Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté desSciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option: *Réseaux et systèmes distribuées (R.S.D)*

Thème

Evaluation de la librairie de sécurité TinySec dans les réseaux de capteurs sans fil : Application à la détection d'événements critiques

Réalisé par :

- **BELHABRI Amine**
- **HADJI Imane**

Présenté le 16 Juin 2016 devant le jury composé de MM.

- *Mr BENAMAR Abdelkrim* *(Président)*
- *Mme DIDI Fedwa* *(Examinateur)*
- *Mr BEKARA Chakib* *(Examinateur)*
- *Mme LABRRAOUI Nabila* *(Encadreur)*

Année universitaire: 2015-2016.

Remerciements

Avec un grand plaisir, nous remercions ***ALLAH*** qui nous a aidé et nous a donné la patience, le courage et la force d'achever ce travail.

Nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire.

Ces remerciements vont tout d'abord au corps professoral et administratif du département d'informatique de l'université ***ABOU BAKR BELKAID*** de Tlemcen pour la richesse et la qualité de leurs enseignants qui déploient de grands efforts pour assurer à leur étudiants une formation actualisée.

Ensuite nous tenons à remercier notre encadreur « ***Mme LABRAOUI Nabila*** » pour ses remarques constructives qui nous ont été très utiles dans la construction du projet et pour l'esprit de recherche auquel elle nous a initiés.

Nous tenons aussi à lui exprimer nos remerciements et notre profonde reconnaissance

Pour sa disponibilité, sa gentillesse, ses conseils et son aimable assistance.

Pour l'orientation, la confiance, la patience qui ont constitué un apport considérable sans lequel ce travail n'aurait pas pu être mené au bon port. Qu'elle trouve dans ce travail un hommage vivant à sa haute personnalité.

Nous tenons aussi à remercier les membres du jury« Mme **DIDI Fedwa** , Mr **BENAMAR Abdelkrim** ,Mr **BEKARA Chakib** » qui ont accepté d'examiner notre mémoire.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches amis «Nabawiya et Ahlem » qui nous ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire

Merci à tous et à toutes.

Dédicace

Nous dédions ce modeste travail :

A la plus belle créature que Dieu a créée sur terre…

A cette source de tendresse, de patience et de générosité…

A nos mères **HADJOU BELAID Souad**

A nos frères Youcef et Abdelrahmane, nos sœurs Salsabile,khawla , Ibtisam et raniya.

A mon **Binôme BELHABRI Amine**, et tous mes amis.

Nous remercions également tous nos professeurs et surtout notre encadreur Mme **LABRAOUI Nabila.**

En un mot à tous les gens qui ont contribué à nos réussites de près ou de loin

BELHABRI Amine

HADJI Imane

Tables de matière

Liste des figures

INTRODUCTION GENERALE

Les progrès réalisés ces dernières décennies dans les domaines de la microélectronique, de la micromécanique, et des technologies de communication sans fil, ont permis de produire à un coûtraisonnable des composants de quelques millimètres cubes de volume. De ce fait, un nouveau domaine de recherche s'est créé pour offrir des solutions économiquement intéressantes et facilement déployables à la surveillance à distance et au traitement des données dans les environnements complexes et distribués : *les réseaux de capteurs sans fil (RCSF)*. Les réseaux de capteurs sans fil sont constituésde nœuds appelés micro-capteurs, Un grand nombre de ces dispositifs sont déployés dans la nature afin de créer un réseau de capteurs à des fins aussi bien de collecter et transmettre des données environnementales vers un ou plusieurs points, d'une manière autonome. Ces derniers, intègrent : une unité de captage chargée de capter des grandeurs physiques (chaleur, humidité, vibrations) et de les transformer en grandeurs numériques, une unité de traitement informatique et de stockage de données et un module de transmission sans fil. Ces réseaux ont un intérêtparticulier pour les applications militaires, environnementales, domotiques, médicales, et bien sûrles applications liées à la surveillance des infrastructures critiques.

En effet, la sécurité est une nécessité pour la majorité des applications qui utilisent les RCSFs, notamment si les nœuds capteurs sont déployés dans des endroits peu sûrs, tels que leschamps de bataille, les lieux stratégiques (aéroports, bâtiments critiques, etc.). Ces nœuds capteurs qui opèrent dans des lieux difficiles d'accès, sans protection et sans possibilité de rechargement de batterie, peuvent être soumis à des actions perturbatrices et malveillantes susceptibles de compromettre l'essence même d'un RCSF. C'est pourquoi, il est primordial de pouvoir leur assurer un niveau de sécurité acceptable. Compte tenu de leurs spécificités contraignantes, la sécurité dans ce type de réseaux relève d'un véritable challenge.

Comme l'objectif premier des nœuds d'un RCSF est de rassembler des donnés de surveillance et de les transmettre à un lieu de décision, cette opération doit se faire sans interférences malicieuses et avec un niveau de sécurité approprié .

Dans notre projet de fin d'études, nous avons étudié et évalué la bibliothèque « TinySec »installée sur le système d'exploitation TinyOS qui est conçue spécialement pour ce type de réseau et qui est écrite dans un langage spécifique optimisé pour les capteurs « le langage NesC».

Afin d'aborder tous les aspects ayant trait au fonctionnement de ces réseaux, notre mémoire est organisé comme suit :

Chapitre I : Généralités sur les réseaux de capteurs sans fil, dans ce chapitre on va présenter les réseaux des capteurs.

Chapitre II : La sécurité dans les réseaux de capteurs sans fil.
Chapitre III :Dans ce chapitre, on présente l'environnement du travail, le choix du simulateur et ses objectifs ainsi que la description de l'interface graphique TinyViz et les différentes étapes pour la réalisation de l'application.

Ce travail est terminé par une conclusion générale et une bibliographie.

CHAPITRE I :

Généralités sur les réseaux de capteurs sans fil

1. Introduction

Les réseaux de capteurs sans fil (RCSFs ou WSNs : Wireless sensor networks en anglais) sont devenus de plus en plus omniprésents. Les milieux scientifiques et industriels leurs prêtent d'en plus d'attention du fait de leurs riches applications dans les domaines : médical, commercial et militaire. Selon MIT's Technology Review, il s'agit de l'une des dix nouvelles technologies qui vont influer sur notre manière de vivre et de travailler. Les RCSFs sont des réseaux de nœuds sans fil dédiés à des applications spécifiques. Ils sont considérés comme un type particulier des réseaux Ad-hoc, dans lesquels les nœuds sont des capteurs intelligents (smart sensors). Les RCSFs sont composés d'un nombre potentiellement très grand (plusieurs milliers) de capteurs qui se communiquent selon un modèle de communication « sources multiples - destination unique », déployés dans la zone à couvrir.

Chaque capteur est capable d'effectuer d'une manière autonome trois tâches complémentaires : mesure d'une valeur physique, traitement de ses mesures, et communication par voie hertzienne. [2]

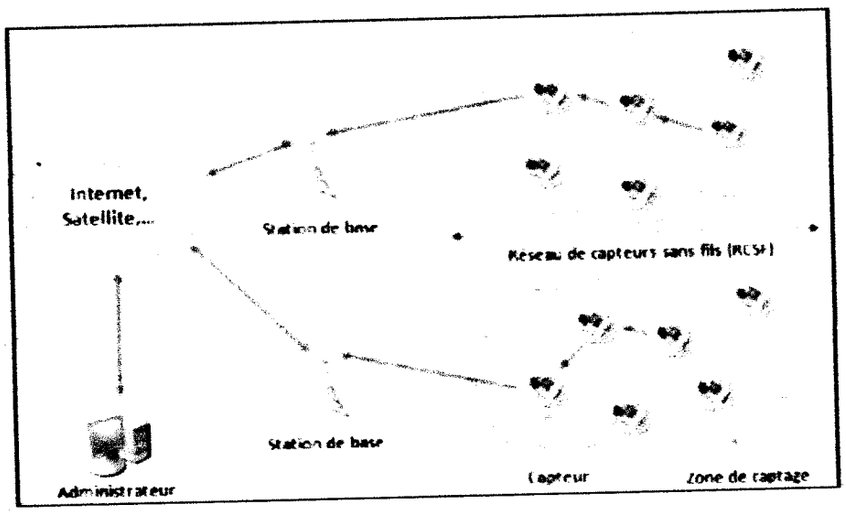


FIGURE 1. 1 : UN RESEAU DE CAPTEURS SANS FIL

2. *Représentation* de capteurs dans les RCSF

Les capteurs ou les motes en anglais sont définis comme étant de petits dispositifsqui ont des objets limités en termes de bande passante, de puissance de calcul, de mémoire disponible et d'énergie embarquée. La position de ces nœuds n'est pas obligatoirement prédéterminée. Ils sont dispersés aléatoirement à travers une zone géographique, appelée champ de captage, qui définit le terrain d'intérêt pour le phénomène capté. Les données captées sont acheminées grâce à un routage multi-sauts à un nœud considéré comme un "point de collecte" ou "collecteur", appelé nœud puits (sink, ou station de base). Ce dernier peut être connecté à l'utilisateur du réseau via Internet ou un satellite. Ainsi, l'usager peut adresser des requêtes aux autres nœuds du réseau, précisant le type de données requises et récoltant les données environnementales captées par le biais du nœud puits[2] .

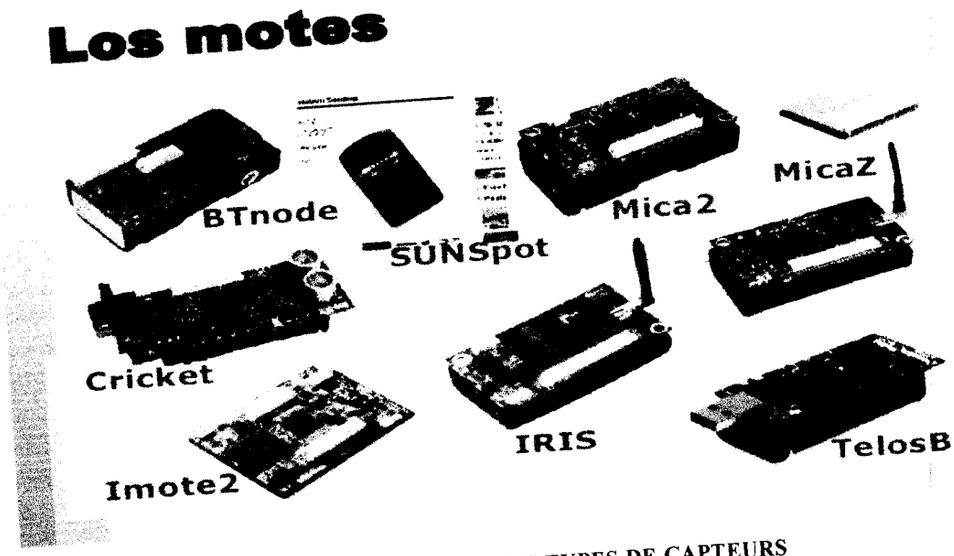


FIGURE 1. 2 : QUELQUES TYPES DE CAPTEURS

3. Applications des réseaux de capteurs sans fil

Le champ d'applications des réseaux de capteurs est de plus en plus élargi grâce aux évolutions techniques que connaissent les domaines de l'électronique et des télécommunications. En effet, les applications des réseaux de capteurs peuvent être militaires, médicales, environnementales, commerciales, etc... [3].

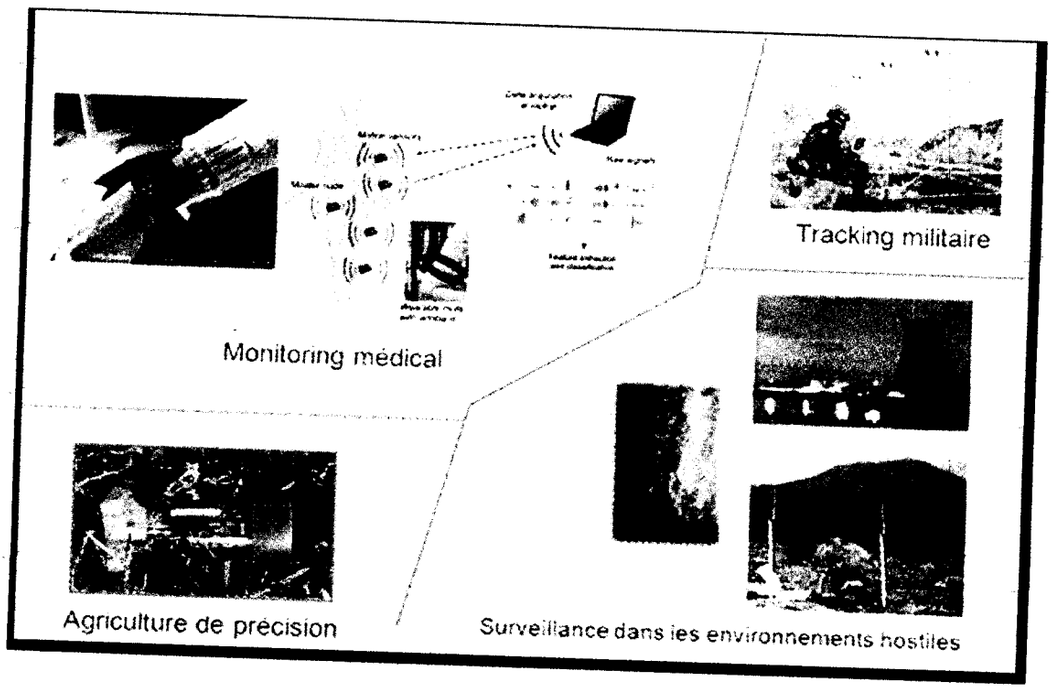


FIGURE 1. 3 : LES APPLICATIONS DES RESEAUX DE CAPTEURS SANS FIL

3.1 Applications militaires

Les RCSFs ont été initialement conçus pour des projets d'application militaire. En effet, le faible coût, la tolérance aux pannes, l'organisation autonome, et le déploiement rapide, représentent des caractéristiques très attirantes pour ce domaine d'application. Par exemple, les RCSFs, peuvent être déployés afin de surveiller les activités des forces ennemies, ou d'analyser le terrain avant d'y envoyer des troupes *(détection d'agentschimiques, biologiques ou de radiations)*[3].

3.2 Applications à la sécurité

La sécurité représente un domaine d'application très important pour les RCSFs. En effet, des capteurs peuvent êtres dans les bâtiments afin de détecter les altérations dans leur structure. En outre, Un réseau de capteurs peut constituer un système d'alarme distribué, qui servira à détecter les intrusions sur un large secteur. Parmi les autres applications de sécurité, on peut

citer la surveillance de voies ferrées, pour prévenir des accidents avec des animaux et des êtres humains, ou la détection de fuites d'eau dans les barrages afin d'éviter les dégâts éventuels[3].

3.3 Applications médicales

La surveillance des fonctions vitales de l'être humain peut être effectuée avec des micros-capteurs avalés ou implantés sous la peau des malades. Des capteurs peuvent être implantés à l'intérieur du corps humain pour traiter certains types de maladies *(telque la détection de cancers)* ou pour collecter des informations physiologiques *(tel que lasurveillance du niveau de glucose)*[3].

3.4 Applications environnementales

Les réseaux de capteurs sans fil peuvent être utilisés afin de surveiller des phénomènes environnementaux. Ainsi, ils sont déployés dans les forêts afin de détecter et de signaler un éventuel début d'incendie. Les capteurs peuvent aussi être semés avec les graines, afin de contrôler l'arrosage des plantes. Dans le domaine industriel, les capteurs sont généralement utilisés afin de détecter des fuites de produits toxiques, ou pour la surveillance des paramètres critiques tels que la température d'un réacteur nucléaire [3].

3.5 Applications de santé

La surveillance des fonctions vitales de l'être humain peut être effectuée avec des micros-capteurs avalés ou implantés sous la peau des malades. Des capteurs peuvent être implantés à l'intérieur du corps humain pour traiter certains types de maladies *(telque ladétection de cancers)* ou pour collecter des informations physiologiques *(tel que lasurveillance du niveau de glucose)* [3].

4. Architecture d'un nœud-capteur sans fil

L'architecture comprend quatre éléments de base pour le fonctionnement du capteur: une unité de captage, une unité de traitement, une unité d'émission/réception et une unité de puissance.

