuds capteurs doivent donc trouver un équilibre pour pouvoir garantir la bonne réception des paquets et en même temps pouvoir garder leurs batteries pour une durée optimale ;

2. Routage incertain :

Un réseau de capteurs sans fil est très contraint en ressources et particulièrement en énergie. Par conséquent, le routage multi-saut est le plus opportun pour l'acheminement des données. Ce mécanisme du routage est d'autant plus critique : les nœuds capteurs ne peuvent communiquer qu'avec les pairs de leur voisinage ambiant qui vont relayer les paquets à travers le réseau. De plus, les paquets sont routés via le canal radio qui est de nature incertaine. En fait, la fragilité des liens radio représente la majeure faiblesse des réseaux communicants sans fil ;

3. Collisions et temps de latence :

La communication broadcast dans les réseaux de capteurs sans fil implique des collisions des paquets dans le canal sans fil. Avec la forte densité des nœuds capteurs dans le réseau, cela peut être un problème majeur.

De plus, la synchronisation entre les nœuds capteurs sera une tâche difficile, et affectera la distribution de clés cryptographiques. Ceci est d'autant critique lorsque le routage multi-sauts, la congestion du réseau, et le traitement des données au niveau des nœuds de capteurs, augmentent le délai de transmission dans le réseau.

De plus, les contraintes intrinsèques liées à l'environnement d'utilisation des nœuds capteurs imposent des restrictions fortes de la quantité de mémoire, et la capacité de calcul dont ils disposent. Ainsi, le respect de contraintes de réactivité est souvent imposé, puisque les nœuds fonctionnent de manière couplée avec leur environnement. Par exemple, le temps maximum autorisé pour la prise d'une décision par le microprocesseur (ou le microcontrôleur) dépend du système physique qu'il contrôle. Un dépassement de cette borne peut avoir des conséquences critiques.

III. Besoin de nouveaux protocoles d'échange de clés dédiés aux réseaux de capteurs sans fil [7] [9]:

Nous le voyons donc, les réseaux de capteurs sans fil se distinguent des réseaux ad hoc et des réseaux classiques par des contraintes différentes en termes d'énergie, de mémoire, de puissance de calcul, de communication multi-sauts, de nombre potentiel de nœuds, de mode de déploiement aléatoire, etc.

Ces contraintes servent comme directives pour le développement de nouvelles stratégies d'échange de clés dédiées et mieux adaptées aux réseaux de capteurs sans fil. De plus, les nouveaux protocoles d'échange de clés doivent être extensibles à des réseaux formés par des centaines voire des milliers de nœuds capteurs sans fil. Par conséquence, un nombre de clés potentiellement important qui nécessite une gestion soigneuse, afin de prendre en considération les contraintes matérielles des nœuds.

De même, ces nouveaux schémas doivent aussi être adaptatifs à la topologie hautement dynamique du réseau : un nœud rejoignant le réseau doit établir des clés avec les

nœuds voisins, un nœud exclu de réseau, ne doit jamais pouvoir établir une communication avec les nœuds du réseau, etc.

L'échange de clés dans les réseaux de capteurs sans fil est jusqu'à aujourd'hui une question critique qui a retenu l'attention de la communauté scientifique. car elle doit tenir compte des faibles ressources à disposition et de la possibilité de capture physique de nœuds capteurs.

Concevoir des solutions d'échange de clés simples, qui doivent prendre en compte les différentes contraintes imposées par ce type de réseaux et permettant la sécurisation des communications, tout en consommant le moins d'énergie possible, ainsi adaptées à une fréquence d'exécution adéquate, est un challenge loin d'être trivial.

La majorité des travaux de recherche menés actuellement concernant les protocoles d'échange de clés pour les réseaux de capteurs sans fil se basent sur un concept commun, qui est le pré-établissement de clés. Ce concept exige un chargement d'information secrète dans les nœuds capteurs avant leur déploiement dans le réseau. Cette information secrète peut être la clé secrète ou une autre information qui permet aux nœuds de dériver la clé secrète réelle. Il ya quatre protocoles de d'échange de clés dans la littérature dédiés aux réseaux de capteurs sans fil, qui sont [5]:

1. Les protocoles déterministes : ces protocoles établissent un lien entre l'identifiant d'un nœud et les clés qui ont été préétablies en lui, pour dériver les clés entre les paires de capteurs ;

2. Les protocoles probabilistes : suivant ces protocoles, les nœuds seront déployés avec un sous-ensemble de clés prises d'un ensemble de clés initialement généré par une entité de confiance, d'une manière à assurer que deux nœuds partage au moins une clé commune avec une forte probabilité ;

3. Les protocoles géographique : la localisation géographique permet aux nœuds de construire une clé commune en utilisant la position des ces derniers dans le réseau. Cela permet d'une part, de déterminer et localiser l'impact d'un nœud compromis et d'autre part d'augmenter la connectivite du réseau. Généralement ces protocoles requirent l'utilisation de composants spéciaux tels que le GPS ou des algorithmes de localisation ;

4. Les protocoles dits t-secure : ils se basent sur des schémas cryptographiques proposés dans la littérature et qui résistent à la corruption de t nœuds où t est un seuil dépendant du schéma utilisé.

Cependant, ces protocoles souffrent souvent des problèmes de scalabilité, connaissance à priori de la phase de déploiement, ou bien faiblesse face à la compromission des nœuds.

Donc, il faut encore chercher des solutions qui puissent concilier l'échange de clés entres les différents nœuds capteurs, la durée de vie, et la rapidité d'exécution des microprocesseurs des nœuds capteurs.

Conclusion :

Bien qu'ils apportent de nombreux avantages, les réseaux de capteurs posent un certain nombre de défis majeurs. En effet, le faible coût de fabrication et la taille réduite des nœuds engendrent des ressources très limitées en termes d'énergie, de mémoire et de calcul. De ce fait, les protocoles d'échange de clés développés pour les réseaux classiques ne sont pas adaptés aux réseaux de capteurs sans fil. C'est pourquoi, de nouvelles approches d'échange de clés dédiées doivent être mises en place, afin de tenir compte les différentes contraintes imposées par ce type de réseaux.

Dans le chapitre suivant, nous proposons un nouveau protocole d'échange de clés basé sur une approche matérielle adapté au contexte des réseaux de capteurs sans fil.

3

Conception de notre protocole matériel d'échange de clés

Introduction :

Dans la plupart des applications des réseaux de capteurs sans fil, la tâche essentielle des nœuds capteurs est la collecte des données physiques depuis leur environnement. Ces informations sensibles doivent être prouvées intègres et confidentielles. Ces deux propriétés cryptographiques sont indispensables pour la sécurité de ces réseaux.

Cependant, malgré que la cryptographie asymétrique fournie de nombreux avantages, elle reste inapplicable pour ce type de système en raison de leur gourmandise en ressources. Cependant, comme nous l'avons vu dans le chapitre précédent, les capacités individuelles des nœuds capteurs sont très réduites, et ne peuvent pas supporter des protocoles complexes.

