République Algérienne Démocratique et Populaire

Ministère de l'Enseignement supérieur et de la recherche Scientifique

Université Abderrahmane Mira de Bejaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de Cycle Master 2 Informatique Professionnel Option: ASR
Administration et Sécurité des Réseaux

Thème
Implémentation d'un protocole d'élection d'un serveur d'authentification dans l'internet des Objets

Le jury est composé de :

Encadreur : Ms El Sakaan Nadim

Président : Mr Atmani Mouloud

Examinateur : Mr Kadjouh Nabil

Examinatrice : Mlle Bouchelaghem Siham

Réalisé par :

Mr Hidjeb Ali

Promotion 2016/2017

« Remerciements »

Louange à Dieu le tout puissant, le miséricordieux, sans lui rien de tout cela n'aurait pu être.

Nous exprimons notre vive reconnaissance à notre encadreur El SAKKAN Nadim pour ses précieux conseils, ses orientations, sa disponibilité, sa sympathie et le temps qu'il nous a consacré, Nous sommes reconnaissants.

Nous remercions chacun des membres du jury pour l'intérêt porté à notre travail en acceptant de l'examiner et de l'enrichir avec leurs propositions.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis qui nous ont soutenu et encouragé tout au long cursus universitaire et de la réalisation de ce mémoire.

Merci à toutes et à tous.

Dédicaces

A ma mère et mon père, je suis vraiment reconnaissant a votre aide et vos sacrifices et soutien dans mon parcours, à ma très chère sœur, à Redha qui nous a beaucoup aidé à réaliser ce travail, a tous mes amis et ma fiancée Sabrina.

Merci

Ali

Table de figure

AMQP Advanced **M**essage **Q**ueuing **P**rotocol

ARPANET Advanced **R**esearch **P**rojects **A**gency **N**etwork

CoAP Constrained **A**pplication **P**rotocol

DNS Domain **N**ame **S**ystem

DNSSEC Domain **N**ame **S**ystem **S**ecurity **E**xtensions

DoS Denial **O**f **S**ervice

ECC Elliptic **C**urve **C**ryptography

EPC Electronic **P**roduct **C**ode

EPCIS Electronic **P**roduct **C**ode **I**nformation **S**ervices

ETSI European **T**elecommunications **S**tandards **I**nstitute

GPS Global **P**ositioning **S**ystem

HTTP HyperText **T**ransfer **P**rotocol

HTTPS HyperText **T**ransfer **P**rotocol **S**ecure

HVAC Heating, **V**entilation and **A**ir-**c**onditioning

IEEE Institute of **E**lectrical and **E**lectronics **E**ngineers

IETF Internet **E**ngineering **T**ask **F**orce

IdO Internet **d**es **O**bjets

Ipv6 Internet **P**rotocol **v**ersion 6

IoT Internet **o**f **T**hings

ITU International **T**elecommunication **U**nion

LEACH Low-**E**nergy **A**daptive **C**lustering **H**ierarchy

LLN Low power **L**ossy **N**etworks

LS Specialty **l**ine

MQTT Message **Q**ueue **T**elemetry **T**ransport

M2M Machine **T**o **M**achine

ONS Object **N**aming **S**ervice

PIR Private **I**nformation **R**etrieval

P2P Peer-**t**o-**p**eer

RBAC Role-**B**ased **A**ccess **c**ontrol

REST Representational **S**tate **T**ransfer

RFID Radio **F**requency **I**dentification

RPL Routing **P**rotocol for **L**ow power and **L**ossy Networks

RSA Rivest, Adi **S**hamir et Leonard **A**dleman

SOAP Simple **O**bject **A**ccess **P**rotocol

TCP/IP Transmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol

TLS Transport **L**ayer **S**ecurity

UDP User **D**atagram **P**rotocol

URI Uniform **R**esource **I**dentifier

VPN virtual **p**rivate **n**etwork

WM-RSA Wireless sensor **M**ote **R**ivest, Adi **S**hamir et Leonard **A**dleman

WSN Wireless **s**ensor **n**etworks

W3C World **W**ide **W**eb **C**onsortium

XMPP Extensible **M**essaging and **P**resence **P**rotocol

6loWPan IPv6 LoW **P**ower **W**ireless **A**rea **N**etworks

Introduction Générale

L'internet des objets a été introduit pour la fois par kevin ashton. Il désigne l'omniprésence autour de nous d'une variété d'objets qui, à travers des schémas d'adressage uniques, sont capables d'interagir les uns avec les autres et de coopérer avec leurs voisin pour atteindre des objectifs communs. Les objets intelligents, qui sont considéré comme la plateforme de base de l'IOT, sont les objets de la vie quotidienne (réfrigérateur, téléviseur….etc.). Ces objets son équipés de composants électronique tels que des supports de communication radio, des processeurs pour le traitement, des capteurs et/ou actionneurs etc. Cet ajout vise à les rendre capables d'être conscient du monde dans lequel ils se trouvent et de prendre son contrôle à un instant donné. Grace à ses potentialités et son aspect ubiquitaire, la montée en puissance de l'IOT peut s'observer dans plusieurs domaines des plus personnelles aux plus industrielles. Ceci a conduit à des bénéfices énormes, meilleur gestion d'énergie, traçabilité des produits, amélioration du suivi de la santé, simplification des taches quotidiennes, etc.