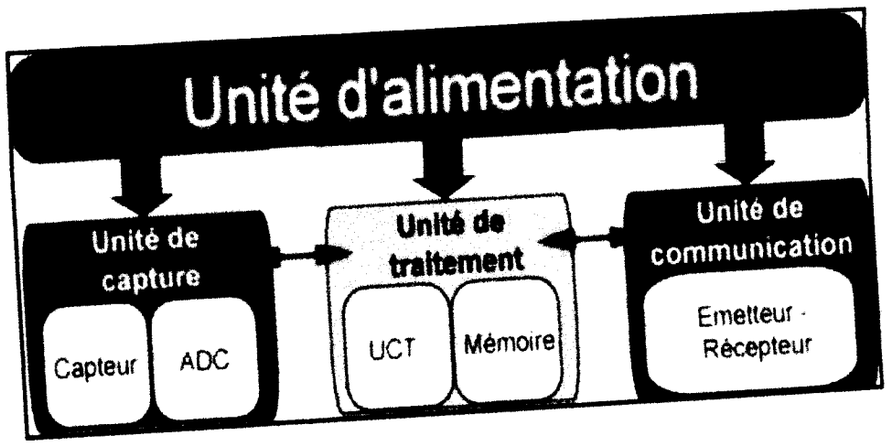


FIGURE 1. 4 : ARCHITECTURE D'UN NŒUD CAPTEUR

4.1 Unité d'acquisition de données

C'est le composant principal d'un nœud sans fil qui contient le ou les capteurs embarqués sur le nœud. Habituellement, un convertisseur analogique-numérique (CAN) convertit les signaux provenant des capteurs (signaux analogiques) en signaux interprétables par l'Unité de Traitement (signaux numériques) [4].

4.2 Unité de traitement des données

L'unité de traitement est composée de deux interfaces : une interface pour l'unité d'acquisition et une interface pour l'unité de transmission. Cette unité est également composée d'un processeur et d'un système d'exploitation spécifique. Elle acquiert les informations en provenance de l'unité d'acquisition et les envoie à l'unité de transmission[5].

4.3 Unité de transmission

Cette unité est responsable de toutes les émissions et réceptions de données via un support de communication radio[6].

4.3Unité de contrôle d'énergie

Batterie : Un micro-capteur est muni d'une ressource énergétique (généralement une batterie de type AAA) pour alimenter tous ses composants[5].

5. Les facteurs influençant l'architecture des RCSF

Les principaux facteurs et contraintes influençant l'architecture des réseaux de capteurs peuvent être résumés comme suit :

5.1 La tolérance de fautes : Certain nœuds peuvent générer des erreurs ou ne plus fonctionner à cause d'un manque d'énergie, un problème physique ou une interférence. Ces problèmes n'affectent pas le reste du réseau, c'est le principe de la tolérance de fautes [7].

5.2 L'échelle : Le nombre de nœuds déployés pour un projet peut atteindre le million. Un nombre aussi important de nœuds engendre beaucoup de transmissions inter nodales et nécessite que le puits "sink " soit équipé de beaucoup de mémoire pour stocker les informations reçues[7].

5.3 Les coûts de production : Souvent, les réseaux de capteurs sont composés d'un très grand nombre de nœuds. Le prix d'un nœud est critique afin de pouvoir concurrencer un réseau de surveillance traditionnel. Actuellement un nœud ne coûte souvent pas beaucoup plus que 1$ [7].

5.4 L'environnement : Les capteurs sont souvent déployés en masse dans des endroits tels que des champs de bataille au-delà des lignes ennemies, à l'intérieur de grandes machines, au fond d'un océan, dans des champs biologiquement ou chimiquement souillés [7].

5.5 L'agrégation de données : Diffuser de grandes quantités de données sur le réseau peut facilement encombrer ce dernier. L'agrégation intelligente des données captées et l'élimination de l'information non désirée et redondante, peut être une solution pour l'utilisation efficace de ressources et d'énergie et l'évitement de congestion [3].

5.6 La topologie de réseau: Le déploiement d'un grand nombre de nœuds nécessite une maintenance de la topologie. Cette maintenance consiste en trois phases : Déploiement, Post-déploiement (les capteurs peuvent bouger, ne plus fonctionner, ...), Redéploiement de nœuds additionnels[7].

5.7 Les contraintes matérielles: La principale contrainte matérielle est la tailledu capteur. Les autres contraintes sont que la consommation d'énergie doit être moindre pour que le réseau survive le plus longtemps possible, qu'il s'adapte aux différents environnements (fortes chaleurs, eau..), qu'il soit autonome et très résistant [7].

5.8 Les médias de transmission: Dans un réseau de capteurs, les nœuds sont reliés par une architecture sans-fil. Pour permettre des opérations sur ces réseaux dans le monde entier, le média de transmission doit être normé [7].

5.9 La consommation d'énergie: Un capteur, de par sa taille, est limité en énergie (< 1.2V). Dans la plupart des cas le remplacement de la batterie est impossible. Ce qui veut dire que la durée de vie d'un capteur dépend grandement de la durée de vie de la batterie [7].

6. La consommation d'énergie d'un nœud-capteur

Il y'a plusieurs formes de dissipation d'énergie :

6.1 Formes de dissipation d'énergie

Les nœuds capteurs sont alimentés principalement par des batteries. Ils doivent donc fonctionner avec un bilan énergétique frugal. En outre, ils doivent le plus souvent avoir une durée de vie de l'ordre de plusieurs mois, voire de quelques années, puisque le remplacement des batteries n'est pas une option envisageable pour des réseaux avec des milliers de nœuds. Afin de concevoir des solutions efficaces en énergie, il est extrêmement important de faire d'abord une analyse des différents facteurs provoquant la dissipation de l'énergie d'un nœud-capteur [3] et pour cela cette dissipation d'énergie se fait selon plusieurs modes [8].

- **La radio :** opère dans quatre modes de fonctionnement : émission, réception ,«idle », et sommeil. Une observation importante dans le cas de la plupart des radios est que le mode « idle » induit une consommation d'énergie significative, presque égale à la consommation en mode réception. Ainsi, il est plus judicieux d'éteindre complètement la radio plutôt que de passer en mode « idle » quand l'on n'a ni à émettre ni à recevoirde données. Un autre facteur déterminant est que, le passage de la radio d'un mode à un autre engendre une dissipation d'énergie importante due à l'activité des circuits électroniques. Par exemple, quand la radio passe du mode sommeil au mode émission pour envoyer un paquet, une importante quantité d'énergie est consommée pour le démarrage de l'émetteur lui-même. Un autre point important est que les données des constructeurs sous-estiment assez régulièrement ces différentes consommations, en particulier concernant la consommation dans le mode « idle » [8].
- **Le MCU *« Unité du microcontrôleur ou Micro Controller Unit »*:** Généralement les MCUs possèdent divers modes de fonctionnement : actif, «idle », et sommeil, à des fins de gestion d'énergie. Chaque mode est caractérisé par une quantité différente de consommation d'énergie. Par exemple, le MSP430[4] Microcontrôleur injecté dans des capteurs de type TmoteSky, de TelosB consomme 3mW en mode actif, 98 µW dans le mode«idle» et seulement 15 µW dans le mode sommeil. Toutefois, la transition entre les

modes de fonctionnement implique un surplus d'énergie et de latence. Ainsi, les niveaux de consommation d'énergie des différents modes, les coûts de transition entre les modes et encore le temps passé par le MCU dans chaque mode ont une incidence importante sur la consommation totale d'énergie d'un nœud-capteur [8].

- **Le détecteur ou le capteur proprement dit** :il y a plusieurs sources de consommation d'énergie par le module de détection, notamment l'échantillonnage et la conversion des signaux physiques en signaux électriques, le conditionnement des signaux et la conversion analogique-numérique. Étant donné la diversité des capteurs, il n'y a pas de valeurs typiques de l'énergie consommée. En revanche, les capteurs passifs (température, sismiques, ...) consomment le plus souvent peu d'énergie par rapport aux autres composants du nœud-capteur. Notons, les capteurs actifs tels que les sonars, les capteurs d'images, etc. peuvent consommer beaucoup d'énergie [8].

6.2 Les Sources de surconsommation d'énergie

Nous appelons surconsommation d'énergie toute consommation inutile que l'on peut éviter afin de conserver l'énergie d'un nœud-capteur [8]. Les causes majeures de la perte d'énergie sont :

- **Les collisions** :elles sont la première source de perte d'énergie. Quand deux trames sont émises en même temps et se heurtent, elles deviennent inexploitables et doivent être abandonnées. Ce que nécessite de les retransmettre de nouveau. Les protocoles MAC essayent à leur manière d'éviter les collisions. Les collisions concernent plutôt les protocoles MAC avec contention [8].
- **L'écoute à vide (idlelistening)** :un nœud dans l'état « idle » est prêt à recevoir un paquet, mais il n'est pas actuellement en train de recevoir quoi que ce soit. Ceci est coûteux et inutile dans le cas des réseaux à faible charge de trafic. Plusieurs types de radios présentent un coût en énergie significatif pour le mode idle. Eteindre la radio est une solution, mais le coût de la transition entre les modes consomme également de l'énergie, la fréquence de cette transition doit alors rester raisonnable [8].
- **L'écoute abusive (overhearing)** :cette situation se présente quand un nœud reçoit des paquets qui ne lui sont pas destinés. Le coût de l'écoute abusive peut être un facteur dominant de la perte d'énergie quand la charge de trafic est élevée et la densité des nœuds est grande, particulièrement dans les réseaux mostly-on [8].

- **L'overmitting :**un nœud envoie des données et le nœud destinataire n'est pas prêt à les recevoir [8].
- **L'overhead des paquets de contrôle :**l'envoi, la réception, et l'écoute des paquets de contrôle consomment de l'énergie. Comme les paquets de contrôle ne transportent pas directement des données, ils réduisent également le débit utile effectif [8].

7. Les mécanismes de conservation de l'énergie

C'est la transmission de données qui se révèle extrêmement consommatrice par rapport aux tâches du noeud-capteur. Cette caractéristique conjuguée à l'objectif de maximisation de la durée de vie du réseau a suscité de nombreux travaux de recherche [9]. Nousintroduisons dans ce paragraphe certains mécanismes de base :

7.1 Mode d'économie d'énergie

Ce mode est possible quelle que soit la couche MAC adoptée. Cela consiste à éteindre le module de communication dès que possible. Par exemple, des protocoles MAC fondés sur la méthode TDMA offrent une solution implicite puisqu'un nœud n'échange des messages que dans les intervalles de temps qui lui sont attribués. Il peut alors garder sa radio éteinte durant les autres slots. Il faut toutefois veiller à ce que le gain d'énergie obtenu en mettant en veille le module radio ne soit pas inférieur au surcoût engendré par le redémarrage de ce module[8].

7.2Traitement local

L'idée de cette technique est que la source peut se censurer. Ainsi une programmation événementielle semble bien adaptée aux réseaux de capteurs. Seuls les changements significatifs de l'environnement devraient provoquer un envoi de paquets le réseau. Dans le même contexte, une grande collaboration est attendue entre les capteurs d'une même région en raison de leur forte densité et dans la mesure où les observations ne varient presque pas entre des voisins très proches. Ainsi les données pourront être confrontées localement et agrégées au sein d'un seul et unique message. Cette stratégie de traitement local permet de réduire sensiblement le trafic [8].

7.3 Organisation des échanges

Ce procédé revient à limiter les problèmes de retransmission dus aux collisions. La solution extrême consiste à utiliser la technique d'accès au medium TDMA. Les collisions

sont ainsi fortement réduites. Cette solution présente l'inconvénient d'être peu flexible et de demander une synchronisation fine des capteurs. Des solutions intermédiaires ont vu le jour, par exemple S-MAC (Sensor MAC) [10].

7.4 Limitation des accusés de réception

L'acquittement systématique est mal adapté à des réseaux denses : il provoque une surcharge du réseau et donc des collisions et des interférences avec les données utiles échangées dans le réseau. Les acquittements par « piggy-backing » seront à privilégier [8].

8. Conclusion

Dans ce chapitre, nous avons présenté les réseaux de capteurs, en parlant sur l'architecture, composants, fonctionnement, domaines d'applications, ainsi les facteurs qui influençant la consommation d'énergie et ses mécanismes pour la conserver. Dans le chapitre suivant, nous introduirons en détail la sécurité des réseaux de capteurs sans fil.

Chapitre II :

La sécurité dans les réseaux de capteurs sans fil

1. Introduction

Comme nous l'avons déjà mentionné la sécurisation des réseaux de capteurs est à la source, aujourd'hui, de beaucoup de défis scientifiques et techniques. Cependant, les nœuds sont exposés à différents types d'attaques qui peuvent carrément endommager le bon fonctionnement du réseau. Ces attaques exploitent essentiellement l'incertitude du canal de communication et le déploiement aléatoire des nœuds capteurs dans des zones difficiles à surveiller. Garantir la sécurité de ce type de réseau est une tâche difficile surtout quand les nœuds ont des capacités matérielles limitées.

Dans ce chapitre, nous présentons premièrement un aperçu sur les problèmes de sécurité dans les réseaux de capteurs sans fil. Ensuite, nous déterminons les objectifs de la sécurité et les attaques avec les différents mécanismes pour atteindre une meilleure sécurité pour notre réseau.

2. Les problèmes de la sécurité dans les RCSF

Les principaux problèmes de sécurité proviennent de trois facteurs : la limitation de ressources, la communication sans fil et le couplage étroit avec l'environnement [11]

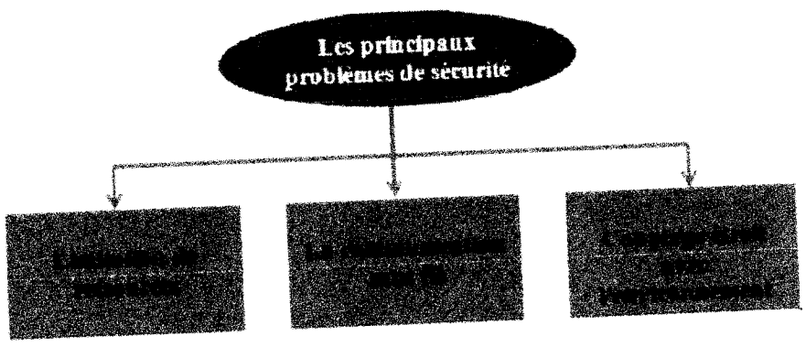


FIGURE 2. 1: CLASSIFICATION DES PROBLEMES DE SECURITE

2.1Limitation de ressources

L'énergie est peut-être la contrainte la plus forte aux capacités d'un nœud capteur. Dans la plupart du temps, l'information transmise est redondante vus que les capteurs sont

généralement géographiquement Co-localisés. La plupart de cette énergie peut donc être économisée par agrégation de données [11].

2.2La communication sans fil multi-sauts

La communication multi-sauts est donc indispensable pour la diffusion des données dans un RCSF. Cela introduit de nombreuses failles de sécurité à deux niveaux différents : attaque de la construction et maintenance des routes, et attaque des données utiles par injection, la modification ou la suppression de paquets. En outre, la communication sans fil introduit d'autres vulnérabilités à la couche liaison en ouvrant la porte à des attaques de brouillage et de style déni de service par épuisement des batteries [11].

2.3 Couplage étroit avec l'environnement

La plupart des applications des RCSFs exigent un déploiement étroit des nœuds à l'intérieur ou à proximité des phénomènes à surveiller. Par conséquent un adversaire bien équipé peut extraire des informations cryptographiques des nœuds capteurs. Comme la mission d'un RCSF est généralement sans surveillance, le potentiel d'attaquer des nœuds, de récupérer leur contenu ou d'injecter des données erronées est important. Du fait que les réseaux de capteurs soient contrôlés à distance, il est également très difficile de savoir si le nœud capteur a été physiquement manipulé ou reprogrammé [11].

3. Les besoins de sécurité typique aux RCSF

Pour déterminer des objectifs de sécurité, il faudra connaitre ce qu'on doit protéger

3.1 Confidentialité Des Données

La confidentialité des données est la question la plus importante dans la sécurité de réseau. L'approche standard pour sécuriser le transfert des données est de crypter les données avec une clef secrète connue par l'émetteur et le récepteur [12].

3.2 Intégrité des données

Un nœud intrus (adversaire) peut modifier les données transférées. Par exemple, un nœud malveillant peut ajouter quelques fragments ou manœuvrer les données dans un paquet.Ce nouveau paquet peut alors être envoyé au récepteur original.

La perte ou les dommages de données peut même se produire sans présence d'un nœud malveillant dû à l'environnement dur de communication. Ainsi, l'intégrité des données

s'assure qu'aucune donnée reçue n'a été changée en transit[12].