Actuellement, la cryptographie symétrique est préférable pour les réseaux de capteurs sans fil. Toutefois, un nouveau problème émerge dans ce cas, et concerne l'échange de clés (qui doivent être secrètes) dans le réseau entre les différents nœuds y compris la station de base. Donc, le problème à soulever est comment établir des clés cryptographiques entre les différents nœuds capteurs.

Dans ce contexte, nous proposons un protocole simple basé sur une approche matérielle. Ce nouveau schéma s'appuie sur le protocole d'échange de clés Diffie-Hellman. Ce protocole réalisé d'une façon matérielle consiste en un circuit électronique permettant principalement d'alléger les calculs des nœuds capteurs.

Dans ce chapitre nous abordons d'abord les concepts de la cryptographie asymétrique et symétrique. Par la suite nous présentons la version originale du protocole Diffie-Hellman, sur lequel se base notre travail. Nous passons ensuite à la présentation détaillée de notre protocole matériel d'échange de clés.

I. La cryptographie :

La cryptographie est une fonction vitale de la sécurité, qui consiste en un ensemble de techniques permettant de protéger une communication moyennant un code secret. On distingue deux formes de cryptographie [10].

1. La cryptographie symétrique :

C'est la cryptographie la plus ancienne également dite à clé secrète. Elle nécessite pour fonctionner que les deux nœuds communicants puissent au préalable échangés une clé secrète connue seulement d'eux. Cette clé secrète est utilisée pour le cryptage et le décryptage. Cette forme de cryptographie permet de garantir la confidentialité, et l'intégrité de donnée [5] [10];

2. La cryptographie asymétrique :

C'est une cryptographie moderne qui a vu le jour dans les années soixante-dix. Au lieu d'une seule clé, il ya deux clés différentes. Une clé publique (qui sera diffusée) pour crypter et une clé privée (gardée secrète) pour décrypter. Chaque nœud peut à l'aide de la clé publique du destinataire crypter un message, et seule le destinataire en possession de la clé privée peut le décrypter [5] [10].

La cryptographie asymétrique repose sur des problèmes mathématiques réputés difficiles. Les plus utilisés sont la factorisation de grands nombres premiers entiers et le logarithme discret. Cette nouvelle forme de cryptographie permet de ne pas pré-charger une clé dans les deux nœuds souhaitant communiqués, de garantir la confidentialité, et de la non répudiation de données, ainsi elle facilite la gestion des clés qui est le défi majeur de la cryptographie symétrique [10].

Cependant, malgré l'aspect révolutionnaire de la cryptographie asymétrique, ce type de cryptographie est impraticable pour les réseaux de capteurs sans fil à cause des contraintes fortes et inhérentes de ce type de réseau vues au chapitre précédent. Pour cela, la plupart des

solutions proposées pour ce type particulier de réseau utilisent uniquement les primitives issues de la cryptographie symétrique.

Malheureusement, la cryptographie symétrique nécessite un partage d'une clé secrète entre les nœuds avant leur déploiement. D'ailleurs c'est leur handicape majeur, car elle s'appuie intégralement sur la non divulgation de cette clé partagée. Si cette dernière est compromise, le réseau est aussi compromis. De plus, si le réseau à N nœuds souhaitant communiquer secrètement, il faut distribuer N*(N-1)/2 clés différentes. Pour un réseau de plusieurs milliers de nœuds, ceci peut être un grand problème [10].

L'échange des clés est l'un des aspects les plus difficiles de la sécurité. Il se fait généralement soit avec un cryptage à clé publique comme par exemple RSA, soit avec le protocole d'échange de clé Diffie-Hellman.

II. Protocole d'échange de clés Diffie-Hellman :

Baptisé d'après les noms de ses inventeurs Whitfield Diffie et Martin Hellman. C'est le premier algorithme à clé publique qui fut inventé en 1976. Sa sécurité repose sur la difficulté de calcul des logarithmes discrets sur un corps fini. Il permet à un groupe d'entités qui ne se connaissent pas au préalable d'échanger une clé secrète sur un canal non sécurisé [10].

Son principe est le suivant :

Pour échanger une clé cryptographique secrète entre deux entités A et B :

1. Les deux entités s'entendent sur deux nombres **p** et **g** tel que :

p > g >=2 et **g** premier avec **p**. Ainsi, **(p-1)/2** est premier avec **p**.

Les deux nombre **p** et **g** sont publics et peuvent être communs à un groupe d'entités.

Le choix de **g** et **p** peut avoir un impact significatif sur la sécurité de ce protocole. Plus important, **p** doit être grand et **g** doit être n'importe quelle racine primitive modulo **p** ;

2. L'entité A choisit un nombre secret aléatoire **x** dans [2, p-2], et envoi à l'entité B le résultat de calcul $\mathbf{X=g^x \bmod p}$;

3. L'entité B choisit un nombre secret aléatoire **y** dans [2, p-2], et envoi à l'entité A le résultat de calcul $\mathbf{Y=g^y \bmod p}$;

4. L'entité A calcule la clé secrète $\mathbf{Ka=Y^x \bmod p}$,
et l'entité B calcule la clé secrète $\mathbf{Kb=X^y \bmod p}$;

Les valeurs **Ka** et **Kb** sont toutes les deux égales à $\mathbf{g^{(xy)} \bmod p}$. Personne ne peut en écoutant la communication calculer cette valeur, car l'intercepteur ne connait que les valeurs **p**, **g**, **X**, et **Y**.

Pour calculer $\mathbf{g^{(xy)} \bmod p}$ il faut résoudre les logarithmes discrets **x=ln (X) / ln (g)**, et **y=ln (Y) / ln (g)**, qui est très complexe à réaliser dans des délais raisonnables.

L'utilisation de ce protocole d'échange de clés dans les réseaux de capteurs sans fil a de nombreux avantages primordiaux :

1. Les nœuds pourraient s'échanger leur clé secrète sur un canal non sécurisé ;

2. Il permet d'assurer la sécurité rétroactive, c'est-à-dire qu'en cas de la divulgation de la clé secrète du système seul l'échange en cours est affecté, mais pas les échanges en aval. Autrement dit, il offre une meilleure résistance contre la compromission de nœuds ;

3. Il permet la scalabilité.

Malheureusement, l'application directe de ce protocole est irréalisable pour les réseaux de capteurs sans fil. Car, il exige en contre partie trop de ressources additionnelles en termes de calcul, de mémoire et d'énergie. En d'autres termes, les opérations arithmétiques effectuées dans ce protocole sont complexes, en particulier car elles se font dans des corps finis GF(p) sur des nombres de plusieurs centaines de bits.

Comme nous l'avons expliqué au chapitre précédent, la contrainte énergétique due à l'autonomie des nœuds capteurs, le faible coût de production de ces derniers, les contraintes liées aux environnements de déploiements impliquent l'utilisation d'une puissance de calcul réduite. Ainsi, les applications pour lesquelles ils sont déployés sont notamment de plus en plus gourmandes en capacités de calculs. Sachant que la faiblesse de la puissance de calcul est aussi préjudiciable pour le temps de réponse du réseau.