Néanmoins, l'IOT n'est qu'en ses début, plusieurs progrès restent à faire en matière de standardisations, de routage et d'identification, d'optimisation de la consommation d'énergie et surtout de sécurité. En effet, l'omniprésence de l'internet des objets dans la vie quotidienne des individus impose l'établissement des solutions de sécurité robustes respectant l'hétérogénéité des objets et leurs capacités limitées. Cette forte intégrité engendre non seulement les menaces classiques d'attaque qui présente sur les données et les réseaux, mais aussi, l'apparition de nouvelles menaces qui touchent à l'intégrité des objets eux-mêmes, les infrastructures et processus ainsi que privacy des personnes.

Ce mémoire est organisé en trois chapitres. Le premier chapitre sera consacré à la présentation de l'internet des objets, ainsi que l'introduction de quelques notions fondamentales utilisées dans le domaine de l'IOT. Dans le deuxième chapitre, nous l'avons consacré pour la conception. Nous commencerons d'abord par la définition de l'authentification et l'explication du principe qu'on a utilisé pour le déroulement de notre simulation. Ensuite, nous présenterons le principe de l'élection. Dans le troisième chapitre nous l'avons consacré pour la réalisation, c'est-à-dire, l'implémentation d'un protocole d'élection d'un serveur d'authentification dans l'internet des objets.

1.1 Introduction

L'Internet des Objets (l'IoT) repose sur l'idée que tous les objets peuvent être connectés à Internet et sont donc capable d'émettre de l'information et éventuellement de recevoir des commandes, il n'existe pas de définition standard, unifiée et partagée de l'internet des objets. Certaines techniques de l'IoT, tandis que l'autres se concentrent plutôt sur les usages et les fonctionnalités. Il faut réussir à exprimer ce que représente l'internet des objets tout en restant accessible aux non experts, et suffisamment concert pour représenter son impact dans la vie quotidienne. L'IoT désigne une information qui se fond dans notre quotidien pour nous simplifier la vie.

Dans ce chapitre, nous présentons l'IDO ou bien IoT (Internet of things) définition, domaine d'application , son architecture , ses axes de recherche, ainsi que les vulnérabilités et les menaces relatives à son déploiement, ainsi que le fonctionnement de l'IoT , et nous consacrons par la suite le reste du chapitre à la définition de bases , et quelques notions utilisées dans le domaine de la sécurité.

1.2 L'internet des objets

1.2.1 Définition

L'internet des objets représente l'extension d'internet à des choses et à des lieux du monde physique. Cela a permet à toute l'humanité de plonger dans les profondeurs de l'internet et des recherches ses mystères pour devenir l'un des outils indispensables dans notre vie quotidienne. Ainsi, son utilisation a touché tous les aspects de la vie quotidienne [1].

L'internet des objets est définit par l'union international des télécommunications comme une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'informations et de la communications interopérables existantes ou en évolution et cela vu dire que l'internet des objets est apparu dans le cadre d'une direction issue de la mécanisation et standardisation , appliquée à l'automatisation du traitement du document et de l'information . Sur support matériel puis numérique.

Il représente les échanges d'informations et de données provenant de dispositifs présents dans le monde réel vers le réseau internet. Aussi l'internet des objets représente les échanges d'informations et de données provenant de dispositifs présents dans la réalité vers le réseau internet. Il est considéré comme la troisième évolution de l'internet, baptisée web 3.0 qui fait suite à l'ère du web social [1]. Surtout avec l'ajout d'une connexion internet qu'à donné une valeur supplémentaire en terme de fonctionnalité, d'information, d'interaction avec l'environnement ou d'usage.

L'internet des objets responsable d'un accroissement exponentiel du volume de donnée généré sur le réseau à l'origine du big data. Alors l'ido est considéré comme un concept ayant des répercussions sur les technologies et la société [2].

Il est considéré le réseau de réseaux qui permet via des systèmes d'identification électronique, et des dispositifs mobiles sans fil, d'identifier des entités numériques et des objets, physiques, et du récupérée, stocker, transférer et traiter entre les mondes physiques et virtuels. Il est le système des systèmes et pas juste le réseau des réseaux. Parfois l'objet deviendra un acteur autonome de l'internet, capable de percevoir, analyser et d'agir selon les contextes engagé, et cela vu dire que l'avènement de l'internet des objets liées à celui des technologies ou méthodes logicielle liées à l'intelligence artificielle, et des sciences de la complexité [2].