3.3 Fraîcheur de données

Officieusement, la fraîcheur de données suggère que les données soient récentes, et elles s'assurent qu'aucun vieux message n'a été rejoué. Cette condition est particulièrement importante quand il y a des stratégies de partager clef utilisée dans la conception. Des clefs typiquement partagées doivent être changées avec le temps. Cependant, cela prend du temps pour de nouvelles clefs partagées d'être propagées au réseau entier. Dans ce cas-ci, il est facile pour l'adversaire d'employer une attaque de rejouer. Pour résoudre ce problème un compteur relatif au temps différent, peut être ajouté dans le paquet pour assurer la fraîcheur de données[12].

3.4 Authentification

Elle permet de coopérer au sein des RCSF sans risque, en contrôlant et en identifiant les participants. Elle apparaît comme la pierre angulaire d'un réseau de capteur sans fil sécurisé. En effet, on ne peut assurer une confidentialité et une intégrité des messages échangés si, dès le départ, on n'est pas sûr de communiquer avec le bon nœud.

Si l'authentification est mal gérée, un attaquant peut se joindre au réseau et injecter des messages erronés. L'utilisation de Code d'Authentification de Message (CAM), ou MAC en anglais (Message Authentification Code), permet d'assurer à la fois l'authentification de l'origine et l'intégrité du message [4].

4.Les attaques

Une attaque est un ensemble de techniques informatiques, visant à causer des dommageset des risques a un réseau. Pour cela, nous présentons les attaques les plus connues dans les RCSF.

4.1 Ecoute du réseau (eavesdropping)

Du fait que les transmissions se font en diffusion par les ondes radio, aucun contrôle d'accès au réseau n'est possible, ce qui est d'autant plus vrai que le réseau peut être déployé dans un environnement ouvert accessible à tout le monde. Il est donc très facile d'intercepter

des données échangées sur un réseau de capteurs et d'accéder à leur contenu si aucun service de confidentialité n'est prévu[4].

4.2 Attaque physique (tampering)

Comme les RCSFs sont très souvent déployés dans des zones sans aucune protection, ils sont très exposés aux attaques physiques qui peuvent être considérées sous différents points de vue. L'un est lié au matériel qui n'est pas qualifié d'inviolable. Dans ces conditions, une attaque aura pour but de récupérer du matériel cryptographique comme les clés utilisées pour le chiffrement. Un autre objectif serait de reprogrammer le capteur pour perturber le réseau et l'application en provoquant volontairement un comportement anormal du nœud. La seconde attaque physique consisterait simplement à supprimer le capteur du réseau en le détruisant[4].

4.3 Attaque de l'identité multiples (sybil attack)

Dans cette attaque le nœud malveillant peut créer un grand nombre d'identités afin de gagner de l'influence sur les autres nœuds du réseau. Chaque identité (ID) peut être générée aléatoirement ou être dupliquée *(recopiée)* d'une identité légitime qui existe déjà. Ainsi, le nœud attaquant peut profiter de ces multiples identités pour être sélectionné comme chef de groupe *(clusterhead)*, ou pour créer des chemins de routage pour son propre intérêt. Les techniques d'authentification et de chiffrement peuvent empêcher un étranger de lancer une attaque Sybille sur le réseau de capteur [4].

4.4 Attaque du trou noir (blackhole ou sinkhole)

Un nœud falsifie les informations de routage pour forcer le passage des données par lui-même. Sa seule mission est ensuite de ne rien transférer, créant ainsi une sorte de puits ou trou noir dans le réseau. L'intrus (nœud malveillant, qui s'introduit illégitimement) se place sur un endroit stratégique de routage dans le réseau et supprime tous les messages qu'il devrait retransmettre, causant la suspension du service de routage du réseau dans les routes qui passent par le nœud intrus[4].

4.5 Attaque du trou gris (grey hole)

Une variante de l'attaque précédente est appelée trou gris, dans laquelle seuls certains types de paquets sont ignorés par le nœud malicieux. Par exemple, les paquets de données ne sont pas retransmis alors que les paquets de routage le sont [4].

4.6 Brouillage radio (jamming)

L'intrus inonde avec du bruit les fréquences radio utilisées par le réseau de manière à empêcher les transmissions et/ou les réceptions de messages. Ce type d'attaque peut affecter

tout ou une partie du réseau selon la portée radio de l'intrus. Dans ce cas-là, l'intention est de provoquer un déni de service [4].

4.7 Attaque du trou de ver (wormhole)

L'intrus capture un message et, en utilisant un canal de faible latence, le retransmet vers un lieu distant dans le réseau. Le canal ainsi créé fait transiter un message à un endroit du RCSF auquel il ne devrait normalement pas arriver. Cette attaque a une influence notable sur le routage dans le réseau [4].

4.8Rejeu, Délai et Altération de Données

L'intrus répète, retarde ou altère le contenu des messages en transit. Les messages peuvent contenir des données de perception prélevées et des données de configuration ou de routage. Ces types d'attaques visent entre autres à créer des boucles, attirer à lui ou éloigner du trafic, augmenter ou diminuer le nombre de routes, générer de fausses erreurs, partitionner le réseau, et augmenter la latence de distribution des données [4].

4.9Attaque de l'inondation de "HELLO"

De nombreux protocoles de routage utilisent des paquets "HELLO" pour découvrir les nœuds voisins et ainsi établir une topologie du réseau. La plus simple attaque pour un attaquant consiste à envoyer un flot de tels messages pour inonder le réseau et empêcher d'autres messages d'être échangés [4].

5.Les mécanismes de sécurité dans les RCSF

Plusieurs mécanismes, sont mis en place afin de répondre à la question de la sécurité dans les RCSF. Nous présentons dans ce qui suit quelques solutions de sécurité les plus répondues et les protocoles de sécurité s aux RCSF.

5 .1 le cryptage des données

Le système cryptographique basé sur des clés sécurisées. Ces dernières permettent de chiffrer et d'authentifier les messages envoyés entre les nœuds capteurs. La sélection d'une méthode de chiffrement adaptée aux réseaux de capteurs est une tache vitale et délicate. Ainsi, les algorithmes cryptographiques doivent respecter la limitation en ressources des nœuds capteurs en n'exigeant pas une grande puissance de calcul et une capacité de stockage élevée. De plus, ils doivent être moins énergivores en énergie.

5.1.1 Le chiffrement

Le chiffrement des données permet d'empêcher l'écoute des données transitant dans un réseau sans fil et de garantir la confidentialité des données. Pour cela, il utilise des clés. On distingue de classes de chiffrement : symétrique ou asymétrique [8].

Le chiffrement symétrique : Le principe de chiffrement symétrique se base sur le partage d'une même clé K de chiffrement entre deux entités pour chiffrer et dé- chiffrer les données en utilisant un algorithme de chiffrement symétrique [8].

Le chiffrement asymétrique : Deux clés différentes sont générées par le récepteur : une clé publique diffusée à tous les nœuds servant au chiffrement de données qu'ils vont émettre au récepteur, et, une clé privée maintenue secrète chez le récepteur servant pour le déchiffrement de ces données lorsque ce dernier les reçoit. Le point fondamental sur lequel repose la sécurité du chiffrement asymétrique est l'impossibilité de déduire la clé privé à partir de la clé publique [8].

5.1.2 Génération de clés

Une solution proposée dans consiste à utiliser une clé de génération. A chaque période ou génération, la station de base envoie une nouvelle clé à l'ensemble du réseau. Cette clé sert de certificat à chacun des nœuds, pour prouver son appartenance au réseau. Si un nœud non identifié tente de rentrer dans le réseau et qu'il ne possède pas cette clé de génération, il ne pourra être accepté en son sein. Cette technique permet aussi de limiter les attaques de substitution d'un capteur et de sa reprogrammation pour être réinjecté dans le réseau [8].

5.1.3La distribution des clés

La distribution des clés est l'une des phases cruciales dans le processus de gestion des clés. Cette phase consiste à distribuer les clés cryptographiques d'une manière efficace et sécurisée sur tous les nœuds légitimes appartenant au réseau. En effet, il existe trois modèles essentiels pour la distribution des clés dans les RCSFs [3] :

La distribution à base d'une clé par réseau (Network keying) :C'est un simple modèle dedistribution qui consiste à utiliser une clé unique partagée par tous les nœuds du réseau. L'idée de base est de pré-charger les nœuds, avant le déploiement par une seule clé.

La distribution à base d'une clé par paire de nœuds (Pair-wise keying): Dans cette solution, une clé sera partagée uniquement entre une paire de nœuds capteurs. Ainsi, chaque nœud est pré-chargé avec N-1 clés secrètes. Chacune de ces clés est connue seulement par ce nœud et un des N-1 autres nœuds *(N étant le nombre de nœuds dans leréseau)*. Ce modèle de distribution permet une résilience parfaite car la compromission d'un nœud n'affecte pas la sécurité des autres nœuds.

La distribution à base de groupe (Group keying): Ce modèle combine les caractéristiques des deux précédents modèles. Au sein d'un groupe de nœuds *(qui forment un cluster)*, les communications sont effectuées à l'aide d'une seule clé partagée *(distribution à base declé par réseau)*.

5.2L'authentification

L'authentification est l'un des mécanismes de base pour la sécurité dans les réseaux de capteurs sans fil. Souvent construite autour d'un système cryptographique, l'authentification permetd'assurer au nœud récepteur que les données ou les paquets de contrôle *(les informations deroutage, de localisation et de gestion clés)* proviennent bien de la bonne source. Traditionnellement, les protocoles d'authentification dédiés au RCSFs utilisent un mécanisme basé sur la cryptographie symétrique. Ce dernier est nommé MAC *(message authentication code)*. Le code d'authentification de message MAC fait partie des fonctions de hachage à clésymétrique. Ainsi, l'émetteur génère une empreinte ou un code d'authentification en utilisant la clé symétrique partagée avec le nœud récepteur. Ce dernier calcule à son tour le code MAC avec cette même clé et le compare au code qu'il a reçu. S'ils sont bien identiques, alors la source est authentique[3].

5.2.1 Protocoles d'authentification

Plusieurs protocoles ont été proposés afin d'assurer l'authentification dans les réseaux de capteurs sans fil[3].

1. **Le protocole SPIN *(Security Protocols for Sensor Networks)*:** le protocole SPIN est un ensemble de mécanismes de sécurité qui assurent l'authentification des messages, l'intégrité et la confidentialité des données. SPIN est particulièrement adapté aux réseaux de capteurs hiérarchiques. Ce protocole propose deux mécanismes d'authentification nommés SNEP et µTESLA. Le premier mécanisme permet l'authentification des

communications unicast *(entre une paire de nœuds)*, tandis que µTESLA assure l'authentification des communications par diffusion *(entre un groupe de nœuds)*.

2. **Le protocole RPT *(Regular and Predictable Times)*** :afin de remédier aux problèmes de SPIN, un nouveau protocole d'authentification. Les auteurs ont proposé de modifier le protocole µTESLA afin qu'il tolère les authentifications urgentes et infréquentées. Ainsi, le nouveau protocole *(nommé RPT)* authentifie dans un temps prédictible l'origine des messages reçus.
3. **Le protocole LEA *(Low Entropy Authentication)*:**Ce dernier utilise un nouveau mécanisme d'authentification basé sur la cryptographie asymétrique.Afin d'être authentifié, le nœud émetteur signe les données à transmettre avec sa clé privée en produisant une signature digitale. Celle–ci sera envoyée avec les données au nœud récepteur. Cedernier déchiffre la signature avec la clé publique, et la compare avec les données reçues. Dans le cas où elles sont identiques, la signature est validée, et l'émetteur sera authentifié comme nœud légitime. Cependant, LEA peut être très consommateur en espace de stockage, étant donné que la taille de la signature est proportionnelle à la taille des messages envoyés. De plus, LEA exige une clé publique unique pour chaque message envoyé, ce qui impose au récepteur de stocker un grand nombre de clés publiques.
4. **Le protocole TinySec *(Tiny security):***TinySec a était proposé afin d'assurer l'authenticité, la confidentialité et l'intégrité des données dans un RCSF. L'objectif de base était de fournir un protocole de sécurité qui ne sollicite pas de grandes puissances de calcul, d'espacede stockage et de bande passante. En effet, les auteurs proposent deux versions du protocole TinySec : TinySec-Auth, dédié uniquement à l'authentification, et TinySec-AE, qui permet le cryptage et l'authentification. Le protocole TinySec est basé sur le mécanisme d'authentification par code *(MAC)*, qui utilise un système de cryptographie symétrique. Cependant, comparé aux protocoles précédents, la taille du code MAC est très réduite *(4 octets au lieu de 8 ou 16 octets)*, ce qui permet de réduire significativement le surcoût de sécurité.
5. **Le protocole MiniSec *(Mini security):***L'idée de base est de proposer un nouveau mécanisme d'authentification qui consomme moins de ressources comparé au protocole TinySec. Pour cela, les auteurs optent pour l'utilisation d'un nouvel algorithme de cryptographiesymétrique, à base de chiffrement par bloc. Ce dernier est nommé OCB *(Offset CodeBook)*. Le protocole MiniSec utilise deux mécanismes d'authentification : le premier est destiné à l'authentification unicast *(MiniSec-U)*, et l'autre à l'authentification

par diffusion *(MiniSecB)*. MiniSec offre un grand niveau d'authentification et de confidentialité, avec moins de consommation en ressources.

5.3 Agrégation des données

Il a été montré dans plusieurs publications scientifiques que la transmission d'un bit est équivalente, en termes d'énergie, à l'exécution d'environ 1000 instructions. Cette valeur augmente avec la portée de la radio. Plus le capteur qui devra transmettre, est loin, et par conséquent il devra augmenter sa puissance d'émission pour atteindre la station de base, plus il consomme plus de l'énergie, ce qui affecte sa durée de vie. Il convient donc d'agréger les données avant les acheminer à la station de base. Les techniques d'agrégation des données, permettent de réduire le nombre de messages redondants et par conséquent réduire la consommation en énergie. Par exemple, si un réseau est déployé pour mesurer la température et que le puits n'est intéressé que par la moyenne des températures, un nœud intermédiaire pourra additionner les valeurs reçues de ses membres et envoyer le résultat au nœud relais dans la direction de la station de base. Le puits recevra alors qu'un seul message, contenant la somme des données au lieu de n messages (ou n est le nombre de capteurs). Ces techniques d'agrégation sont souvent utilisées. Elles sont cependant difficiles à mettre en œuvre lorsque les données sont chiffrées car le traitement des données devient alors très délicat[13].

6. Conclusion

Dans ce chapitre, nous avons présenté la sécurité des réseaux de capteurs, en parlant sur les problèmes de la sécurité, les objectifs ainsi que les attaques et leur mécanismede défense avec les différents protocoles. Dans le chapitre suivant, nous introduirons en détail l'implémentation et l'évaluation de Tinysec.

Chapitre III :

Implémentation et évaluation de l'application

1.Introduction

Dans le cadre du projet, nous avons mis en place une plateforme d'expérimentation qui a pour but de tester, de valider et de simuler le fonctionnement d'un réseau de capteurs. Sa principale fonction est de vérifier le comportement des capteurs développés avant même de les avoir déployé en situation réelle. Les domaines d'utilisation des réseaux de capteurs sont variés, dans notre projet nous nous sommes intéressées plus particulièrement à leur utilisation dans la modélisation et la simulation d'un système de détection d'un évènement critique par exemple le feu de forêt, c'est ce que nous allons présenter dans ce chapitre et à la fin de l'évaluation de l'application les résultats obtenus.

2.Le système d'éxploitation TinyOS

TinyOS est un système d'exploitation open source intégré, modulaire, destiné aux réseaux de capteurs miniatures. Cette plate-forme logicielle ouverte et une série d'outils développés par l'Université de Berkeley est enrichie par une multitude d'utilisateurs. En effet, **TinyOS** est le plus répandu des **OS** pour les réseaux de capteurs sans-fil. Cet OS est capable d'intégrer très rapidement les innovations en relation avec l'avancement des applications et des réseaux eux même tout en minimisant la taille du code source en raison des problèmes inhérents de mémoire dans les réseaux de capteurs. **TinyOS** est en grande partie écrit en C mais on peut très facilement créer des applications personnalisées en langages C, NesC, et Java. Il peut être installé à partir d'un environnement Windows ou bien Linux [14].