Ces paramètres entraînent ainsi un développement de protocoles dédiés aux réseaux de capteurs sans fil très contraints. L'énergie et le microprocesseur sont des ressources typiques à

prendre en compte lors de développement des protocoles de sécurité pour les réseaux de capteurs sans fil.

Dans ce contexte, nous avons opté pour une implémentation de ce protocole par matériel.

III. présentation de notre protocole matériel d’échange de clés:

Dans cette section nous donnons la description détaillée de notre protocole matériel d’échange de clés.

III.1. Modèle du réseau et d’attaquant :

Notre protocole se base sur les hypothèses suivantes :

Nous considérons une architecture distribuée de grande échelle, où les nœuds sont déployés d’une façon aléatoire et peuvent être mobiles ou statiques. Les nœuds capteurs peuvent être homogènes ou hétérogènes.

Nous supposons que l’attaquant peut être passif (écoute passive des transmissions, etc.) ou actif (brouillage, injection des données, compromission de capteurs, etc.) durant le fonctionnement du réseau.

Ainsi, si un nœud légitime est compromis, nous supposons que toutes les informations stockées sont accessibles par l’attaquant.

Nous supposons aussi que les informations précédemment transmises via le réseau ne sont plus intéressantes pour l’adversaire. C'est-à-dire, l’adversaire s’intéresse aux données actuellement transmises.

III.2. Description détaillée de notre protocole :

Notre protocole matériel d’échange de clés basé sur Diffie-Hellman consiste en un circuit électronique qui décharge totalement le microprocesseur d’un nœud capteur des calculs concernant les clés cryptographiques, en réduisant ainsi la latence résultante et l’énergie consommée.

Les particularités du nouveau protocole :

1. La réduction du nombre de bits des paramètres publics (p, g, X, et Y), et également ceux des paramètres privés (x, et y) ;
2. L'augmentation de la fréquence d'échange des clés entres les nœuds capteurs.

Sachant que la faille de sécurité induite par la réduction du nombre de bits est comblée par l'augmentation de la fréquence de changement des clés, de telle sorte que l'attaquant ne puisse pas avoir le temps de casser la clé.

Tous les paramètres de ce protocole seront codés sur **6 bits.** Nous choisissons la valeur deux (2) pour la racine primitive **g** (g = 2). Car, rien n'empêche de prendre **g** la plus petite valeur qui convient. De plus, le choix (g = 2) allège le coût de l'exponentiation modulaire qui est l'opération de base et la plus coûteuse de ce protocole ; du fait que les nœuds capteurs sont trop contrains en ressource de calcul.

Comme évoqué précédemment le choix des deux nombres **p** et **g** peut avoir un impact substantiel sur la sécurité de protocole. Pour cela nous avons choisi le modulo **p** égale à **59** (p = 59). Cette valeur est le plus grand nombre premier codé sur 6 bits satisfaisant la condition **p** et **(p-1)/2** sont premiers entre eux.

En d'autres termes, notre protocole se résume dans les étapes suivantes :

Deux nœuds A et B veulent établir une clé cryptographique secrète commune :

1. Le nœud A choisit un nombre secret aléatoire **x** dans [2, 57], et envoi au nœud B le résultat de calcul **X=2**x mod 59**.
2. Le nœud B choisit un nombre secret aléatoire **y** dans [2, 57], et envoi au nœud A le résultat de calcul **Y=2**y mod 59**.
3. Le module du nœud A calcule la clé secrète **Ka=Y**x mod 59**, et le module du nœud B calcule la clé secrète **Kb=X**y mod 59** ;

Génération des paramètres secrets x et y :

Pour la génération des nombres secrets **x** et **y**, nous avons opté pour le générateur de nombres pseudo aléatoires Blum Blum Shub (BBS) baptisé d'après ses inventeurs [10]. Ce dernier est appelé aussi générateur à résidu quadratique et il est considéré comme le générateur le plus simple et le plus efficace pour la génération des clés cryptographiques.

Le générateur fonctionne comme suit :

1. Choisir deux grands nombres premiers **p** et **q** soient congrus à **3** modulo **4**. Le produit de ces nombres est **n = p* q** qui est un entier de blum ;
2. Choisir un autre entier aléatoire **x** qui soit premier par rapport à **n** et calculer :
   $\mathbf{x_0 = x^2 \bmod n}$; ce nombre est le germe de générateur ;
   La génération de la suite aléatoire se fait comme suit:
   Le $\mathbf{i^{eme}}$ bit pseudo aléatoire est le bit le moins significatif de **xi** où :
3. $\mathbf{x_i = (x_{i-1})^2 \bmod n}$.

Algorithme.3.1. générateur de nombre pseudo aléatoire BBS.

La sécurité de ce générateur est basée sur les mathématiques sous-jacentes à la factorisation de nombre n. Toutefois, à moins qu'un adversaire puisse factoriser n, il ne pourra jamais prédire la sortie de générateur.

De même, pour ce générateur nous utilisons aussi des nombres de petite taille. Les nombres **p** et **q** seront sur **4 bits** ; et donc le nombre **n** sera sur **8 bits**. Pour la chaine aléatoire générée nous utilisons **6 bits**. Cette dernière sera régénérée régulièrement.

Comme nous l'avons remarqué, l'opération principale de notre protocole est l'exponentiation modulaire. Cette dernière est réalisée par une série de multiplication modulaire.

Pour réaliser ces opérations arithmétiques, nous avons considéré les algorithmes de la multiplication et exponentiation modulaire du Montgomery:

L'algorithme de Montgomery pour la multiplication modulaire :

La multiplication du Montgomery [11] est une méthode efficace pour réaliser la multiplication modulaire. Nous présentons ici une version simple cette multiplication modulaire.

L'algorithme de Montgomery calcule:

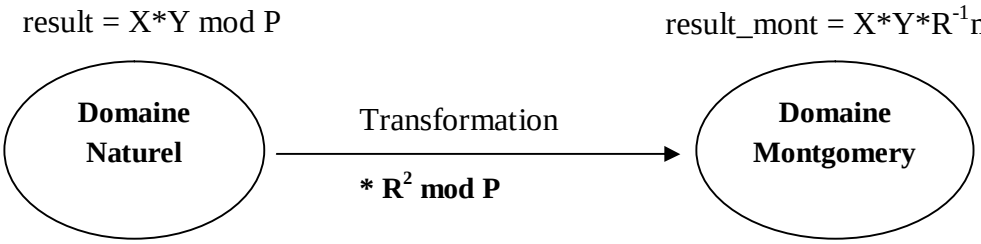
$X*Y*R^{-1} \bmod P$, où X, Y, et P sont sur n bits, et $R=2^n$;

Au lieu de calculer X*Y mod P, où X, Y, et P sont sur n bits ;

Notons que les paramètres X, Y, et P sont des nombres naturels non signés.