1.2.2 Domaine d'application de l'internet des objets

Le marché des objets connectés est promis à une grande croissance dans les années à venir car il a une valeur immense dans les différents domaines d'objets connectés pour les professionnels. Cependant, seules quelques applications sont actuellement déployées [2].

L'utilisation de l'IDO permettra le développement de plusieurs applications intelligentes qui toucheront essentiellement ceux qu'on citera dans ce qui suit, nous citrons brièvement des exemples d'applications de l'IDO [3].

a- L'internet des objets dans le domaine de la santé

Les objets connectés peuvent servir à réduire quelque éléments de dépenses pour les remplacer par d'autrs il permet aussi de favoriser l'hospitalisation à domicile, qui assurera le contrôle et le suivi des signes cliniques des patients par la mise en place des réseaux personnels de surveillance, ces réseaux seront constitués de bio-captures posés sur le corps des patients ou dans leurs lieux d'hospitalisation. Cela facilitera la télésurveillance des patients qui permettras de réduire les erreurs médicales, optimiser la consommation de médicaments ou encore leur prise régulière, et même encourager la prévention de certaines maladies, l'internet des objets permettre aussi de suivre sa tension, son rythme cardiaque, la qualité de sa respiration ou encore sa masse graisseuse, et d'autres objets connectés médicaux , brosse a dent connectée ou encore, le scanner qui calcule le nombre de calories dans votre assiette[4].

b- L'internet des objets dans le domaine des sportifs :

De nombreux objets connectés comme des montres ou des bracelets connectés vous permettrons pendant la journée de calculer le nombre de pas effectuée, la distance par courue, votre temps d'activités, les calories brulées, ainsi pendant la nuit en calculant vos heurs de sommeil. Pour les passionnés de High-tech, c'est un grand marché qui s'ouvre à eux ! De la montre connectée au téléviseur connecté en passant par les appareils photos, les montre, les drones, les lunettes (Google glass)[6].

c- L'internet des objets dans le domaine domotique

Les objets connectés sont une réelle révolution, ils permettent de la rendre connectée, d'où le nom très utilisé de smart home des nombreux dispositifs de sécurité détecteur de fumée, surveillance, serrure connecté dans le domaine de l'électroménager réfrigérateur connecté, l'électroménager connecté. De la décoration de la maison des designs, lampe connecté, cadre lumineux, plante connecté. L'internet des objets change les modalités d'accès au réseau et produit de nouvelles interactions homme-machine.

Il existe aussi des villes intelligente (Smart Caties) est utiliser pour désigner l'écosystème cyber physique émergeant par le déploiement d'une infrastructure de communication avancée et de nouveaux services sur des scénarios à l'échelle de la ville. Grace à des services avancés, il est en effet possible d'optimiser l'utilisation des infrastructures physiques de la ville (par exemple, les réseaux routiers, le réseau électrique, etc.) et la qualité de vie des citoyens [7].

d- L'internet des objets dans le domaine de L'automobile

Le marché des transports à déjà anticipé l'arrivée des objets connectés. Parmi les enjeux les plus fréquents que ce domaine fait naitre on retrouve la réduction des accidents et des embouteillages, le partage de voitures, le développement des offres de VTC et de TAX ou encore la gestion des flots automobile [7].

e- L'internet des objets dans le domaine de la sécurité

Pour le cabinet en stratégie, ces entreprises vont rapidement se positionner comme des alliés des personnes qui résident dans leur domicile. En fournissant des données relatives à la consommation d'énergie aux foyers, ces groupes vont apparaitre comme des arguments contre le facteur EDF pour les fournisseurs d'énergie la précision sera difficile à tenir car ils seront probablement contraints d'accompagner leurs clients dans une baisse de leurs facteurs énergétique [8].

f- L'internet des objets dans le domaine de l'industrie

Le déploiement de L'IoT dans l'industrie sera certainement un grand support pour le développement de l'économie et le secteur des services, puisque L'IDO permettra d'assurer un suivi total des produits, de la chaine de production, jusqu'à la chaine logistique et de distribution en supervisant les conditions d'approvisionnements. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers.

Certains éditeurs tels que SAP et CISCO montrant d'ores et déjà comment certaines zones industrielles comme le port d'Hambourg ont pu être équipés en pucs et autres objets connectés. L'internet couvre un énorme nombre d'industries et utilise des cas qui s'étendent d'un seul dispositif contraint aux déploiements croisés de technologies intégrées de systèmes Cloud connectés en temps réel.

g- L'internet des objets dans le domaine de l'agriculture

L'IoT présentera des outils de choix pour la supervision de l'environnement des cultures, ce qui permettra une meilleure aide à la décision en agriculture. L'IoT servira non seulement à optimiser l'eau d'irrigation, l'usage des intrants et la planification des travaux agricoles, mai aussi, cette technologie peut être utilisée pour lutter contre la pollution (l'air, le sol et les eaux) et améliorer la qualité de l'environnement en général.