3.Tinysec

TinySEC est une librairie de sécurité intégrée dans le système d'exploitation **TinyOS-1.x**. L'objectif de cette librairie est de pouvoir détecter les paquets non autorisés lorsqu'ils sont injectés pour la première fois dans le réseau et éviter leur propagation dans le réseau qui amènerait par les communications engendrées, à une perte d'énergie. Pour cette raison, **TinySEC** met en place des mécanismes d'authentification basés sur le code MAC, de chiffrement des informations et une protection contre les redondances d'informations. Pour permettre une plus grande liberté d'actions, **TinySEC** supporte deux options de sécurité différentes :

TinySec-Auth : La sécurité concerne seulement l'authentification des données. Les données ne sont pas chiffrées, contrairement au code MAC qui est calculé à partir de l'entête du paquet pour assurer l'authenticité de l'expéditeur.

TinySec-AE : La sécurité porte à la fois sur l'authentification et l'encryptage des données. Les données sont chiffrées et envoyées avec un code MAC généré à partir des données chiffrées et de l'entête du paquet.

Pour l'authentification et l'encryptage des données **TinySec**utilise un chiffrement par blocs de type CBC-MAC. De la même manière que pour SNEP, **TinySec** utilise un vecteur initial pour le chiffrement du premier bloc et des chaînes de bits aléatoires ajoutés au message pour empêcher un attaquant d'analyser le trafic par comparaison des paquets. Cependant **TinySec** n'utilise pas de compteur pour chaque chiffrement, ce qui empêche de garantir la fraîcheur des données et laisse possible les attaques de type rejeu de paquets. Il est aussi à noter que **TinySec** n'est pas adapté à TinyOs-2.x [8].

4. Management de clé

TinySec utilise une clé symétrique (single) cela implique qu'il faut utiliser le même pc pour installer tous les nœuds. Onpeut changer la clé dans le fichier suivant : (c:\tinyos\cygwin\home\administrateur/tinyos_keyfile). Si on ne change pas la clé prédéfinie dans tinySec alors par défaut ce dernier utilise cette clé «6D524D67F24F178B0A69933FDD6C6F7B ».

Voila le fichier de « TinyOS_keyfile » :

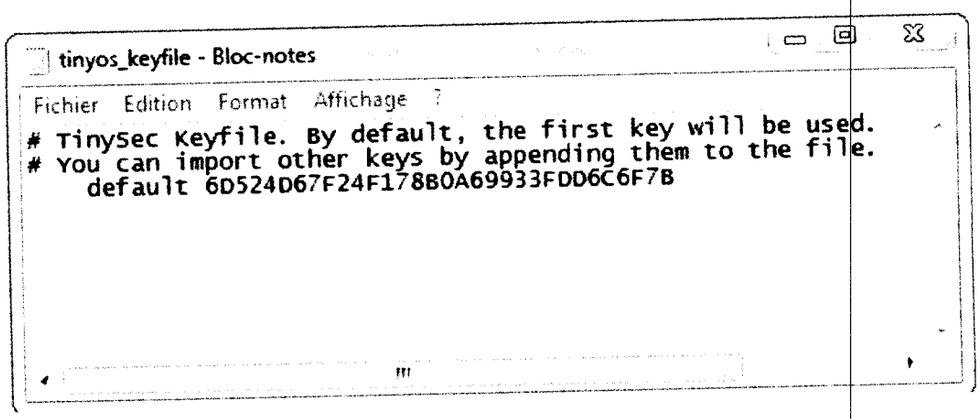


FIGURE 3. 1 : LE FICHIER KEYFILE

Pour notre application, nous avons utilisé deux clés dans les deux architectures : une clé de taille 16 bits et une clé de 32 bits.

5. Les étapes d'écriture d'une application avec TinySec :

Pour écrire une application avec avec TinySec ,il faut suivre ces étapes :

1- Utiliserla version TinyOS x.1
2- Dans le fichier makefile , il faut qu'on ajoute la condition suivante « TinySec= true ;» .
3- Par défaut le tinysec authentifie tous les messages sans les chiffrer.
4- Utiliser l'interface **TinySecmode**.
5- Dans TinySecmode , on trouve deux commandes une pour l'envoie des messages et une pour la réception .

command result_t setTransmitMode(uint8_t mode);
command result_t setReceiveMode(uint8_t mode);

la commande **setsetTransmitMode** prend un des arguments suivants :

TINYSEC_AUTH_ONLY
TINYSEC_ENCRYPT_AND_AUTH
TINYSEC_DISABLED

et la commande **setReceiveMode**prend un des arguments suivants :

TINYSEC_RECEIVE_AUTHENTICATED
TINYSEC_RECEIVE_CRC
TINYSEC_RECEIVE_ANY

✓ **La commande SetTransmitMode :**

Par défaut, TinySec utilise l'argument « tinysec _auth_only » pour l'envoie et l'authentification des messages.

L'argument suivant **TINYSEC_ENCRYPT_AND_AUTH**sert àauthentification et chiffrer en même temps.

Par contre TINYSEC_DISABLED sert à envoyer normalement les messages corrigés par le **CRC (kifeche ysamouhe).**

✓ **la commande setReceiveMode :**

On a l'argument TINYSEC_RECEIVE_AUTHENTICATED qui reçoit de TINYSEC_AUTH_ONLY et TINYSEC_ENCRYPT_AND_AUTH par contre l'argument TINYSEC_RECEIVE_ANY reçoit depuis les trois arguments d'envoi. Cet argument TINYSEC_RECEIVE_CRC reçoit depuis TINYSEC_DISABLED.

Nous avons utilisé le simulateur **TOSSIM** dans notre application car nous ne possédons pas de capteurs réels de type meca2.

6. Simulateur de réseau de capteur

L'objectif de la plateforme est de simuler un réseau de capteurs, ce qui sous-entend que nous n'utilisons pas de capteurs réels. Dans cette optique, nous présentons deux simulateurs que nous avons étudié **TOSSIM.**

TOSSIM est le simulateur de **TinyOS.** Il permet de simuler le comportement d'un capteur (envoie/réception de messages via les ondes radios, traitement de l'information, ...) au sein d'un réseau de capteurs. Pour une compréhension moins complexe de l'activité d'un réseau, **TOSSIM** peut être utilisé avec une interface graphique **TinyViz,** permettant de visualiser de manière intuitive le comportement de chaque capteur au sein du réseau.

TinyViz est une application graphique qui donne un aperçu de notre réseau de capteurs à tout instant, ainsi que des divers messages qu'ils émettent. Il permet de déterminer un délai entre chaque itération des capteurs afin de permettre une analyse pas à pas du bon déroulement des actions.

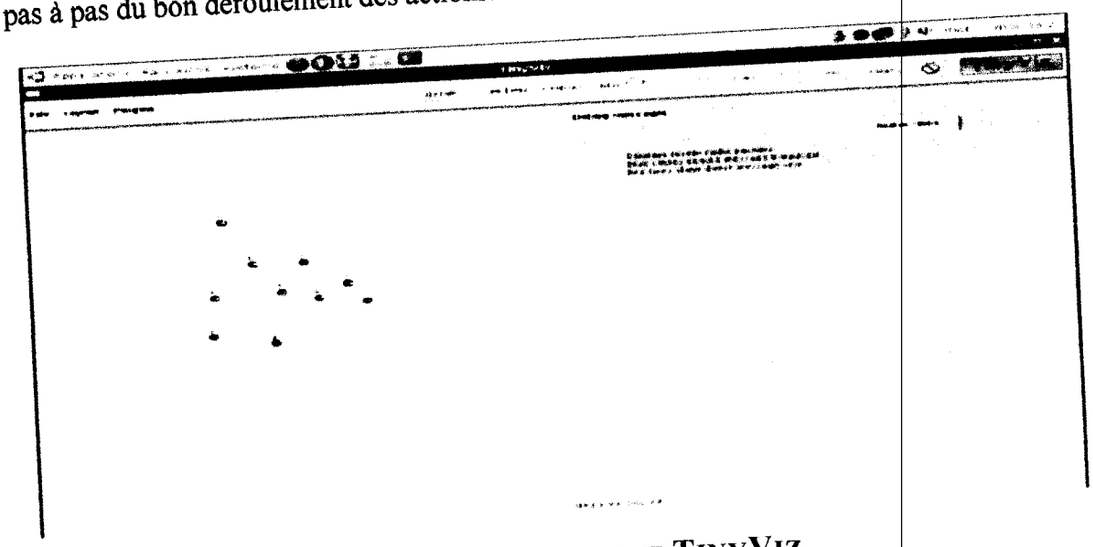


FIGURE 3. 2 : FENETRE GRAPHIQUE TINYVIZ.

On peut voir dans la partie de gauche de la figure 3 tous les capteurs. Ils sont déplaçables dans l'espace, ou si l'on possède une configuration particulière, on peut charger un fichier qui positionnera chaque capteur à l'emplacement spécifié.

L'interface graphique **TinyViz,** qui permet la visualisation des échanges radios, conjointement aux messages de débogage, ce qui permet, à chaque instant de la simulation, d'avoir une vue globale de l'activité du réseau étudié. **TinyViz** offre la possibilité de ralentir la simulation par un délai, afin d'observer le déroulement des évènements, ce qui est très intéressant lorsque le réseau est surchargé de messages[15].

7. Les métriques de simulations

Dans notre simulation, nous nous intéresserons essentiellement aux taux de détection de notre application puisqu'elle constitue le paramètre le plus critique dans l'évaluation performance d'un système de détection d'un événement critique.
Notre étude est basée sur deux métriques très importantes, voire même critiques dans les réseaux de capteurs sans fils qui sont : la consommation d'énergie. La consommation d'énergie est un facteur vital dans un RCSF, une fois l'énergie épuisée le réseau ne sera plus fonctionnel.

- ✓ **Consommation d'énergie :**Le Cluster Head représente l'axe de notre étude de consommation d'énergie dans le RCSF puisqu'il représente une passerelle entre le Sink et le Sender et effectue des opérations plus importantes qu'un nœud ordinaire, nous avons utilisé la fonction energest dans "sys/energest.h" pour afficher la quantité d'énergie consommée par le Cluster Head.

8. Topologie du réseau

Agrégation :considérée comme approche préventive, l'opération d'agrégation effectue un traitement supplémentaire sur les données brutes captées depuis l'environnement. Un nœud agrégateur combine les données provenant de plusieurs nœuds en une information significative. Ce qui réduit considérablement la quantité de données transmises en consommant moins d'énergie pour leur dissémination. Ceci permet donc d'augmenter la durée de vie du réseau[6].

L'agrégation de données dans les réseaux de capteurs consiste à remplacer les lectures individuelles de chaque capteur par une vue globale, collaborative sur une zone donnée(clustering). On peut utiliser par exemple de simples fonctions d'agrégat

telles que MIN, MAX, ou MOYENNE.Pour notre application,nous avons utilisés une série de 10 messages reçus par un « chef de zone » qui renvoievers le puits qu'un seul message, résumant l'information contenue dans ces 10 messages en calculent la moyenne : elle exprime la grandeur qu'auraient chacun des membres de l'ensemble s'ils étaient tous identiques sans changer la dimension globale de l'ensemble. Ceci réduit le nombre de messages envoyées et donc économise l'énergie [16].

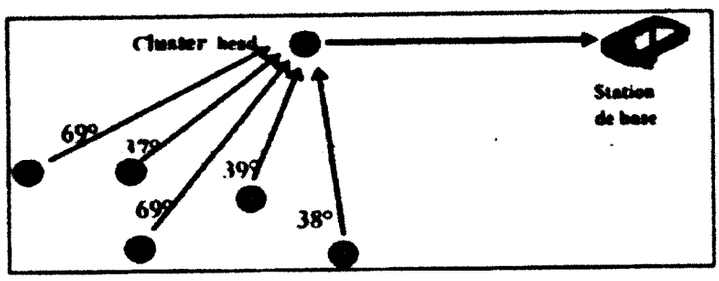


FIGURE 3. 3 : AGREGATION DE DONNEES (TEMPERATURE).

Notre application consiste à simuler un réseau de capteurs qui permet de détecter un évènement critique, les nœuds de ce réseau sont des capteurs de température. Pour cela on propose une architecture plate « hiérarchique » et une architecture clustérisée.

a. ARCHITECTURE PLATE

C'est une architecture surN niveaux tel que tous les nœuds possèdent le même rôle ; le premier niveau est constitué d'une station de base, le deuxième niveau c'est les pères des nœuds et dans le dernier niveau on trouve les nœuds fils. Comme il est présenté dans la figure ci-dessous, dans chaque niveau on installe certains nombres de capteurs (nœuds ordinaires).

Nœud collecteur (Sender) : Il s'occupe de la détection de la température dans son environnement, chiffre cette donnée en utilisant TinySec puis l'envoi au nœud père en utilisant la fonction suivante : **Tos_local_address** -1/5

Le nœud père : Il s'occupe de recevoir les données transmises par les nœuds Sender sans les déchiffrer, calcule leur moyenne et il envoie le résultat à la station de base.

Station de base (Sink) : La Station de Base s'occupe du déchiffrement des données pour en déduire la température moyenne dans le réseau.

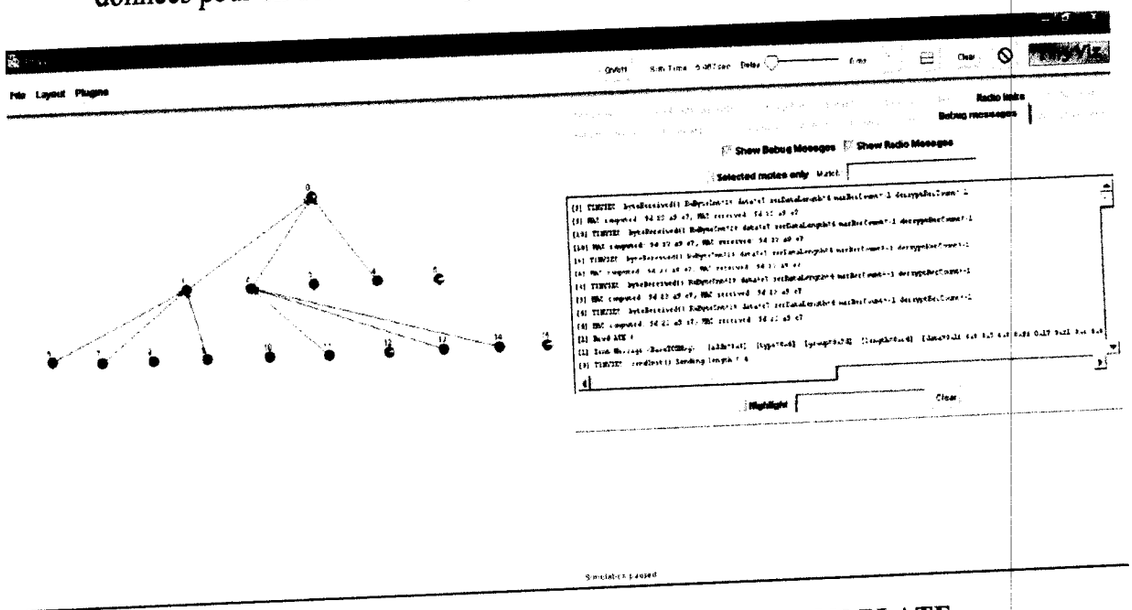


FIGURE 3. 4: TOPOLOGIE 1 DE L'APPLICATION PLATE.

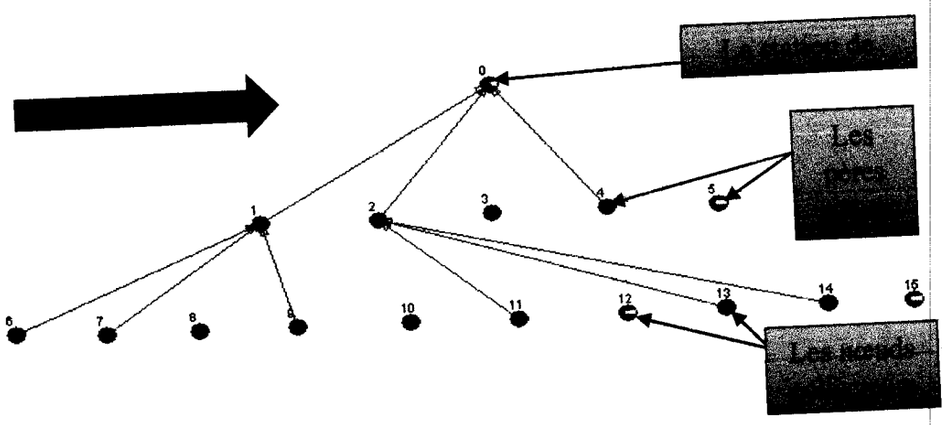


FIGURE 3. 5: LES COMPOSANTES DE L'ARCHITECTURE PLATE.

a.1 La consommation d'énergie totale

En termes de consommation d'énergie, on remarque un écart important entre les deux architectures, et pour la calculer dans **TinyViz,** il faut qu'on utilise « **postprocess.py** » qui se trouve dans « **PowerTossim** » qui est une fonction prédéfinie dans **TinyViz** ». Ainsi qu'on

doit aussi vérifier deux conditions : Par exemple nous avons voyez un message pendant tous les **250 ms** mais avec une architecturede **10** nœuds dans les deux cas de fonctionnement « critique et non critique », Cela veut dire que nous avons tester le pire des cas quand tous les nœuds veulent détecter un feu ou bien quand il n'y a pas un feu mais à condition que le chiffrement avec une clé de 16 bit ou bien qu'avec une clé 32 bit.

a.1.1 Le mode TinySec-Auth

D'après les figures suivant, nous voyons tout d'abord que le chiffrement avec une clé de 16 bit consomme moins d'énergie que le chiffrement qui utilise une clé de 32 bit moins de 13% MJoule.