Autrement dit, avant d'exécuter la multiplication modulaire du Montgomery, les paramètres X et Y doivent être convertis en domaine du Montgomery

Les éléments de Montgomery seront calculés comme suit :



X ⟶ X_mont = montgomeryMult (X, R^2 mod P)

= X*R^2*R^{-1} mod P

= X*R mod P

Y ⟶ Y_mont = montgomeryMult (Y, R^2 mod P)

= Y*R^2*R^{-1} mod P

= Y*R mod P

result ⟶ result_mont = montgomeryMult (X_mont, Y_mont)

= X*R * Y*R *R^{-1} mod P

= X*Y*R mod P

Où :

X, Y, et result sont des éléments de domaine naturel ;

X_mont, Y_mont, et result_mont sont des éléments de domaine du Montgomery.

R^2 mod P est la constante du Montgomery.

Pour convertir le résultat trouvé dans le domaine du Montgomery, en domaine naturel, nous faisons une multiplication Montgomery de résultat par un. En d'autres termes :

result = montgomeryMult (result_mont, 1)

= X*Y*R*1*R^{-1}mod P

result = X*Y mod P.

Notons que la base utilisée pour la multiplication et l'exponentiation de Montgomery est la base binaire.

Le principe de fonctionnement de l'algorithme de multiplication modulaire du Montgomery est le suivant :

Entrées : $X = (x_{n-1}, \ldots x_1, x_0)_2$; $Y = (y_{n-1}, \ldots y_1, y_0)_2$; $P = (p_{n-1} \ldots p_1, p_0)_2$;

Sorties : $Z = X*Y*R^{-1} \bmod P$

1. Z = 0 ;
2. For i in 0 to n-1 loop
3. Z:= Z + xi * Y;
4. Z:= $Z+Z_0$ * P;
5. Z:=Z div 2;
6. end for;
7. If Z >= P then Z:= Z-P;
8. end.

Algorithme.3.2. la multiplication modulaire du Montgomery.

Comme évoqué au dessus, pour multiplier deux nombre il faut effectuer quatre multiplications de Montgomery. Dans notre protocole la dernière multiplication sera omise. C'est-à-dire nous éliminons la multiplication qui permet de convertir le résultat final de Montgomery en domaine naturel. Car l'algorithme de l'exponentiation modulaire du Montgomery nécessite aussi que les paramètres de l'exponentiation soient dans le domaine du Montgomery.

4. L'algorithme de Montgomery pour l'exponentiation modulaire [12]:

L'algorithme d'exponentiation modulaire du Montgomery se déroule comme suit :

Entrées : $X = (x_{n-1}, \ldots x_1, x_0)_2$; $E = (e_{n-1}, \ldots e_1, e_0)_2$; $P = (p_{n-1} \ldots p_1, p_0)_2$;

Sorties: result = X**E mod P

1. result_mont := montgomeryMult (1, R2 mod P);
2. X_mont := montgomeryMult (X, R2 mod P);
3. For i in 0 to n-1 loop
4. X_mont := montgomeryMult (X_mont, X_mont);
5. If E(i) = 1 then
6. result_mont := montgomeryMult (result_mont, X_mont);
7. end for;
8. result := montgomeryMult (result_mont, 1);
9. end.

Algorithme.3.3. l'exponentiation modulaire du Montgomery.

Conclusion :

Etant donnée les différents domaines sensibles auxquels peuvent s'appliquer les réseaux de capteurs sans fil, la sécurisation des applications développées pour ces derniers devient un élément essentiel et indispensable.

En fait, il serait inutile d’intégrer un algorithme cryptographique dans un réseau de capteurs sans fil si leur mécanisme d’échange de clés correspondant n’est pas fiable. Ce dernier est crucial pour pouvoir offrir un niveau de sécurité appréciable.

Dans ce contexte nous avons proposé un nouveau type de protocole d’échange clés qui permet d’établir une communication sécurisée entre les différents nœuds capteurs.

Le chapitre suivant sera consacré à l’implémentation matérielle de ce protocole.

4

Implémentation matérielle

Introduction :

Nous avons décri dans le chapitre précédant notre protocole d'échange de clés. Dans ce chapitre nous allons présenter l'architecture générale de notre protocole et les trois modules qui la composent. Le premier permet de générer les paramètres secrets x et y. Le deuxième et le troisième effectuent la multiplication et l'exponentiation modulaire respectivement. Notre protocole matériel est implémenté avec le langage de description du matériel VHDL.

Nous commençons ainsi par une brève description du langage VHDL, ainsi que l'environnement de développement Active-HDL. Par la suite, nous présentons l'architecture générale du protocole et ses différents modules. Nous présentons ensuite quelques scenarios de simulation.

I. Le langage VHDL :

VHDL (VHSIC Hardware Description Language) [13] est un langage de description pour les circuits numériques. Il a été développé dans le cadre du projet VHSIC (Very high speed integrated circuits) commandité par le département de la défense américaine DoD au début des années quatre-vingts. C'est un standard IEEE depuis 1987 largement utilisé en Europe. Il autorise plusieurs méthodologies de conception (comportemental, flot de données, structurel).

Il est indépendant de la technologie utilisée FPGA, CPLD, ASIC, etc., et permet d'aller d'un niveau d'abstraction très élevée par une description algorithmique jusqu'à un niveau proche du matériel, où l'on décrit le système par un ensemble de porte logique et d'interconnexion. Entre les deux se trouve le niveau RTL (Register Transfer Level) qui permet de définir le système par une architecture de type machine de Moore ou Mealy. Cette abstraction permet d'ailleurs de simuler sur ordinateur avant de programmer le moindre circuit.

II. le logiciel Active-HDL :

Active-HDL de la compagnie Aldec est un environnement intégré destiné au développement de systèmes numériques décrit par un langage de description matérielle (comme VHDL, Verilog et SystemC), par schémas, par diagrammes d'états ou avec une combinaison des trois. Il intègre plusieurs outils de description de designs, des compilateurs pour plusieurs langages de description matérielle, un simulateur, des outils de débogage, et des outils de profilage et de vérification. Le logiciel intègre, de plus, des outils de synthèse et d'implémentation d'autres compagnies, permettant ainsi de travailler avec différentes technologies dans un environnement unifié [14].

III. Implémentation matérielle de notre protocole d'échange de clés:

III.1. Architecture générale du protocole :

Notre circuit est composé de trois modules. Un module pour générer les paramètres privés x et y (par le générateur BBS), un autre module pour calculer les paramètres publics X et Y, et le dernier module est utilisé pour calculer la clé secrète.