L'usage des objets connectés se démocratise dans l'agriculture. De nombreuses amélioration ou découlent la gestion des engins agricoles, la maitrise de l'irrigation ou la gestion optimisée des intrants, que la surveillance de la croissance des plantes ou encore la prévention des risques météo. De quoi renouveler en profondeur les pratiques des cette activité ancestrale, grâce à l'analyse des données récoltées et au pilotage de plus en plus fin des exploitations [9].

1.2.3 Architecture de l'internet des objets

Des la fin des années 1990, le développement de l'internet Protocol version 6 (IPV6) a permis d'envisager l'internet des objets (ou internet of things) l'enjeu était déjà de disposer d'une quantité d'adresses IP suffisante pour connecter des objets de consommations à Internet. Pas de Pile de communication depuis lot-A initiative.

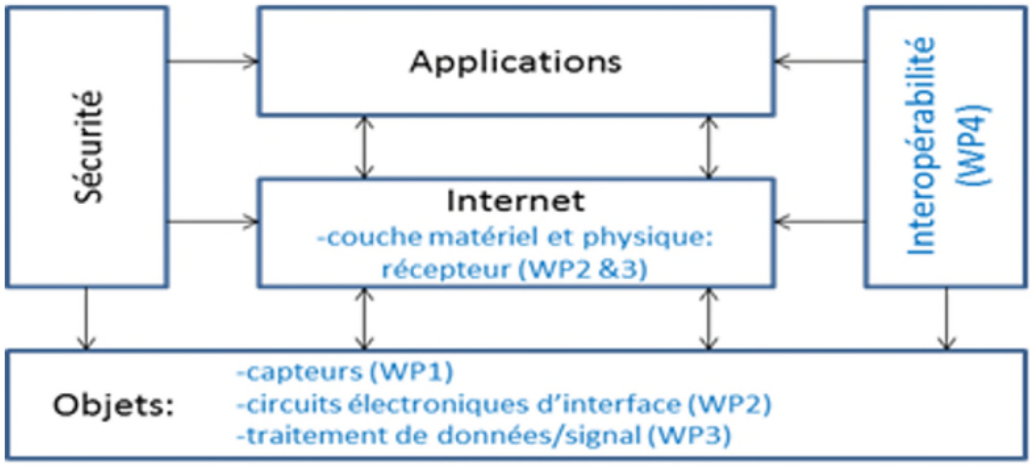
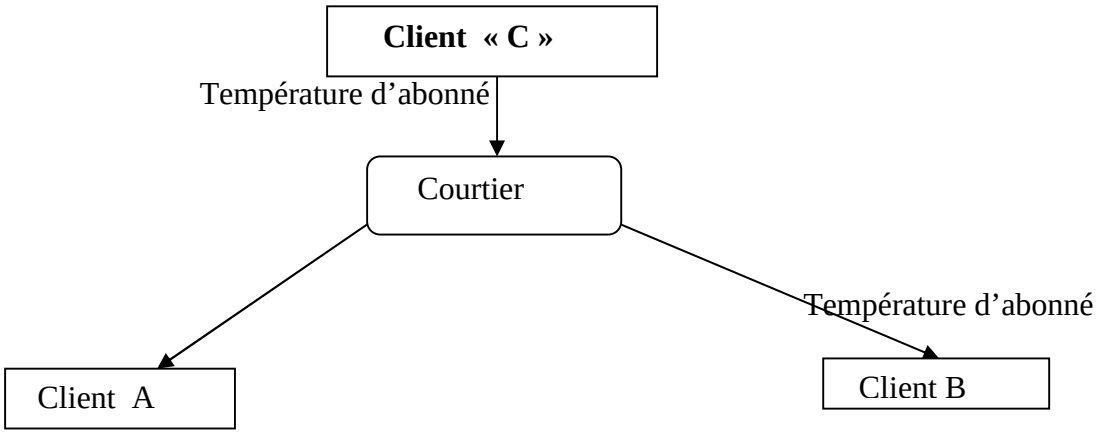
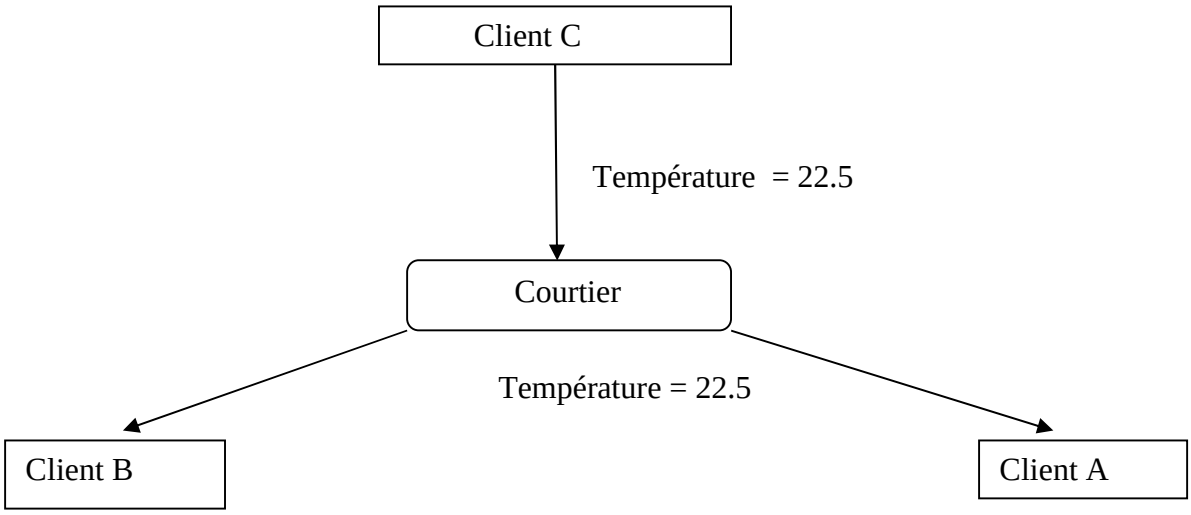