Ensuite, nous remarquons qu'il y'a plus d'énergie consommée lors de la détection d'un feu par rapport à une situation normale dans laquelle le nœud père calcule la somme des dix messages reçus et il envoie juste un message à la station de base pour minimiser le Trafic dans le réseau, éviter l'interférence des messages. Par contre dans l'état critique avec détection de feu, ce qui implique que la température est plus que 50°, le nœud père reçoit ce message directement il envoie à la station de base (le sink).

Cette dernière déclenche une alerte pour nous informer qu'il y'a un feu.

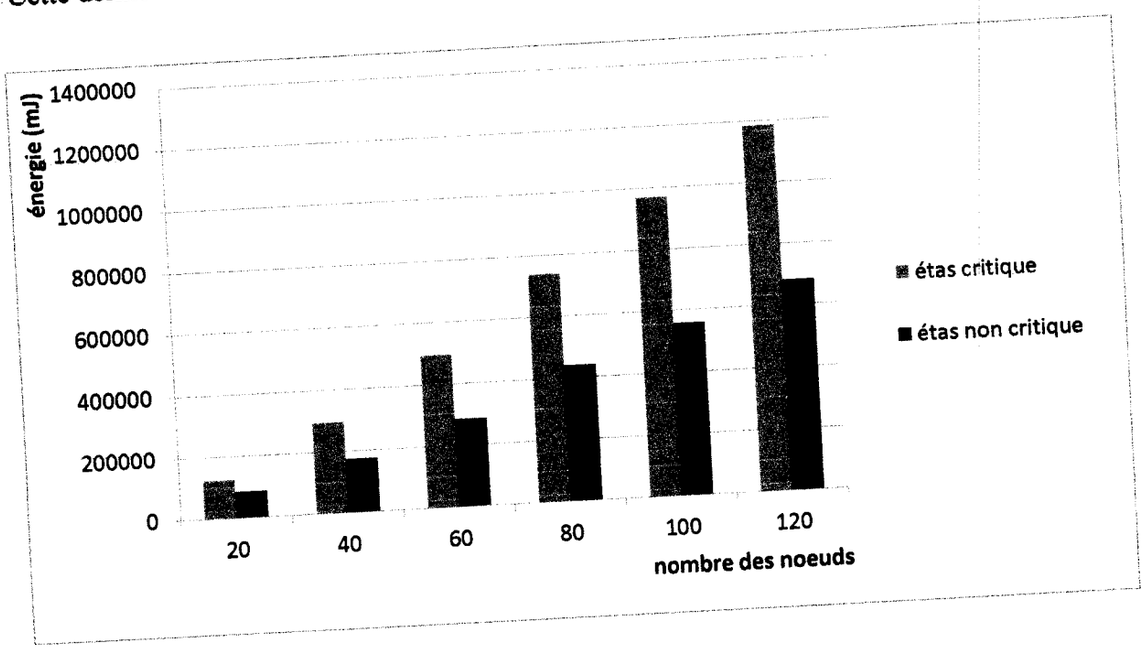


FIGURE 3. 6: CONSOMMATION D'ENERGIE AVEC UNECLE DE 32 BIT (MODE TINYSEC AUTH).

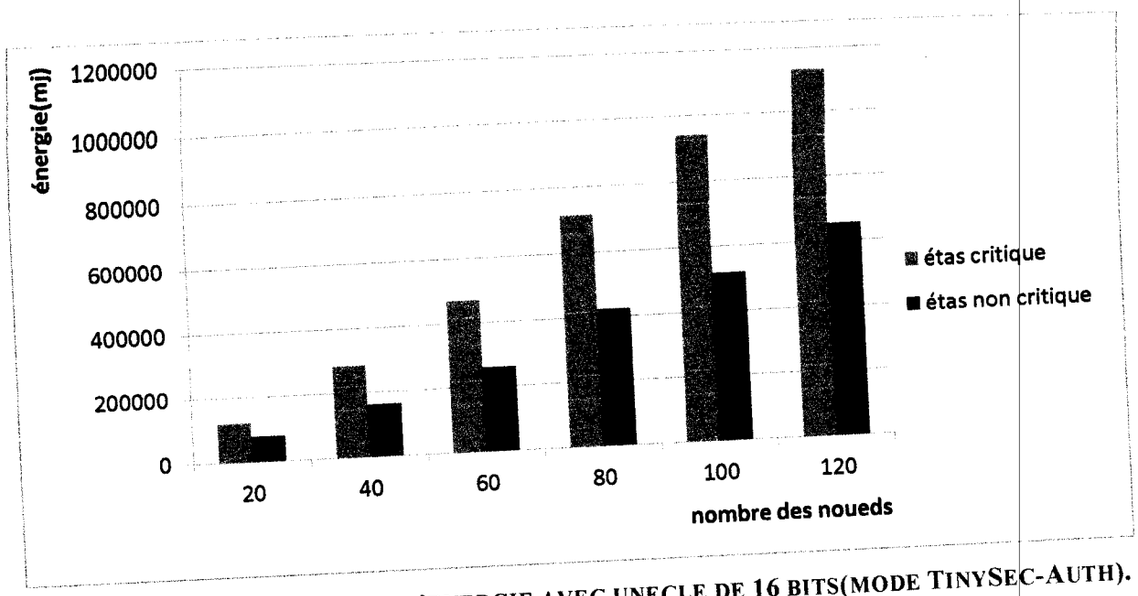


FIGURE 3. 7: CONSOMMATION D'ENERGIE AVEC UNECLE DE 16 BITS(MODE TINYSEC-AUTH).

a.1.2 Le mode Tinysec-AE :

Nous observons les mêmes résultats dans ce mode que Tinysec-Auth mais dans le mode AE consomme plus énergie que TinySec-Authcar il y'a le chiffrement de message par contre dansTinySec- Auth pas de chiffrement de message.

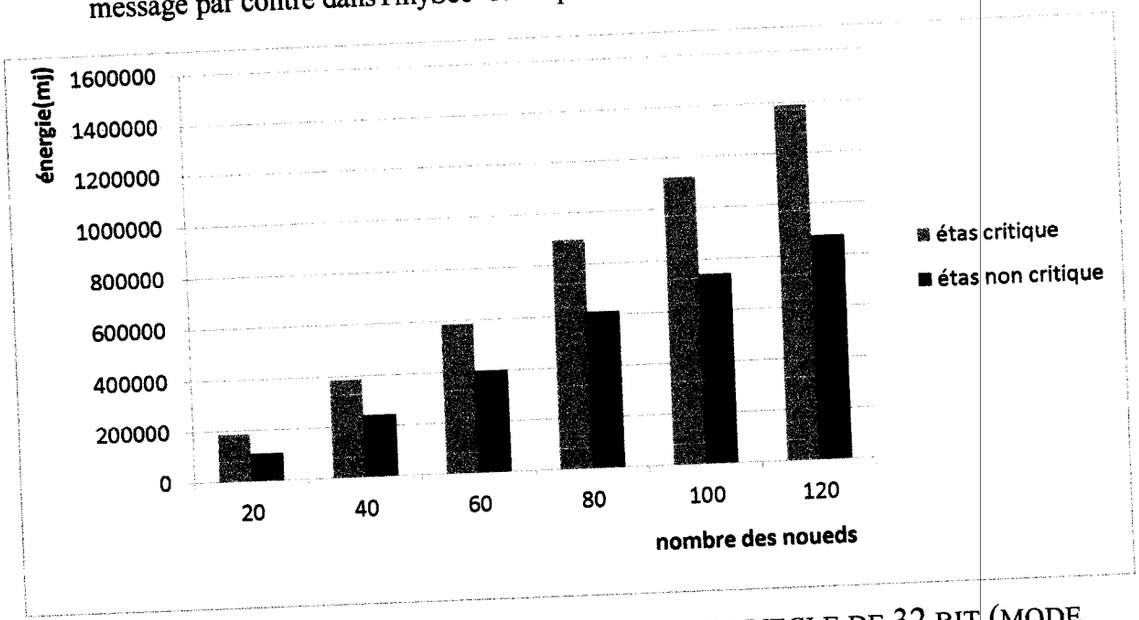


FIGURE 3. 8: CONSOMMATION D'ENERGIE AVEC UNECLE DE 32 BIT (MODE TINYSEC -AE).

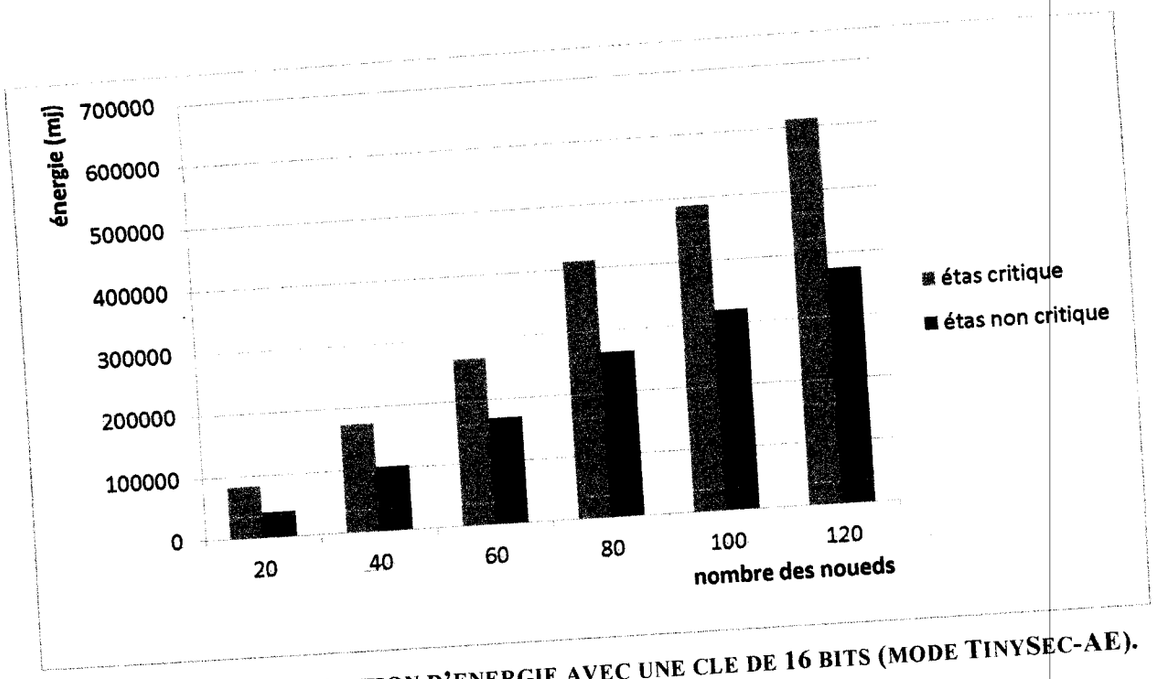


FIGURE 3. 9: CONSOMMATION D'ENERGIE AVEC UNE CLE DE 16 BITS (MODE TINYSEC-AE).

a.2 Consommations d'énergie du CPU

a.2.1 Le mode TinySec-Auth : Avec ce mode nous remarquons que l'énergie avec détection de feu est deux fois plus que dans une situation normale.

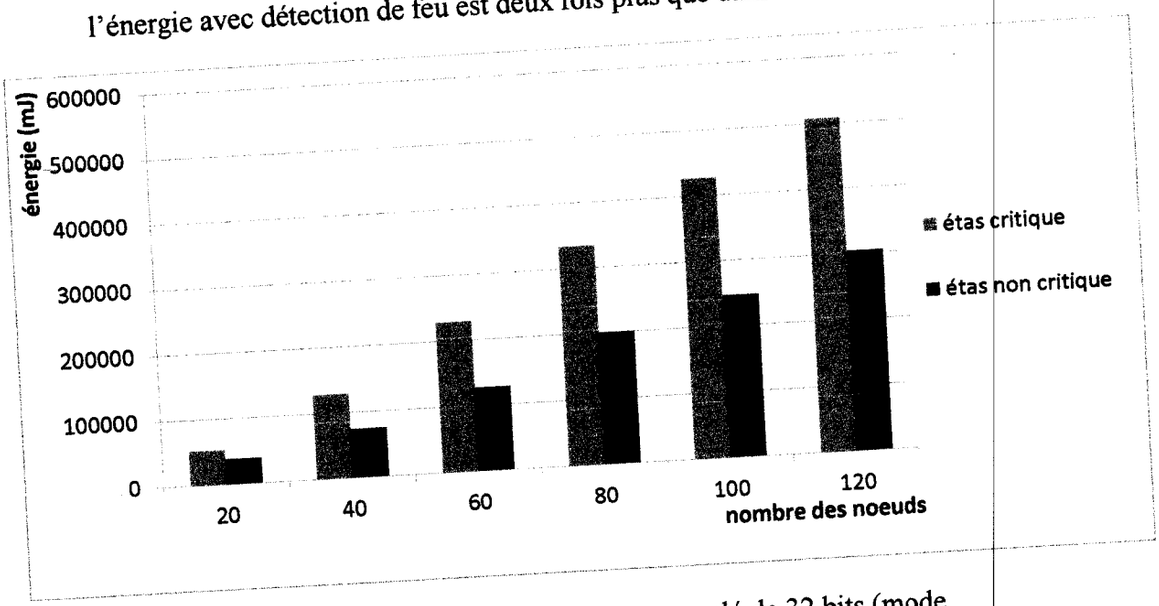


Figure 3. 10 : Consommation d'énergie du CPUavec une clé de 32 bits (mode TINYSEC-AUTH).

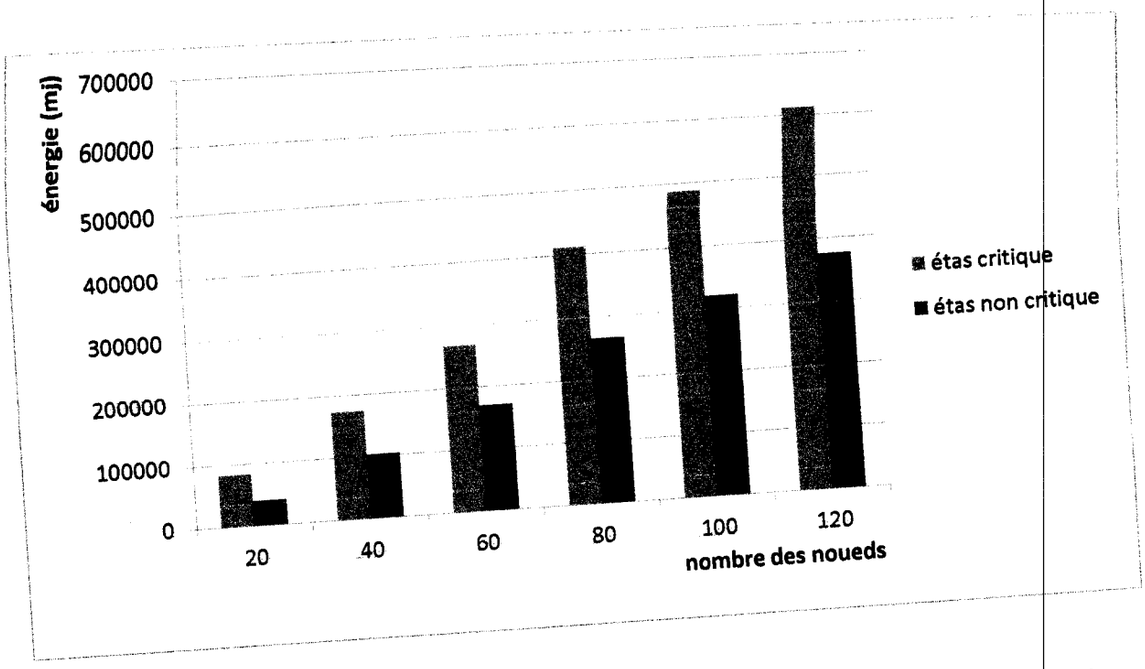


FIGURE 3. 11: CONSOMMATION D'ENERGIE DU CPU AVEC UNE CLE DE 16 BITS (MODE TINYSEC-AUTH).

a.2.2 Le mode TinySec-AE : Avec les deux figures ci-dessous,nous montrons la consommation d'énergie du CPU dans le mode TinySec-AE.