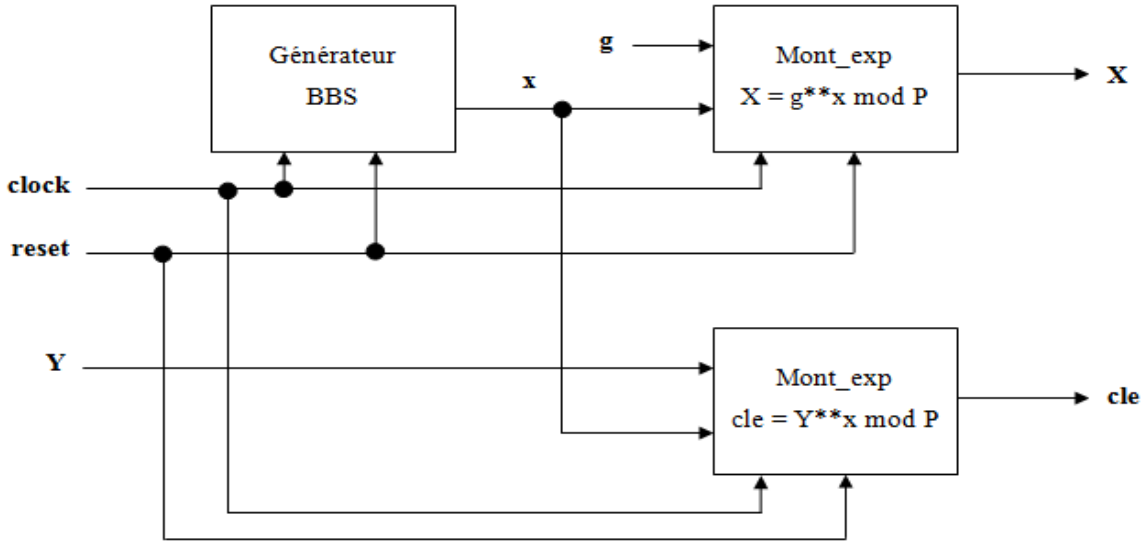


Figure.4.1. architecture générale du protocole.

III.2. Le module BBS :

Ce module est responsable de la génération des paramètres privés x et y de protocole. Il repose sur l'algorithme.3.1.présenté dans le chapitre précédent.

La figure.4.2. donne le schéma et les signaux d'interface du générateur. Comme évoqué au chapitre précédent, la taille de la chaine aléatoire générée est 6 bits.

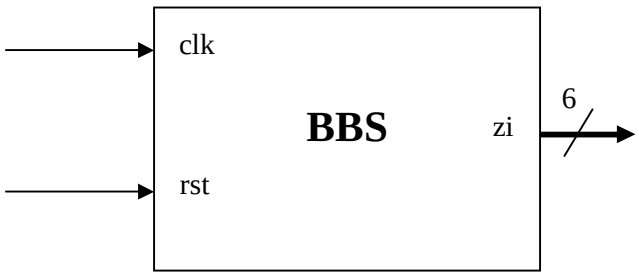


Figure.4.2. Module du générateur des paramètres privés x et y.

L'organigramme ASM (Algorithmic State Machine) correspond à ce générateur est le suivant :

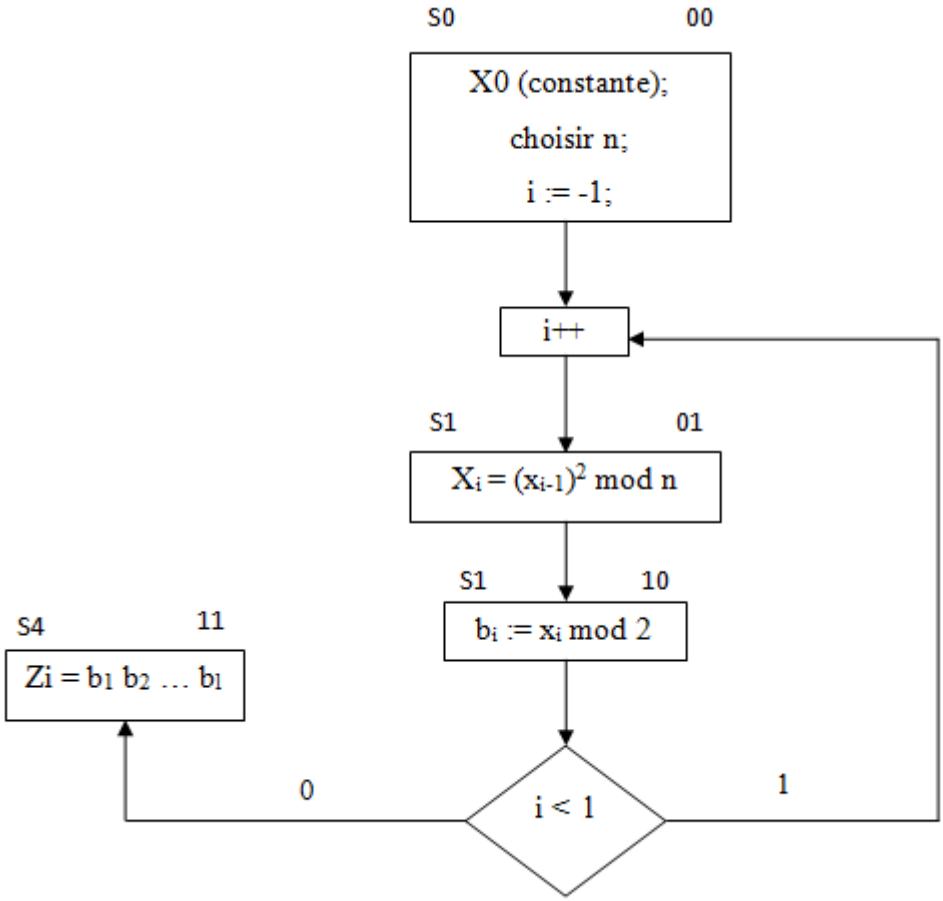


Figure.4.3. Bloc ASM du générateur BBS.

III.2.1. Simulation de module du générateur BBS :

La figure.4.4. illustre la simulation de module du générateur de nombres pseudo aléatoire. Pour la simulation fonctionnelle, nous avons crée une instance de ce générateur ayant les paramètres suivant :

N = p*q = 7*19 = 133 ; x = 100 ; $x0 = 100^2 \bmod 133 = 25$;

$x1 = 25^2 \bmod 133 = 93$; $x2 = 93^2 \bmod 133 = 4$; $x3 = 4^2 \bmod 133 = 16$; $x4 = 16^2 \bmod 133 = 123$; $x5 = 123^2 \bmod 133 = 100$; $x6 = 100^2 \bmod 133 = 25$;

La séquence aléatoire générée est : $100101_2 = 37_{10} = 25_H$

A 0 ns le signal RESET est mis à 1 pour initialiser la chaîne. A 100 ns, une chaine pseudo aléatoire est générée (suivant l'exemple au dessus).

Cette chaîne générée sera une entrée pour le module de l'exponentiation modulaire.