Figure 1 : Lot de communication [2].



Plus tard, le client « A » publie une valeur de 22,5 pour la température du sujet le courtier transmet le message à tous les clients souscrits.



MQTT (Message Queue Telemetry) à un modèle client, serveur, où chaque capture est un client et se connecte à un serveur connu sous le nom de courtier, sur TCP. Le MQTT est orienté vers les messages chaque est un morceau discret de données pour le courtier, chaque message est publie sur une adresse connu sous le nom de sujet les clients peuvent s'abonner à plusieurs sujets, chaque client souscrit à un sujet reçoit chaque message publié sur le sujet par exemple, imaginez un réseau simple avec trois clients et un courtier centrale. Les trois clients ouvrent des connexions TCP avec le courtier, les clients B et C s'abonnent à la température du sujet. [2] Le modèle d'abonné de l'éditeur permet aux clients MQTT de se communiquer individuellement, un à plusieurs et plusieurs à un. Correspondance des thèmes dans MQTT, les sujets sont hiérarchiques comme un système de classement (cuisine, four, température) les caractères génériques sont autorisés lors de l'enregistrement d'un abonnement mais pas hors de la publication, permettant d'observer les hiérarchies entières par les clients.

1.2.3.1 Architecture et Standardisation

Les racines de l'IDO remontent aux technologies M2M (machine à machine) pour le contrôle des processus à distance. L'IDO qui est aujourd'hui un mélange de plusieurs technologies telles que la RFID, NFC, les capteurs et actionneurs sans fil, le M2M, l'ultrage bande ou 3/4G, IPv6, et RPL nécessite la définition d'une architectures et des standards afin de facilité son développement dans le future. L'ETSI propose une architecture découpée e trois domaines distinct, le domaine du réseau d'objets, le domaine du réseau cœur d'accès et le domaine des applications M2M et applications clients. [3]

1.2.3.2 Le domaine du réseau d'objet s

Dans ce domaine nous trouvons les différentes technologies d'interconnexion des objets M2M, RFID, Bluetooth, IETF6L low PAN, IETFRPL et des passerelles vers les réseaux cœur de transport. [3]

1.2.3.3 Le domaine du réseau cœur d'accès

Dans ce domaine nous trouverons les différentes technologies de réseaux de transport et d'accès comme xDSL, WIMAX, WLAN, 3/4G, etc. [6]

1.2.3.4 Le domaine des applications M2M et applications clientes

Ce domaine est composé de plateformes M2M, les Middlewares et API des applications M2M, processus métiers exploitant l'IDO, etc.