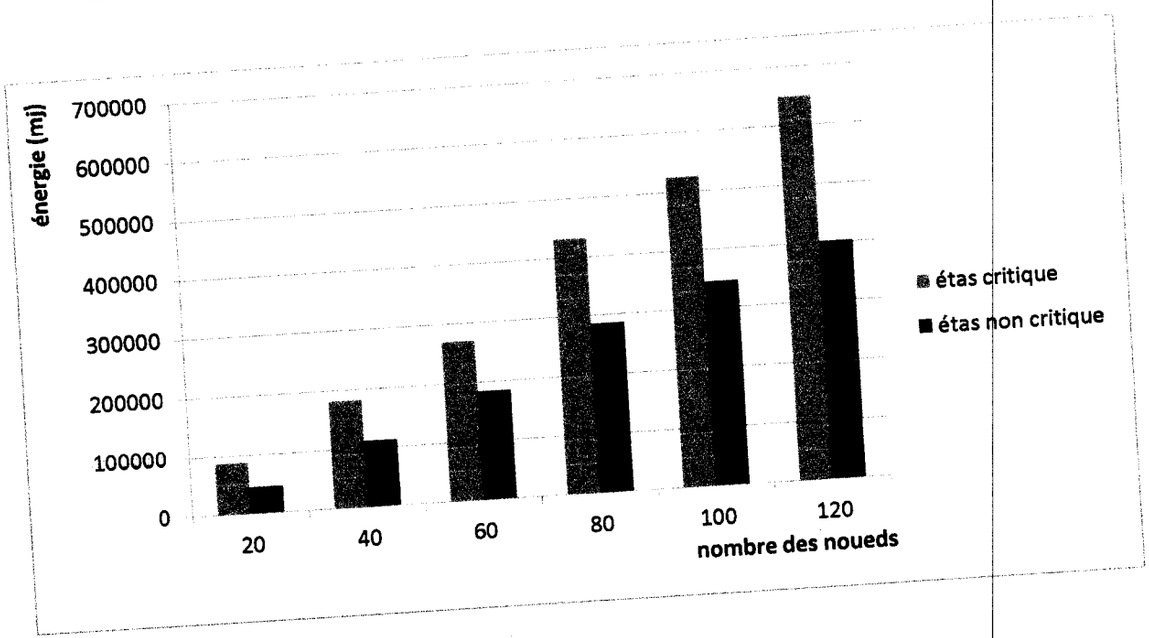


FIGURE 3. 12: CONSOMMATION D'ENERGIE DU CPU AVEC UNE CLE DE 32 BITS (MODE TINYSEC-AE).

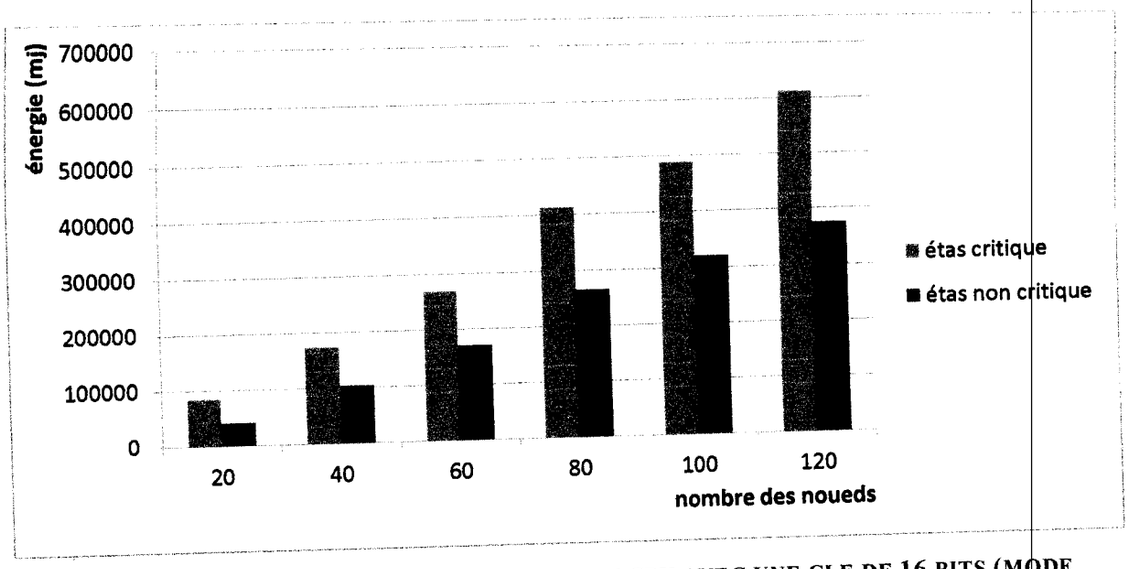


FIGURE 3. 13: CONSOMMATION D'ENERGIE DU CPU AVEC UNE CLE DE 16 BITS (MODE TINYSEC-AE).

9. La comparaison d'énergie entreTinySec-Auth et TinySec-AE :

La figure ci-dessous présente la différence totale de consommation d'énergie par les nœuds quand on utilise le mode TinySec-AE et TinySec-Auth.Cependant nous voyons que l'énergie dans TinySec-AE est plus grande que TinySec-Auth car ce dernier utilise plusieurs en tête dans la trame d'envois et de réception de message .

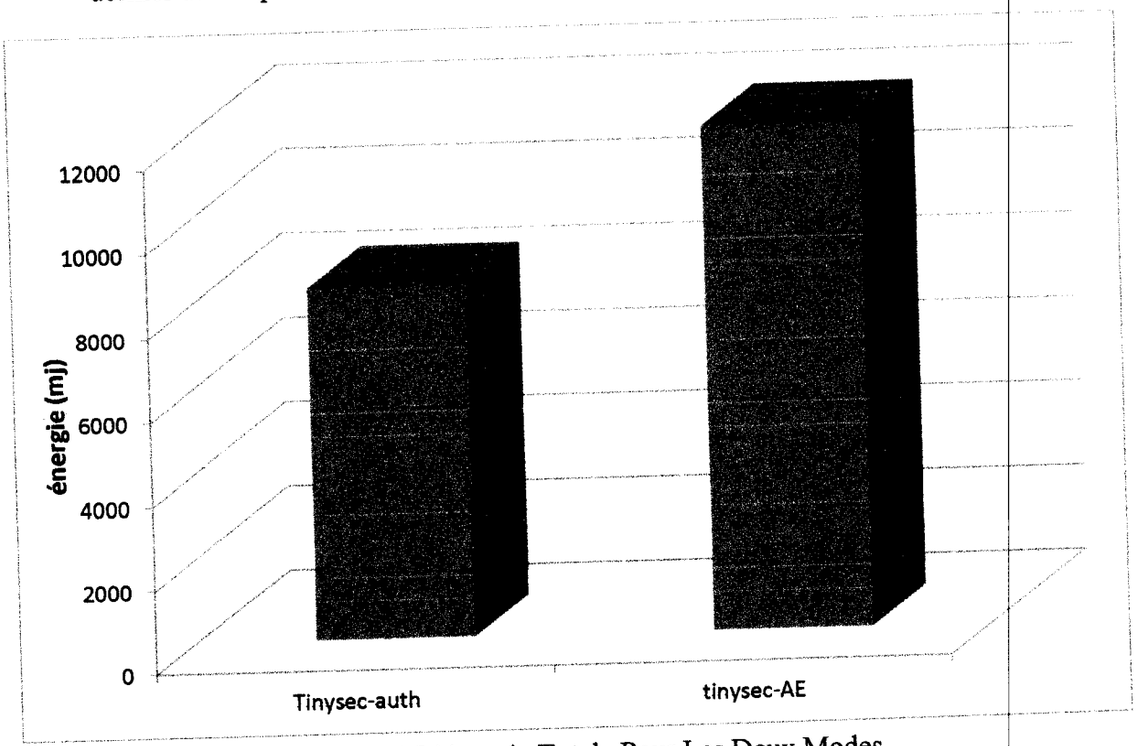


Figure 3. 14:L'énergie Totale Pour Les Deux Modes.

10. L'effet des modes TinySec sur le fonctionnement du Cpu :

La figure ci-dessous présente la différence de consommation d'énergie par les nœuds quand on utilise le mode TinySec-AE et TinySec-Auth.Cependant nous voyons que l'énergie consommer par la CPU dans le mode TinySec-AE plus que TinySec-Auth car ce dernier est traité plus des paquets que dans l'autre mode .

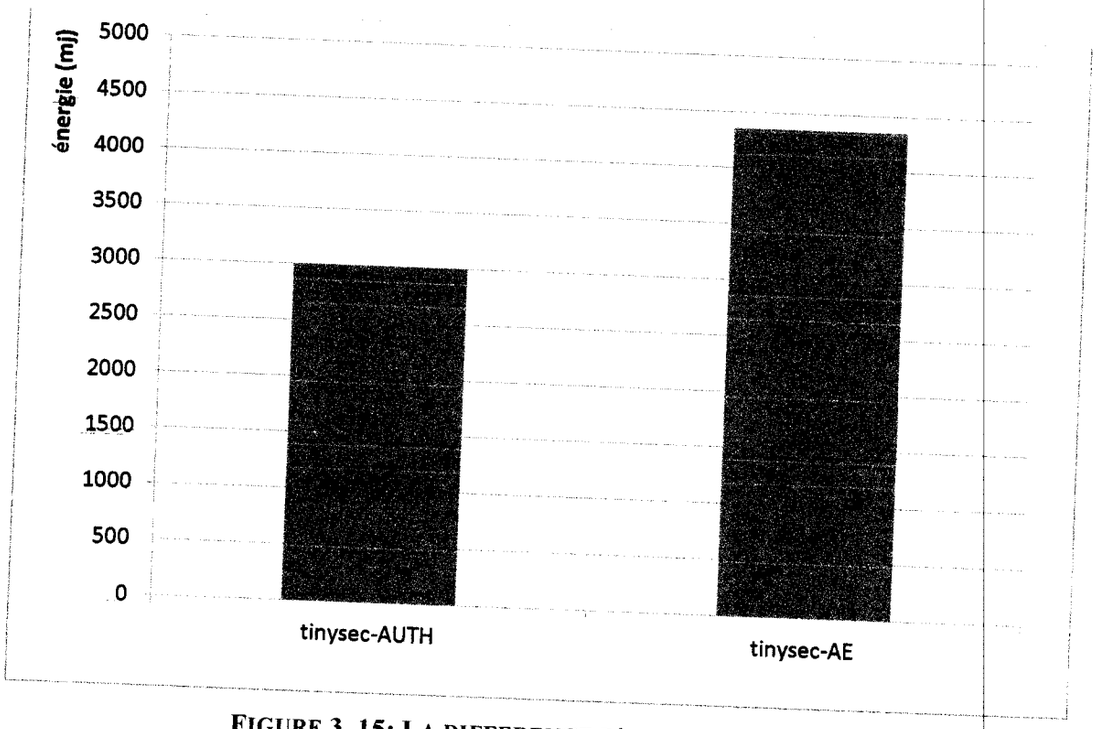


FIGURE 3. 15: LA DIFFERENCE D'ENERGIE DE CPU.

B. l'architecture clustérisée

C'est une architecture de zone, chaque zone est constituée d'un cluster Head et plusieurs nœuds collecteurs.

Nœud collecteur (Sender) : Il s'occupe de la détection de la température dans son environnement, chiffre cette donnée en utilisant TinySec puis l'envoi au nœud père en utilisant la fonction suivante : **Tos_local_address** -1/5.

Cluster Head :

Le cluster Head reçoit des valeurs en entrées venant des nœuds ordinaires, il doit faire un calcul pour l'envoyer au sink et décider par la suite sur la Température d'une zone ou non. Parmi les méthodes de calcul nous distinguons deux méthodes, il faut choisir entre la moyenne qui est la somme de l'ensemble des valeurs mesurées divisée par le nombre des capteurs dans l'état critique ou bien le cluster Head envoie directement la valeur de température reçu par les nœuds ordinaires à la station de base cela implique l'état critique c'est-à-dire le cas de feu.

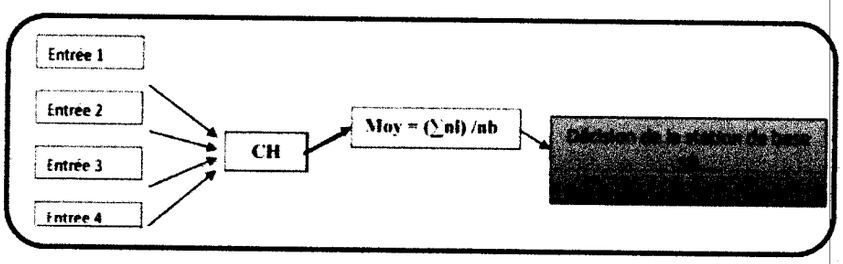


FIGURE 3. 16 : ARCHITECTURE CLUSTERISEE

Station de base (Sink) : La Station de Base s'occupe du déchiffrement des données pour en déduire la température moyenne dans le réseau.

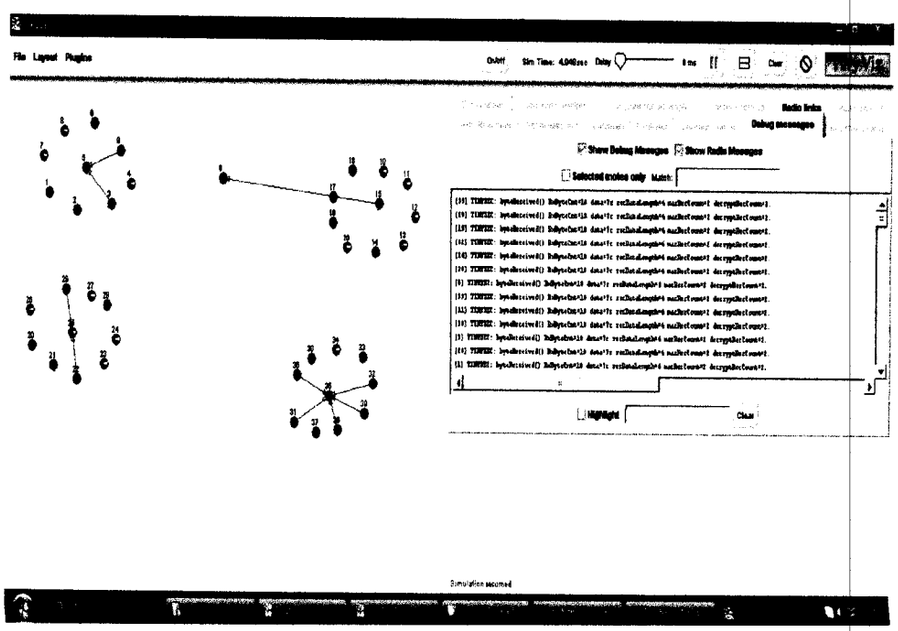


FIGURE 3. 17:LA TOPOLOGIE 2 DE L'APPLICATION : CLUSTERISEE.

La figure 3.24 représente quelques transmissions unicast de capteur membre vers le responsable de la zone (CH), Chaque membre capte la température et attend le début de son slot pour qu'il puisse l'envoyer à son CH. Quand ce dernier reçoit les différentes températures,il s'allume en vert.Nous avons utilisé une fonction statistique,à savoir la moyenne.