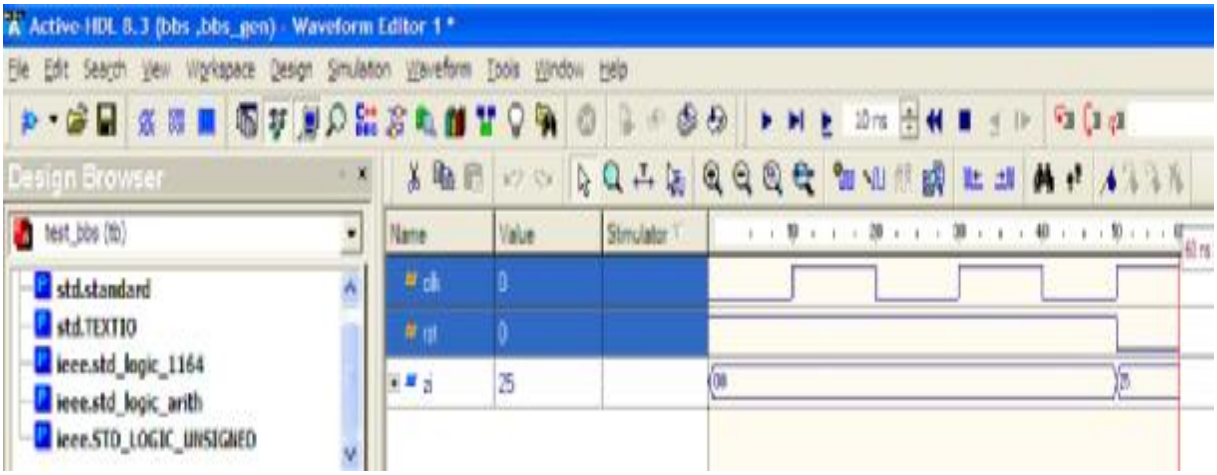


Figure.4.4. Simulation de générateur pseudo aléatoire BBS.

III.3. Le module du la multiplication modulaire :

Ce module repose sur l'algorithme.3.2. présenté dans le chapitre précédent. Il réalise la multiplication modulaire de deux nombres X et Y de domaine du Montgomery. Le résultat de module sera dans le domaine de Montgomery. Comme expliqué au chapitre 3, nous n'avons besoin de converti le résultat dans le domaine naturel, dû fait que ce module sera intégré dans le module responsable de l'exponentiation modulaire du Montgomery.

La figure.4.5. donne le schéma et les signaux d'interface du multiplieur modulaire. Les entrées et la sortie du module seront sur 6 bits.

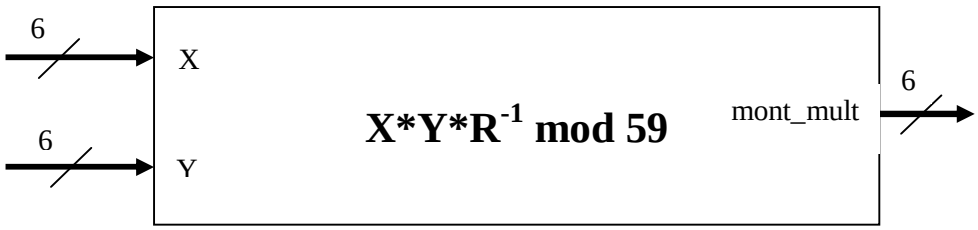


Figure.4.5. Module de la multiplication modulaire de Montgomery.

L'organigramme ASM (Algorithmic State Machine) correspond au module de la multiplication modulaire du Montgomery est le suivant :

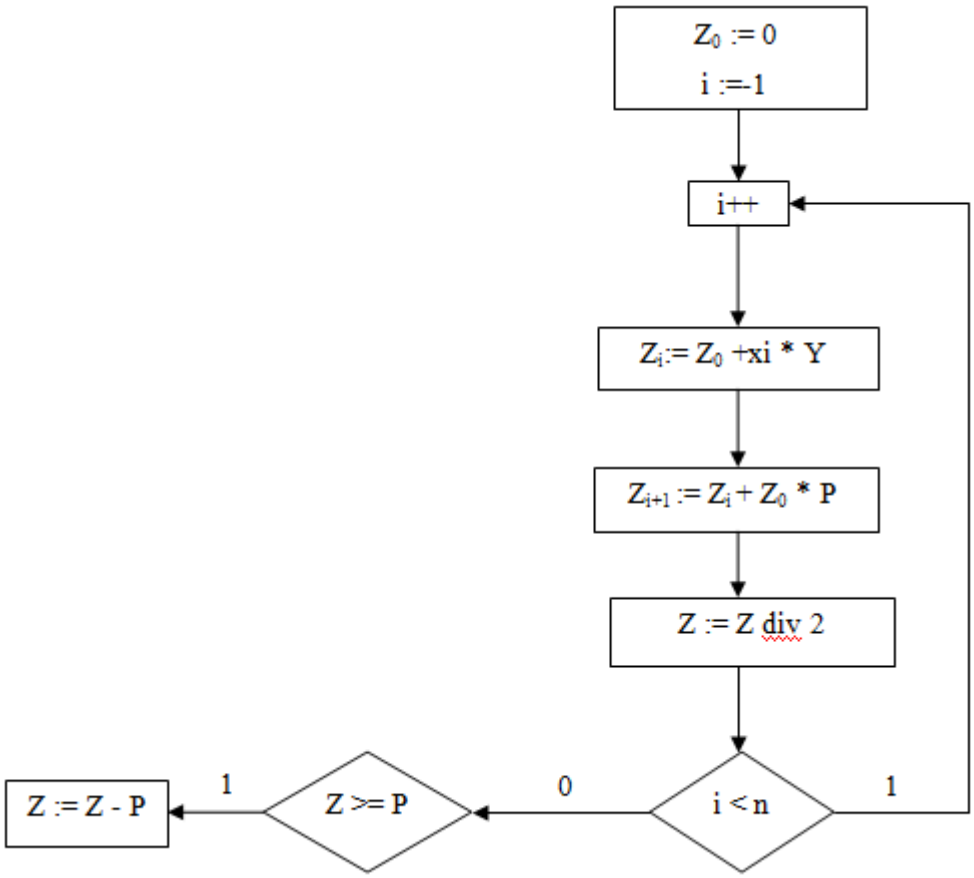


Figure.4.6. Bloc ASM de multiplier modulaire.

III.3.1. Simulation de module du la multiplication modulaire:

La figure.4.7. illustre la simulation de fonctionnement de module du la multiplication modulaire.