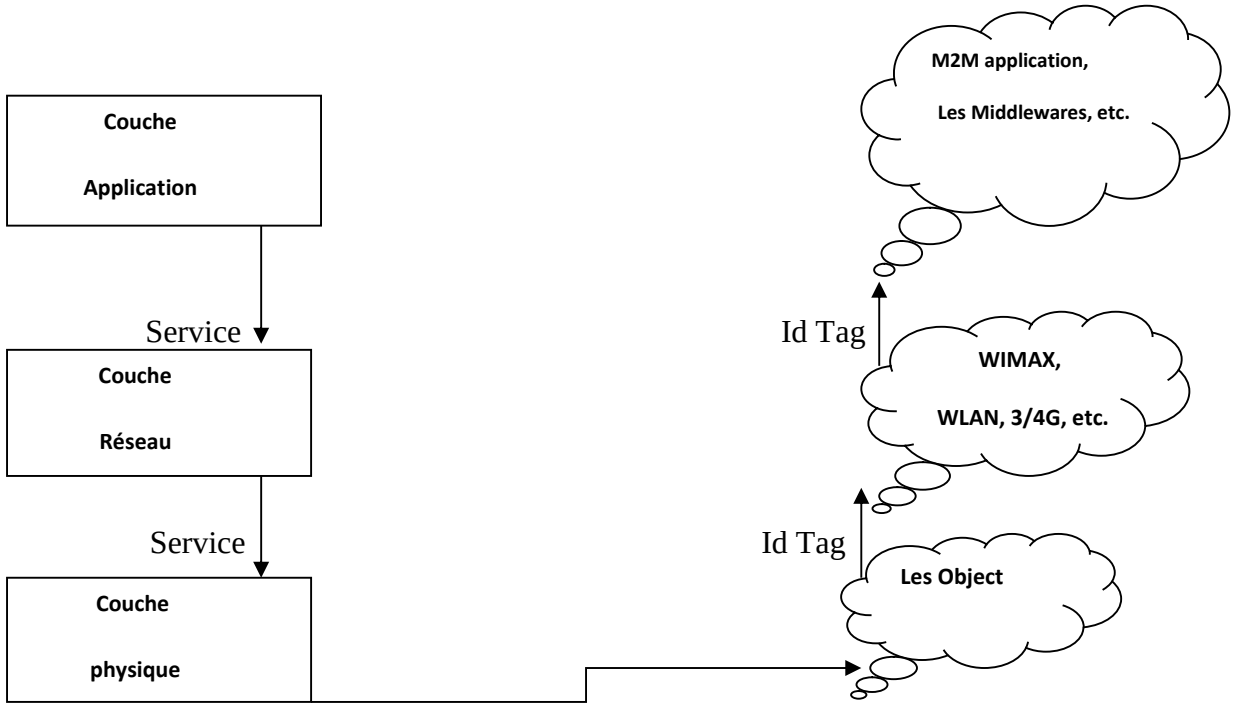


Figure 2 : Architecture de L'internet des Objets. [6]

1.2.4 Fonctionnement de L'IOT

Si certain objets fixes peuvent être connectés par des réseaux filaires, la croissance de l'internet des objets devrait majoritairement être portée par l'utilisation de technologies sans fil et mobiles. Les technologies de connectivité sans fil sont nombreuses et variées, et l'usage de l'une ou l'autre est souvent avant tout décidé par la portée du réseau envisagé. Certains cas d'usage nécessitent également l'association de technologies sans fil et filaire pour relier les équipements à des réseaux privés étendus ou à Internet.

Un point saillant des développements technologiques actuels autour de l'internet des objets à trait au bouleversement de la dichotomie classique dans le monde des fréquences être, d'une part ,des technologies à courte portée opérant en bandes libre souvent foisonnantes et déployées par l'utilisateur lui-même et, d'autre part, des technologies à grande portée opérant en bande de fréquence soumise à autorisation préalable sous licence, déployées par un nombre réduit d'opérateurs. [8]

Le développement de réseaux à bas débit et longue portée, en bandes libres, entraine ainsi un foisonnement d'initiatives et de développement.

1.2.4.1 Technologies de l'IOT

L'IOT permet l'interconnexion des différents objets intelligents via l'Internet. Ainsi, pour son fonctionnement, plusieurs systèmes technologiques sont nécessaires. L'IOT désigne diverses solution techniques (RFID,TCP/IP, technologies mobiles, etc.) qui permettent d'identifier des objets , capter , stocker, traiter, et transférer des données dans les environnement physiques, mais aussi entre des contextes physiques et des univers virtuels. [7]

En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IOT, nous mettons l'accent seulement sur quelques-unes qui sont, selon Han et Zhongshan, les technologies clés de l'IOT. Ces technologies sont les suivantes : RFID,WSN et M2M, et elles sont définies ci-dessous.

RFID : est une technologie sans fil qui est utilisée pour l'identification des objets, elle englobe toutes les technologies qui utilisent des ondes radio pour identifier automatiquement des objets ou des personnes. C'est une technologie qui permet de mémoriser et de récupérer des informations à distance grâce à une étiquette qui émet des ondes radio. Il s'agit d'une méthode utilisée pour transférer les données des étiquettes à des objets, ou pour identifier ces objets à distance. L'étiquette contient des informations stockées électroniquement être lues à distance [7],[10] .

WSN : est un ensemble de nœuds qui communique sans fil et qui sont organiser en un réseau coopératif. Chaque nœud possède une capacité de traitement et peut contenir différent type de mémoire, un émetteur-récepteur RF et une source d'alimentation. Il peut aussi tenir compte des divers capteurs et actionneurs. Constitue un réseau de capteurs sans fil qui peut être une technologie nécessaire au Fonctionnement de l'IoT. [7]

M2M : est l'association des technologie de l'information et de la communication avec des Objets intelligents dans le but de donner à ces derniers les moyens d'interagir sans intervention humaine avec le système d'information d'une organisation d'une organisation ou d'une entreprise . [7], [10]

1.2.4.2 Composants de l'IoT

L'IoT n'est pas une technologie, mais un système ou l'intégration de tous les composants induit une complexité que l'interopérabilité diminue mais n'évite pas. La gestion des interfaces y est déterminante [7], [9].