B.1 Consommation d'énergie Totale

b.1.1 TinySec-Auth :

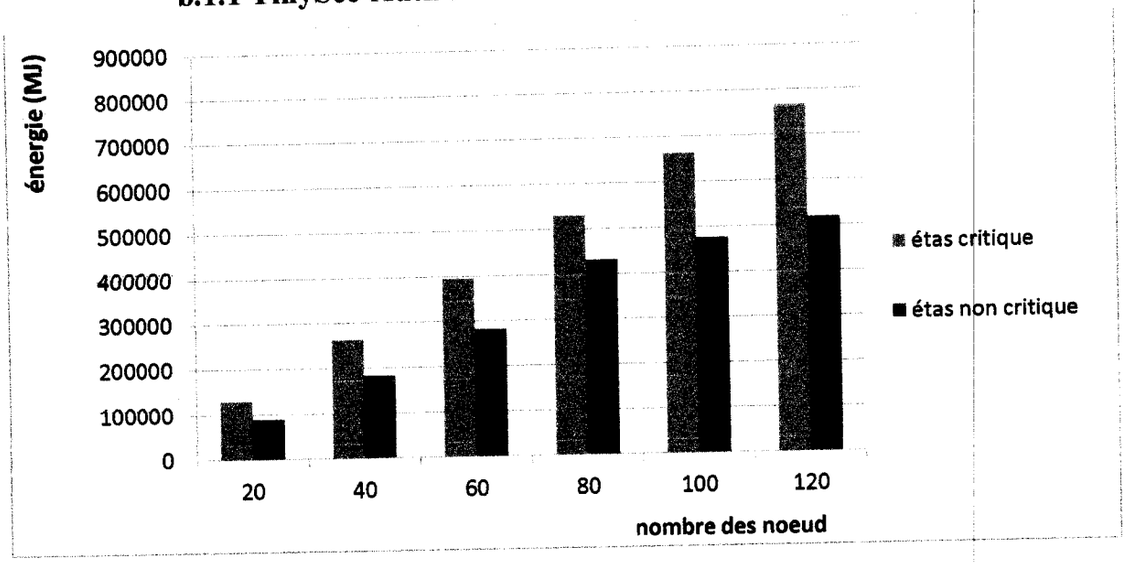


FIGURE 3. 18: CHIFFREMENT AVEC UNECLE 32 BIT.

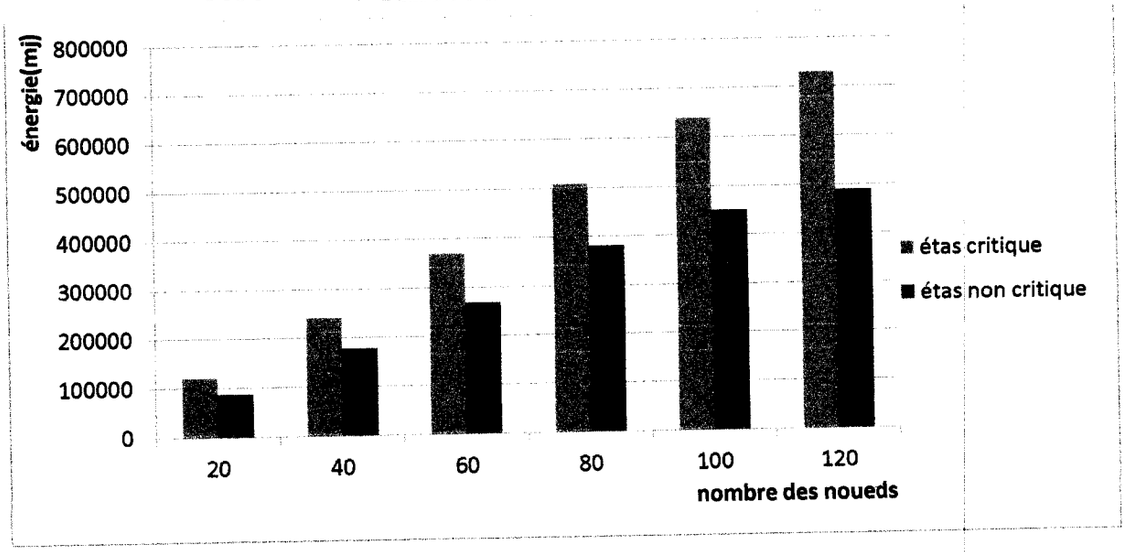


FIGURE 3. 19: CHIFFREMENT AVEC UNE CLE 16 BIT.

B.2TinySec-AE :

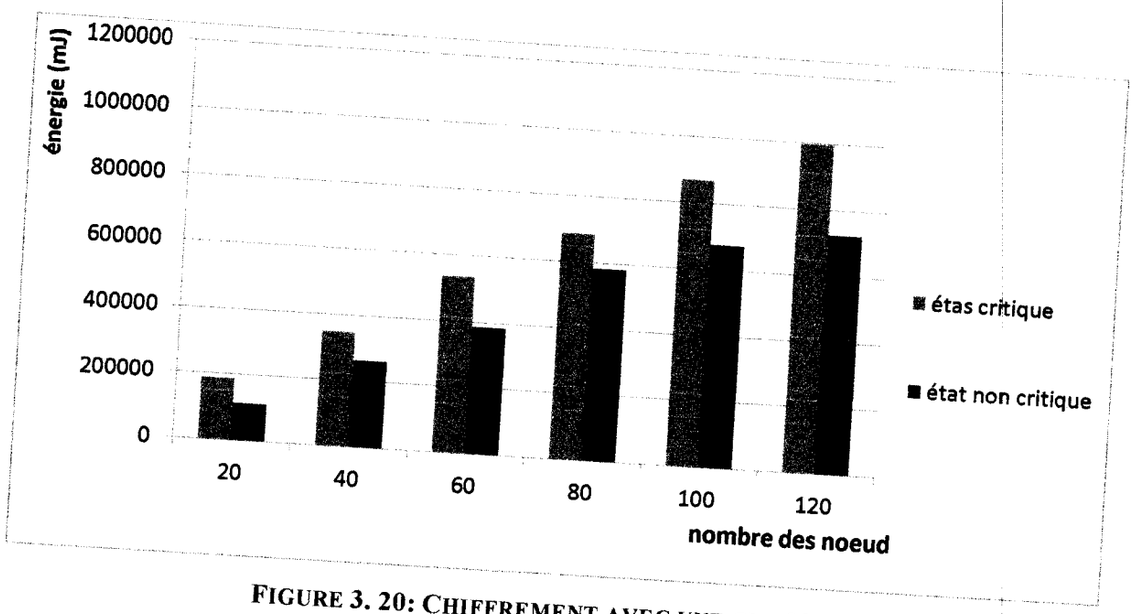


FIGURE 3. 20: CHIFFREMENT AVEC UNE CLE 32 BIT.

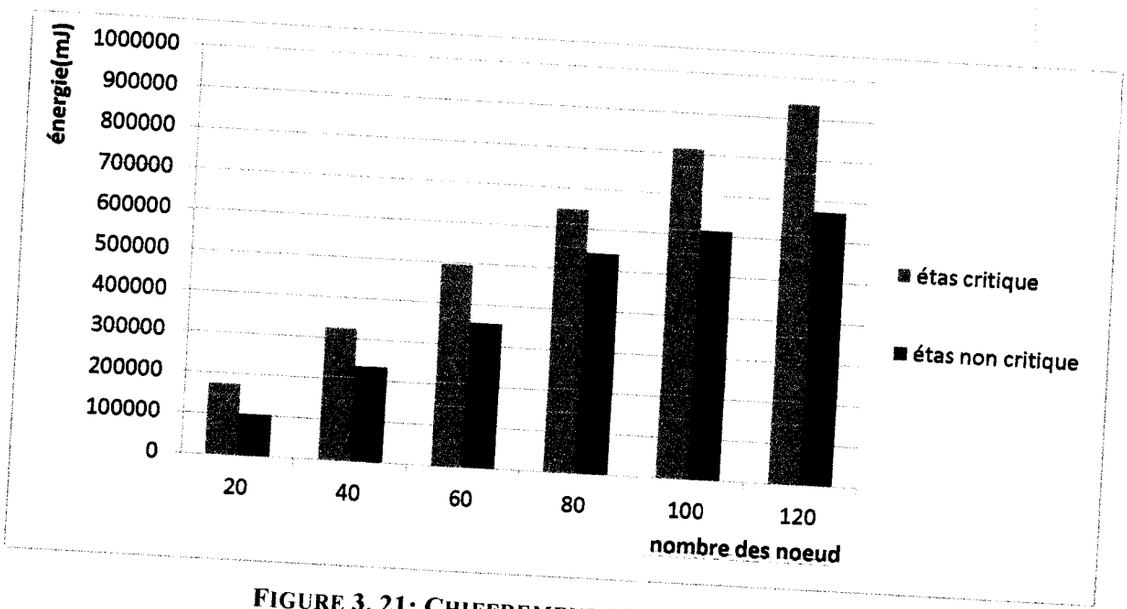


FIGURE 3. 21: CHIFFREMENT AVECUNE CLE 16 BIT.

C. Consommations énergie par CPU

C.1 TinySec- Auth :

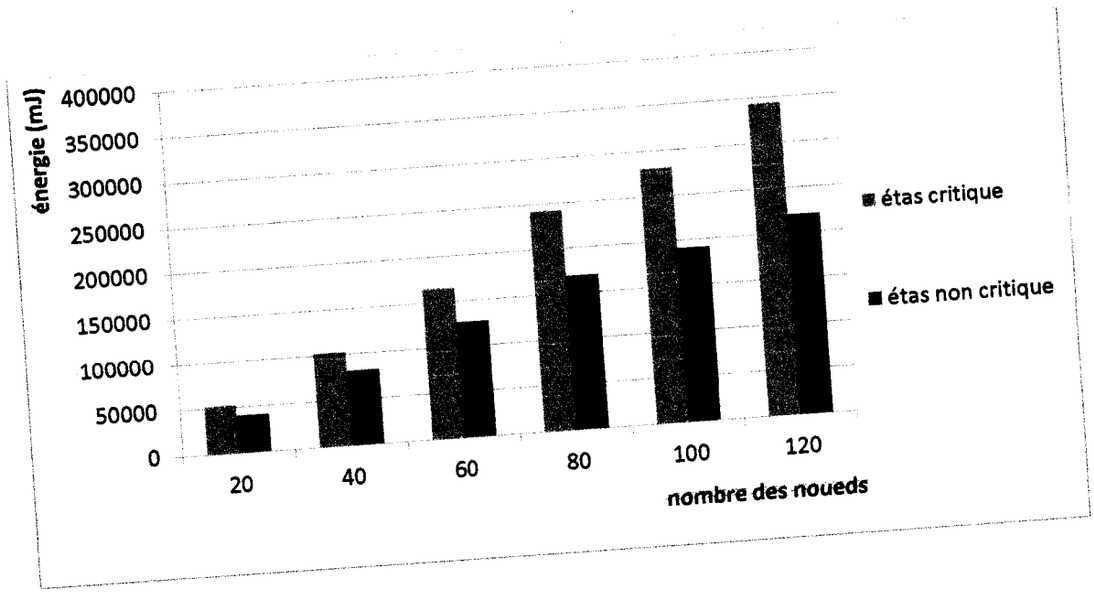


FIGURE 3. 22: CHIFFREMENT AVECUNE CLE 32 BIT.

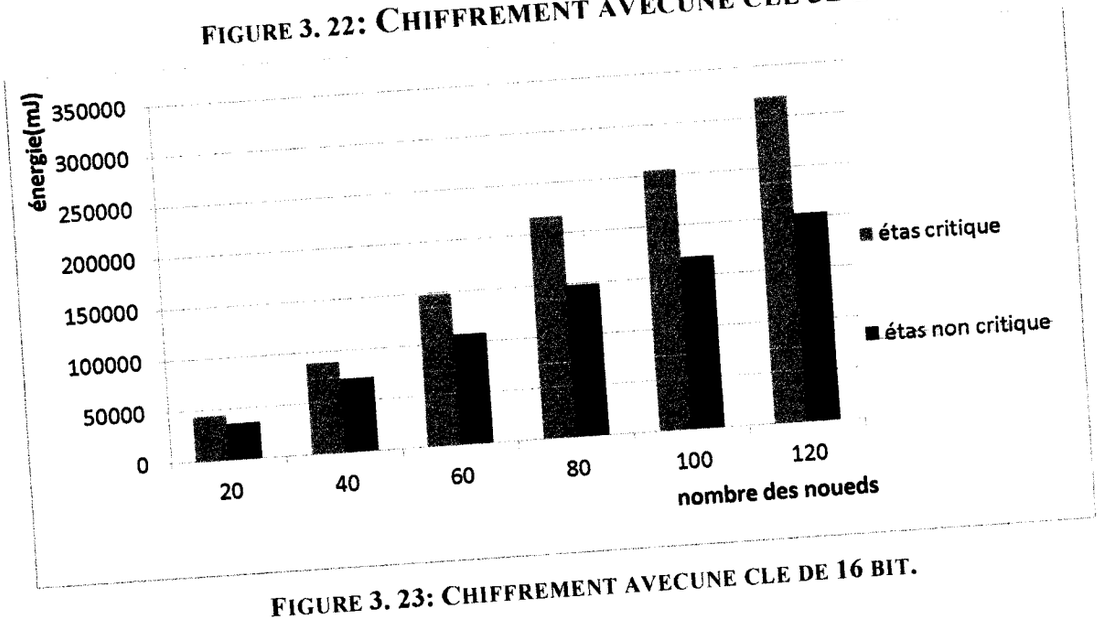


FIGURE 3. 23: CHIFFREMENT AVECUNE CLE DE 16 BIT.

C.2 TinySec- AE :

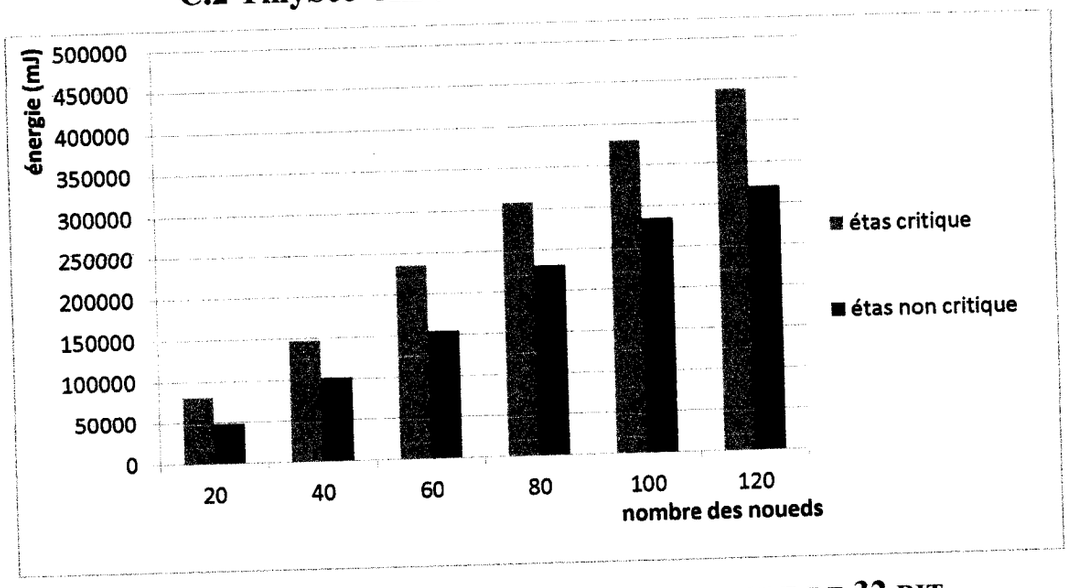


FIGURE 3. 24: CHIFFREMENT AVECUNE CLE DE 32 BIT.