Pour instancier le multiplieur, nous considérons les paramètres de domaine du Montgomery suivant :

$X = 02_H$; $Y = 12_H$;

Le résultat est : 13_H ;

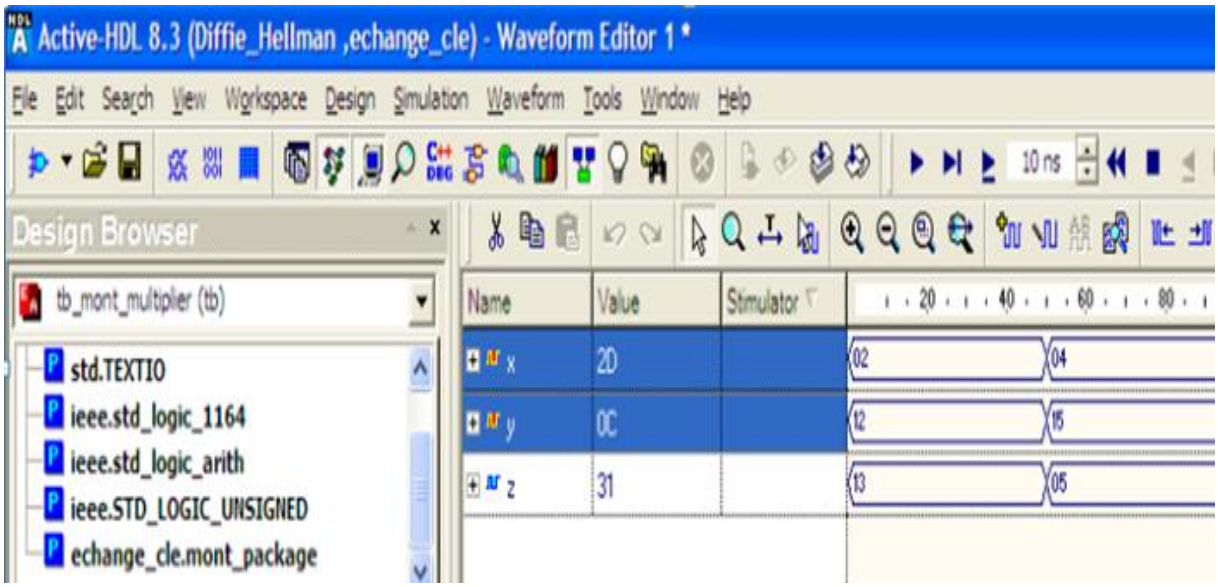


Figure.4.7. Simulation de module du la multiplication modulaire.

III.4. Le module du l'exponentiation modulaire :

Ce module repose sur l'algorithme.3.3. présenté au chapitre précédent. D'après notre protocole, l'opération de base est l'exponentiation modulaire. Ici les paramètres d'entrées seront dans le domaine de Montgomery, et le résultat final sera dans le domaine naturel.

La figure.4.8. donne le schéma et les signaux d'interface du module de l'exponentiation modulaire. Les entrées et la sortie du module seront sur 6 bits.

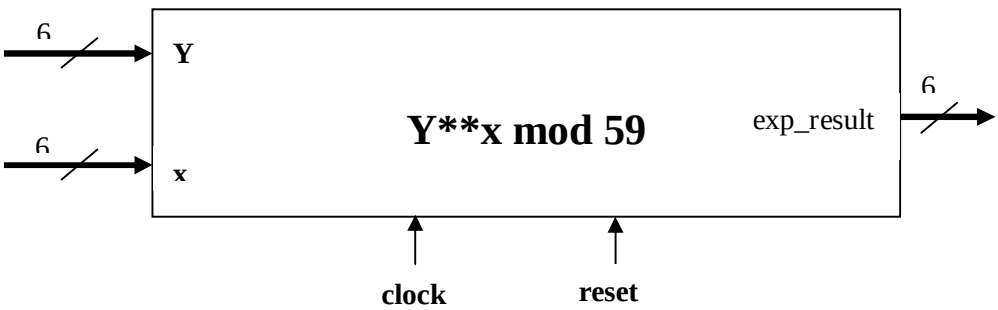


Figure.4.8. Module du l'exponentiation modulaire de Montgomery.

L'organigramme ASM (Algorithmic State Machine) correspond au module de l'exponentiation modulaire du Montgomery est le suivant :

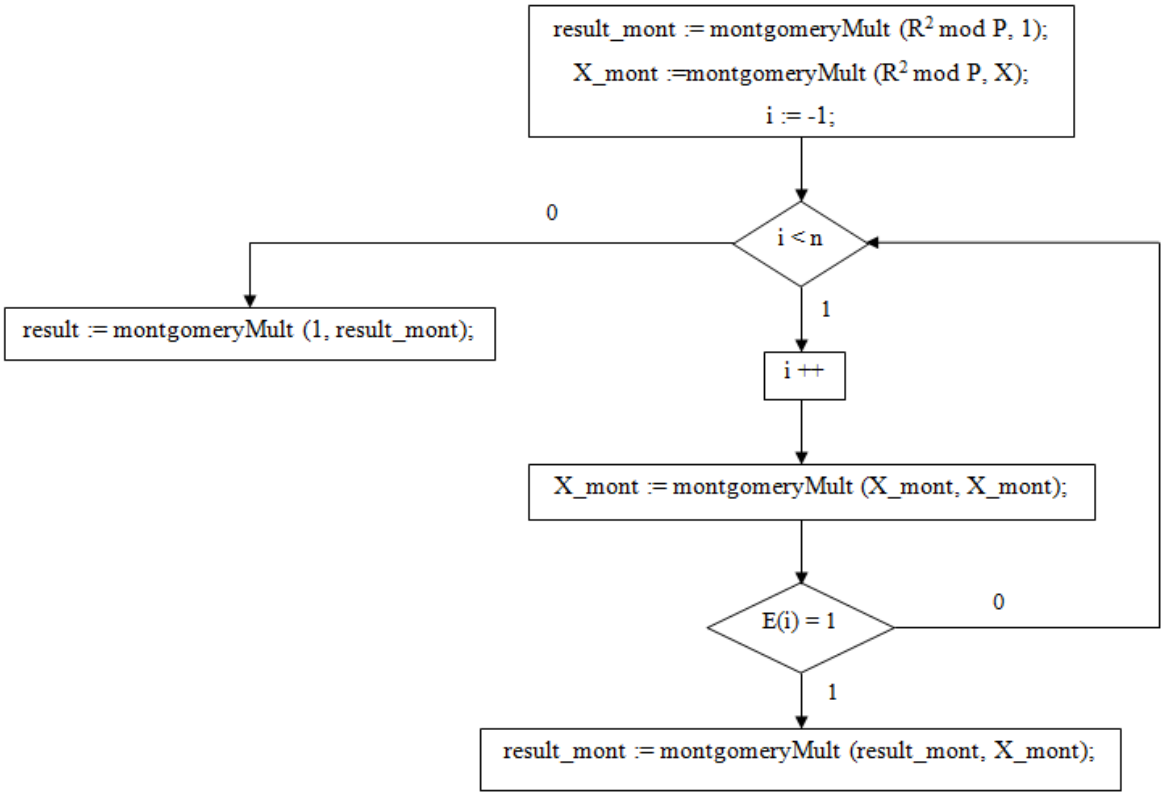


Figure.4.9. Bloc ASM du l'exponentiation modulaire du Montgomery.