Voici les principaux systèmes technologiques nécessaires au fonctionnement de l'IoT :

1. **Type de systèmes :** Identification, **Les Enjeux** c'est de reconnaitre chaque objet de façon unique et recueillir les données stockées au niveau de l'objet. **Les Technologies Anciennes** c'est les Codes barres, solution RFID simple. **Et Technologie Récente** sont Solution RFID complexes, Surface Acoustique Waves, puces optique, ADN
2. **Type de systèmes :** Capteurs, **Les Enjeux** c'est de Recueillir des informations présentes dans l'environnement pour enrichir les fonctionnalités du dispositif. **Les Technologies Anciennes** c'est le Thermomètre, Hydromètre. **Les Technologie Récente** sont les Capteurs miniaturisés nanotechnologies.
3. **Type de systèmes :** Connexion, **Les Enjeux** C'est de Connecter les systèmes entre eux. Et **les Technologies Anciennes :** Câbles … etc. Et **Les Technologie Récente** c'est le Bluetooth, Near Field Communication (NFC), Wi-fi …etc.
4. **Type de systèmes :** Intégration. **Les Enjeux** c'est Intégration les systèmes pour que les données soient transmises d'une couche à l'autre. **Les Technologies Anciennes** C'est le Middlewares. Et **les Technologie Récente** sont Middlewares évolués.
5. **Type de systèmes :** traitement de données. **Les Enjeux** c'est de stocker et analyser les données pour aider à la prise de décisions. **Les Technologies**

Anciennes sont Excel, ERP, CRM. Et **les Technologie Récente :** Datawarehouse 3D compatible avec les puces RFID, Web sémantique…

6. **Type de systèmes :** Réseaux. **Les Enjeux** C'est de Transférer les données dans les mondes physiques et virtuels. **Les Technologies Anciennes** on citera L'internet, Ethernet… Et **Les Technologie Récente** C'est Réseau EPC global.

Lier un objet ou un lieu à internet est un processus plus complexe que la liaison de deux pages Web. L'IOT exige sept composants :

Une étiquette physique ou virtuelle pour identifier les objets et les lieux. Quelques systèmes d'étiquetage sont décrits ci-dessous. Pour permettre aux barquées dans des marqueurs visuels.

Un moyen de lire les étiquettes physiques, ou de localiser les étiquettes virtuelles.

Un dispositif mobile tel qu'un téléphone cellulaire, un assistant personnel ou un ordinateur portable.

Un logiciel additionnel pour le dispositif mobile.

Un réseau sans fil de type 2G, 3G ou 4G afin de permettre la communication entre le dispositif portable et le serveur contenant l'information liée à l'objet étiquette.

L'information sur chaque objet lié. Cette information peut être contenue dans les pages existantes du Web, les bases de donnée comportant des informations de type prix, etc.

Un affichage pour regarder l'information sur l'objet lié. A l'heure actuelle, il est probable que ce soit l'écran d'un téléphone mobile [3],[9].

1.2.4.3 protocoles de fonctionnement de L'IOT

De nombreuses normes IOT sont proposées pour faciliter et simplifier les taches des programmeurs d'applications et des fournisseurs de services. Différents groupes ont été créée pour fournir des protocoles, y compris les efforts menés par le W3C, IETF, EPC global, IEEE et l'ETSI [3].

L'IOT ambitionne de faire communiquer chaque système avec tous autres au moyen de protocoles communs. La mise en application à une large échelle du concept d'IOT apparait largement tributaire d'une standardisation de la communication entre objets dite M2M.

- Au niveau de la couche de liaison, le standard **IEEE 802.15.4** est plus adapté que l'Ethernet aux environnements industriels difficiles.
- Au niveau réseau, le standard 6loWPan a réussi a adapter le protocole IPV6 aux communication sans fil entre nœud a très faible consommation.
- Au niveau routage, l'IETF a publié en 2011 le standard RPL.
- Au niveau de la couche application le protocole CoAP qui tente d'adapter http, beaucoup trop gourmand aux contraintes des communications entre nœuds à faible consommation [11].

1.2.4.4 CoAP (Constrained Application Protocol)

Est un protocole de couche D'application pour les applications IOT. Il d´définit un protocole de transfert Web Basé sur les fonctionnalités HTTP, est lié à UDP (et non TCP) par d´défaut qui le Rend plus approprié pour les applications IOT. En outre, CoAP modifie certaines Fonctionnalités HTTP pour répondre aux exigences de l'IOT telles que la faible Consommation d'´energie et le fonctionnement en présence de liens `a perte et Bruyants.