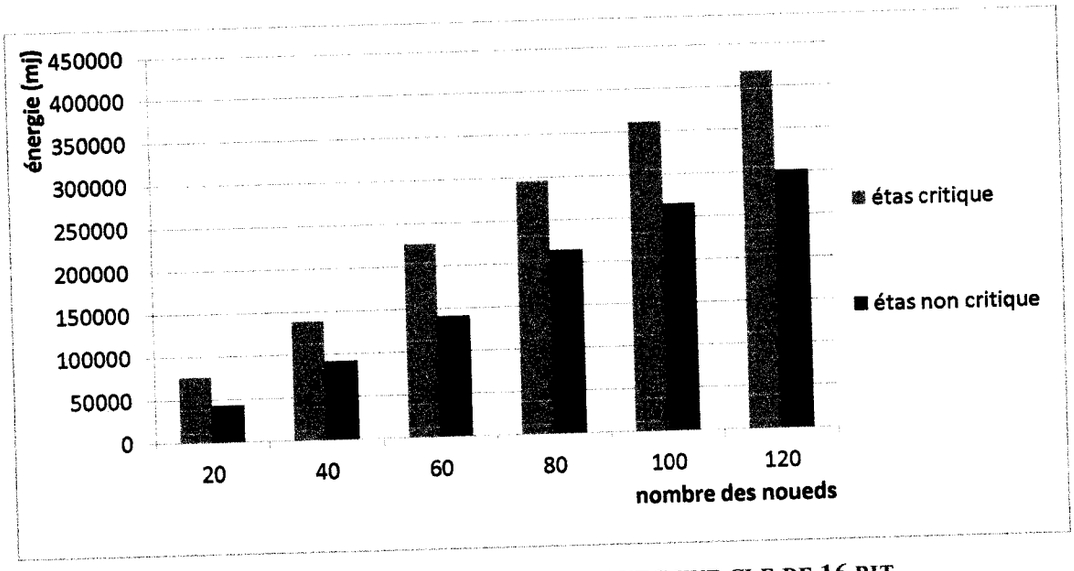
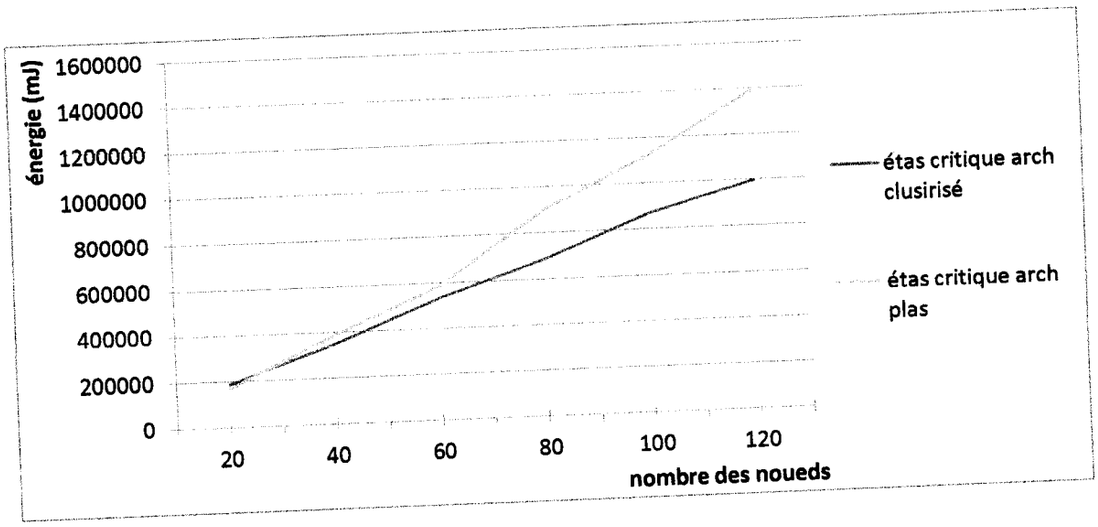


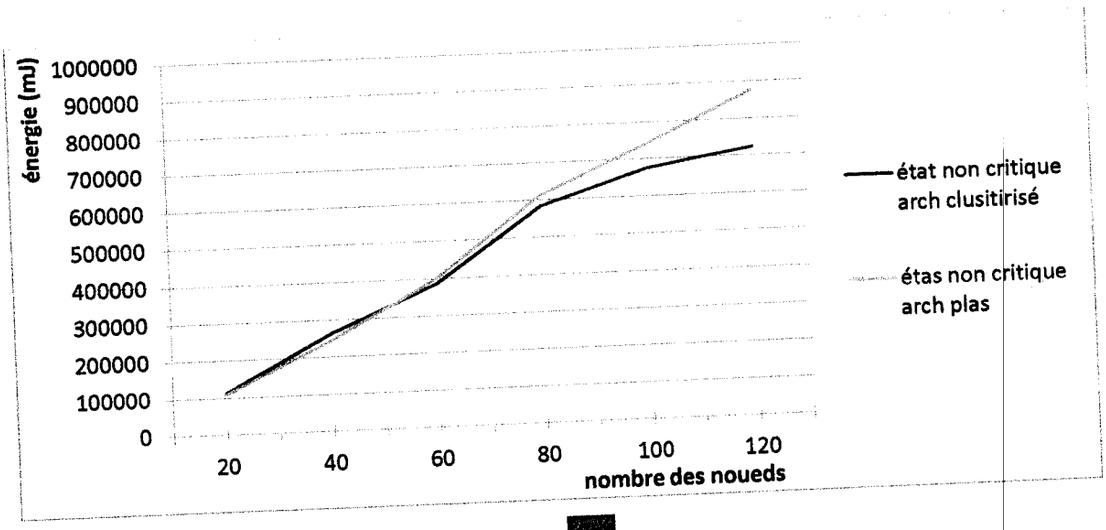
FIGURE 3. 25: CHIFFREMENT AVEC UNE CLE DE 16 BIT.

11.Critique comparative des deux approches

D'après les résultats obtenus, on peut constater que chaque approche a ses avantages et ses inconvénients. Dans l'approche plate, La consommation d'énergie est beaucoup plus importante que clustérisée.

Dans l'architecture plate, quand le dernier nœud envoie un message, il va se passer par deux pères pour qu'il puisse arriver au sink. Par contre dans l'architecture clustérisée, il va passer par un seul cluster Head.





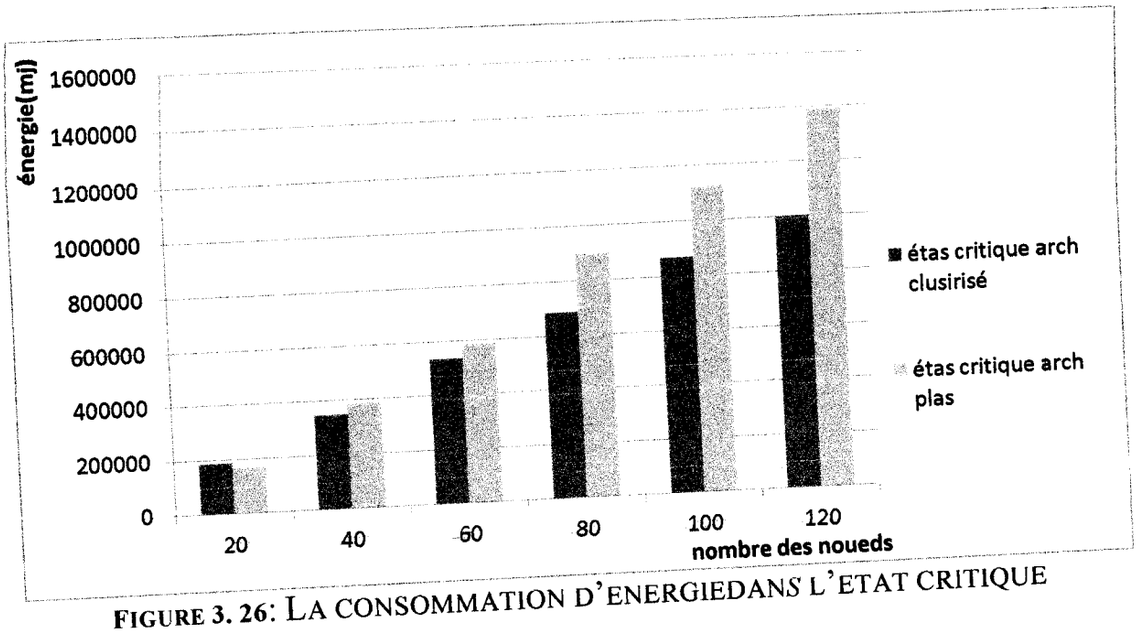


FIGURE 3. 26: LA CONSOMMATION D'ENERGIEDANS L'ETAT CRITIQUE

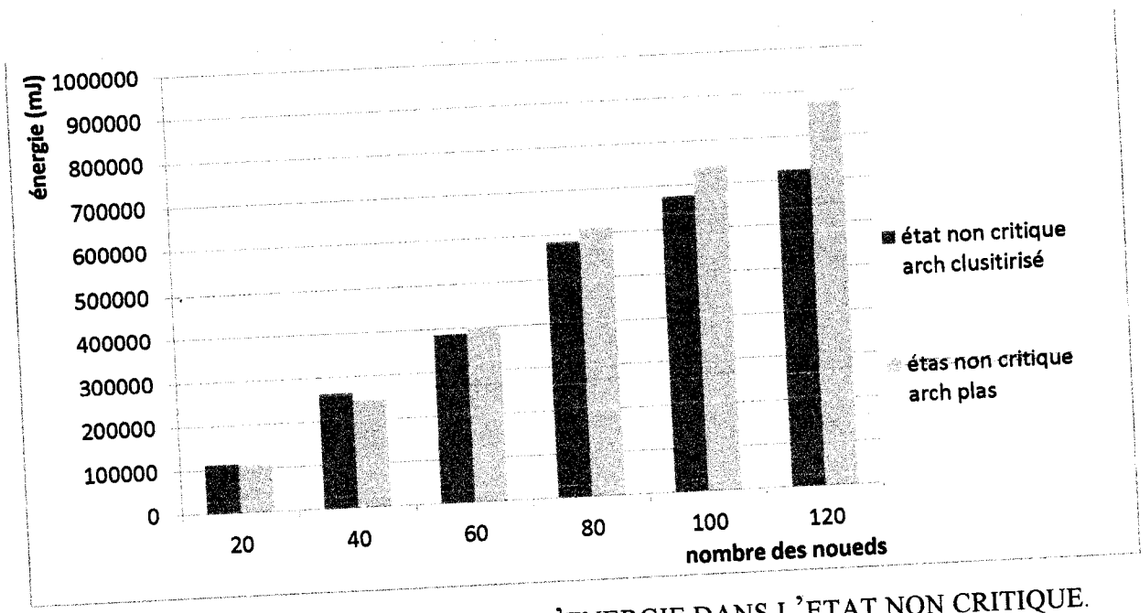


FIGURE 3. 27: *LA* CONSOMMATIOND'ENERGIE DANS L'ETAT NON CRITIQUE.

Conclusion

Dans ce chapitre nous avons évalué la librairie de sécurité TinySec, dans une application de détection d'événement par exemple dans notre cas un feu de forêt. Afin de faire une étude comparative, nous avons utilisé deux architectures plates et clustérisé. Nous avons également

utilisé deux modes de sécurité : avec authentification seule et avec authentification et chiffrement des données.

Il est clair que lors la détection d'un événement critique est beaucoup plus coûteuse car cela nécessite une la transmission urgente de l'information et ceci dans les deux architectures de réseau et dans les deux modes de sécurité. Désormais la sécurité est coûteuse en termes d'énergie et de calcul CPU et c'est le prix à payer si on veut assurer l'authentification et la confidentialité.

Conclusion générale

Les réseaux de capteurs sont une nouvelle technologie qui a surgit après les grands progrès technologie concernant le développement des capteurs intelligents, des processeurs puissants et des protocoles de communications sans fil. Ils ont été classés parmi les 21 technologies les plus importantes du 21éme siècle. En effet, la recherche dans le domaine des capteurs est en train de vivre une révolution importante, ouvrant des perspectives d'impacts significatifs dans de nombreux domaines tel que la détection d'un état critique comme c'est le cas de notre travail, pour que ces réseaux puissent mener à bien leurs missions ils doivent assurer un certain niveau de contrôle qui diffèrent selon l'application déployée.

Au cours de notre mémoire, nous nous sommes intéressées à mettre en place un réseau de capteurs pour la surveillance de l'environnement : capter la température et détection s'il y'a un feu. Nous avons également évalué la librairie de sécurité TinySec en termes de consommation d'énergie et de calcul CPU. Il a fallu pour cela prendre en main beaucoup de nouvelles technologies, comme TinyOS et le nesC.

D'un point de vue personnel, ce projet nous a apporté des bénéficies personnels, il a permis de découvrir un nouveau domaine, une nouvelle manière de programmer et de concevoir une application, avec des contraintes techniques et matérielles très importantes, la découverte de TinyOS et le NesC. Ce projet été particulièrement intéressant par le fait que les réseaux de capteurs sans fil sont vraiment en plein expansion de nos jours, mais encore trop peu connu des personnes extérieures à ce domaine, la recherche sur les réseaux de capteurs est actuellement en pleine essor.

Comme perspective de recherche, il serait intéressant de comparer la librairie TinySec avec une autre librairie telle que MiniSec. Cette dernière présume une consommation moins importante que celle de TinySec.

Bibliographie

[1] M.Messai , Sécurité dans les réseaux de capteur sans fil , université de Bejaia ,2008.

[2] S. Meldjem et C. Khalfi et N. Merabtine et K. Hadj Rabah, Les réseaux de capteurs, université de Houari Boumediene, 2013.

[3] D.Boubiche ,Une approche inter-couches(cross-layer) pour la sécurité dans les R.C.S.F , université de Batna .

[4] N. Labraoui , La sécurité dans les réseaux sans fil Ad Hoc , université de Tlemcen , 2012.

[5] A.Fares , Développement d'une bibliothèque de capteurs , université de Montpellier 2, 2008.

[6] A.Hadj Adda et W.Benallal , Mise en place d'un schéma de routage pour la tolérance aux pannes dans les RCSF , université de Tlemcen ,2014.

Résumé

Les réseaux de capteurs sans fil (RCSF) sont un type spécial de réseaux sans fil ad hoc dédié à une application particulière, telle que les applications environnementale, médicales, militaires et domestique. Ces applications ont souvent besoin d'un niveau de sécurité élevé.Cependant l'impossibilité d'une intervention humaine, a poussé les utilisateurs à s'intéresser à ces réseaux pour la surveillance et la sécurité de l'environnement ainsi la collection des données. Vu que les capteurs sont très limités en termes de ressource (CPU, stockage, énergie), qu'ils sont une proie facile aux compromissions, qu'ils fonctionnent sans assistance humaine, et peuvent être déployés dans des environnements ouverts et hostiles, les RCSF sont sujets à différents types de menaces et d'attaques. Dans ce mémoire, nous présentons l'évaluation de la librairie de sécurité TinySec dans les réseaux de capteurs sans fil : par la suite, notre application à la détection d'évènements critiques a pour but de tester, de valider et de simuler le fonctionnement du réseau et sa principale fonction est de vérifier le comportement des capteurs développés avant même de les avoir déployé en situation réel.

Mots clés : Réseaux de capteurs sans fils , sécurité des RCSF, Tinysec .

Abstract

Wireless Sensor Networks (WSN) are a special kind of network ad hoc wireless dedicated to a particular application, such as the environmental, medical, military and domestic. These applications often require a high level of security.However the impossibility of human intervention has pushed users to focus on these networks for surveillance and security of the environment and the collection of data. Since the sensors are very limited in terms of resources (CPU, storage, energy), they are easy prey to compromises, they operate without human assistance, and can be deployed in open and hostile environments, WSN are subject to different types of threats and attacks. In this paper, we present Evaluation of TinySec security library in wireless sensor networks: by following our application to the detection of critical events aims to test, validate and simulate the operation of the network and its main function is to check the behavior of developed even before the sensors have deployed in real situation.

Keywords: networks without son sensors WSN security, Tinysec .

ملخص

شبكات الاستشعار اللاسلكيةهي نوع خاص من شبكة مخصصة لاسلكية مخصصة لتطبيق معين، مثل البيئة والطبية والعسكرية والمحلية. وغالبا ما تتطلب هذه التطبيقات على مستوى عال من الأمن.

ومع ذلك استحالة التدخل البشري قد دفع المستخدمين إلى التركيز على هذه الشبكات لمراقبة وأمن البيئة وجمع البيانات. منذ أجهزة الاستشعار ومحدودة للغاية من حيث الموارد (وحدة المعالجة المركزية، والتخزين، والطاقة)، إلا أنها تعمل من دون مساعدةلحلول وسطويمكن نشرها في بيئات مفتوحة ومعاديةفهي فريسة سهلةتخضع لأنواع مختلفة من التهديدات والهجمات .

عن TinySecفي هذه المذكرة ، ونحن تعامل تقييم المكتبة الأمنيةفي شبكات الاستشعار اللاسلكية:WSN الكشف الأحداث الهامة يهدف إلى اختبار والتحقق من صحة ومحاكاة تشغيل الشبكة وظيفتها الرئيسية هي للتحقق من سلوك أجهزة الاستشعار المتقدمة قبل الوضع الحقيقي .

كلمات البحث: شبكات الاستشعار ، والسلامة.