L'architecture générale de module exponentiation modulaire est la suivante :

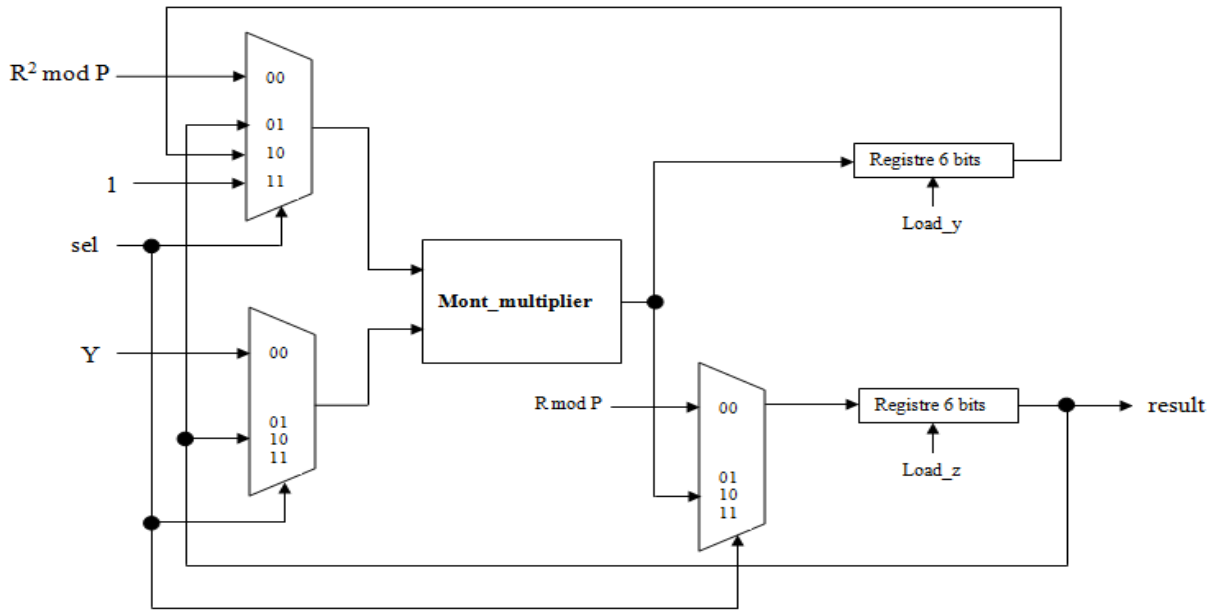


Figure.4.10. l'architecture générale du module de l'exponentiation modulaire de Montgomery.

III.4.3. Simulation de module du l'exponentiation modulaire:

La figure.4.11. illustre la simulation de module de base de notre protocole qui est l'exponentiation modulaire. Notons que la multiplication et l'exponentiation modulaire se font de bit le moins significatif au bit le plus significatif.

Pour la simulation fonctionnelle, nous prenons les paramètres suivant :

Y = 02H ; x = 04H ;

Le résultat de Y^x mod P est : $z = 10_H = 16_{10}$

A 0 ns le signal RESET est mis à 1 pour initialiser le résultat. Apres 12 impulsion d'horloge, le résultat de l'exponentiation est calculé (resultat est dans le domaine de naturel).

Figure.4.11. Simulation de module du l'exponentiation modulaire.

Conclusion :

Dans ce chapitre, nous avons présenté l'architecture générale de notre protocole d'échange de clés, ainsi que ses différents modules. Ce protocole sera un module additionnel ajouté au nœud capteur si l'application l'exige.

Conclusion générale :

Les réseaux de capteurs sans fil représentent actuellement un nouveau sujet de recherche innovant, mais avec des contraintes exclusives et certains défis à relever. Parmi les problèmes posés à l'heure actuelle dans ce type de réseaux est le problème de la sécurité, auquel une solution dédiée doit être apportée.

Ce mémoire a pour objectif d'apporter une solution adéquate au problème d'échange de clés dans les réseaux de capteurs sans fil.

Dans un premier temps, nous avons étudié l'opportunité de la sécurité et le besoin d'établir une communication sécurisée dans la plupart des applications de ces réseaux. Diverses vulnérabilités ont été étudiées et pour y faire face, la technique de cryptographie s'est avérée une solution clé.

Ensuite, nous avons présenté les différentes contraintes des réseaux de capteurs sans fil qui empêchent l'utilisation directe des solutions de sécurité habituelles des réseaux classiques, et la nécessité de développer des protocoles dédiés.

De cette étude, résulte notre contribution qui consiste en une proposition d'un protocole matériel d'échange de clés.

Concevoir un protocole efficace d'échange de clés pour les réseaux de capteurs sans fil reste encore un domaine de recherche ouvert. Il serait donc possible comme perspective de notre travail, de combiner notre protocole avec l'algorithme de cryptage DES, qui sera aussi une solution matérielle.

Bibliographie :

[1] I. Akyildiz, W. Su, E. Cayirci, Y. Sankarasubramaniam. « A survey on sensor Networks », *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, Georgia Institute of Technology, Atlanta, USA. Août, 2002.

[2] RYO SUGIHARA and RAJESH K. GUPTA « Programming Models for Sensor Networks: A Survey » University of California, San Diego; ACM Journal Name, Vol. V, No. N, Month 20YY, Pages 1–27.

[3] Asad Madni, Harish Ramamurthy, Rajit Gadh, « Wireless Industrial Monitoring and Control using a Smart Sensor Platform », Sensors Journal, IEEE, Page(s): 611 – 618, California University, Los Angeles, May 2007.

[4] RYO SUGIHARA and RAJESH K. GUPTA « Programming Models for Sensor Networks: A Survey » University of California, San Diego; ACM Journal Name, Vol. V, No. N, Month 20YY, Pages 1–27.

[5] Jaydip Sen « A Survey on Wireless Sensor Network Security» International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, August 2009, pages 55-78.

[6] Al-Sakib Khan Pathan et. al.: «Secrity in Wireless Sensor Networks: Issues and Challenges» in Feb., 2006, ICACT2006, ISBN 89-5519-129-4 pp(1043-1048).

[7] Vishal Rathod 1, Mrudang Mehta, «Security in Wireless Sensor Network: A survey», ganpat university journal of engineering & technology, vol.-1, issue-1, jan-jun-2011.

[8] CHEE-YEE CHONG, MEMBER, IEEE AND SRIKANTA P. KUMAR, SENIOR MEMBER, IEEE «Sensor Networks: Evolution, Opportunities, and Challenges», PROCEEDINGS OF THE IEEE, VOL. 91, NO. 8, AUGUST 2003.

[9] Chaudhari H.C. and Kadam L.U. «Wireless Sensor Networks: Security,Attacks and Challenges», International Journal of Networking, Volume 1, Issue 1, 2011, pp-04-16.

[10] Bruce Scheneier, «Cryptographie appliquée », deuxième édition, Algorithmes, Protocoles et codes sources en C.

[11] E. Savas, A. F. Tenca, and ç. K. Koç, «A Scalable and Unified Multiplier Architecture for Finite Fields *GF*(*p*) and *GF*(2*m*) », Electrical & Computer Engineering, Oregon State University, Corvallis, Oregon 97331

[12] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, «HANDBOOK of APPLIED CRYPTOGRAPHY »

[13] R.Airiau, J.M.Bergé, V.Olive et J.Rouillard- CENT « *VHDL: Du langage à la modélisation*»

[14] «Guide pratique – Active–HDL 8.3 sp1 update 3 (v. 0.8, 16 janvier 2012)