CoAP a été conçu sur la base de REST qui représente un moyen plus Simple d'échanger des données entre les clients et les serveurs via HTTP. REST Peut être considéré comme un protocole de connexion qui repose sur L'architecture sans serveur apatride. Il est utilisé dans les applications de réseaux Sociaux et mobiles et élimine l'ambigu¨ıt´e en utilisant les méthodes HTTP get, post, put et delete. Il permet aux clients et aux serveurs d'exposer et de consommer Des services Web comme le protocole d'accès aux Objets simples (SOAP), mais de Manière plus simple en utilisant les identificateurs de ressources uniformes (URI). CoAP vise à permettre à de minuscules appareils `a faible puissance, le calcul et Les capacités de communication `a utiliser les interactions RESTful. Avec CoAP, Les interactions entre services web de l'Internet des PC et de l'Internet des Objets Deviennent bien plus simples à réaliser, une passerelle applicative assez légère Correspondance entre les commandes REST et CoAP se charge de l'adaptation D'un monde à l'autre [11],[7].

1.2.4.5 MQTT Message Queue Telemetry Transport

Représente un protocole De messagerie idéal pour les communications IOT et M2M. Il vise à connecter des périphériques et des réseaux intégrés aux applications et au middleware. MQTT Utilise le modèle de publication souscription pour offrir une flexibilité de transition Et une simplicité d'implémentation. Il convient aux périphériques à ressources Limitées qui utilisent des liens peu fiables ou à faible bande passante. MQTT est Construit en haut du protocole TCP. Il se compose de trois composants, abonnés, éditeurs et courtiers. De nombreuses applications utilisent MQTT telles que les Soins de santé, la surveillance, le compteur d'´energie et la notification de Facebook. Par conséquent, le protocole MQTT permet d'acheminer les périphériques de petite taille, à faible consommation et à faible mémoire dans des zones vulnérables et Réseaux à faible bande passante [7].

1.2.4.6 XMPP (Protocole de messagerie et de présence extensible)

XMPP Est une Norme de messagerie instantanée IETF (IM) qui est utilisé pour les conversations Multipartis, les appels vocaux et vidéo et la télé présence. Il permet aux utilisateurs De communiquer entre eux en envoyant des messages instantanés sur Internet quel Que soit le système d'exploitation qu'ils utilisent. XMPP permet aux applications De messagerie instantanée d'accéder `a l'authentification, au contrôle d'accès, à la Mesure de la confidentialité, au cryptage hop-by-hop et à la compatibilité avec D'autres protocoles. Beaucoup de fonctionnalité XMPP en font un des protocoles Préfères par la plupart des applications de messageries instantanées et pertinentes Dans le cadre de l'IOT. Il fonctionne sur une vari´et´e de plateformes basées sur Internet de manière décentralisé. XMPP est sécurisé et permet d'ajouter de Nouvelles applications au-dessus des protocoles de base.

1.2.4.7 AMQP (Message avancé Protocole de mise en file d'attente)

AMQP Est un Protocole de couche d'application standard ouvert pour l'IOT se concentrant sur des Environnements axés sur les messages. Il requiert un protocole de transport sécurisé

Comme TCP pour échanger des messages. Il prend en charge une communication Fiable via des primitives de garantie de livraison de messages, en définissant un protocole Au niveau du fil, les implémentations AMQP peuvent inter opérer entre elles. Les communications sont traitées par deux composants principaux :

- Échanges et files d'attente de messages. Les échanges sont utilisés pour acheminer les messages vers les files d'attente appropriées.

- Le routage entre les échanges et les files d'attente des messages repose sur certaines règles et conditions prédéfinies. Les messages peuvent être stockés dans les files d'attente, puis envoyés au récepteur par la suite. AMQP prend également en charge le modèle de communication publié.

1.2.5 Axes de Recherche

1.2.5.1 La standardisation

L'IDO tel qu'il est aujourd'hui manque de standards et de certification commune qui permettent d'assurer une compatibilité entre objets connectés tournant sous différents écosystèmes, une telle initiative joueras un rôle très important dans le développement de l'IDO dans le future, puisqu'elle offre des solution pour l'amélioration de l'interopérabilité et permet de produits ou à des services de concurrencer à un niveau plus élevé, Malheureusement, les Travaux de Recherche des standards qui peuvent tenir face aux problèmes de l'interopérabilité, d'accès aux support radio, d'interopérabilité sémantique, d'assurance de la sécurité et de la privacy sont confrontés aux problèmes de la croissance rapide de l'IDO qui constitue un vrais souci dans les processus de standardisation [5],[6].

1.2.5.2 La sécurité et la protection de la privacy

Le niveau d'acceptation des nouvelles technologies et services offert par l'IDO au niveau de la société est fortement lié au degré de fiabilité des informations et de protection des données privées des utilisateurs. Bien que plusieurs projets aient été lancés dans le but de trouver des solutions adéquates pour la protection de la privacy et d'assurer une protection rigoureuse aux utilisateurs finaux à la confidentialité, la privacy et la gestion de la confiance [6].

1.2.5.3 La nouveauté dans les environnements de l'IDO

L'IdO est un réseau complexe géré par plusieurs parties prenantes, dans lequel certains services doivent être fournis publiquement, par conséquent, de nouveaux services ou applications verront le jour, ces derniers doivent être retenus dans le marché sans créer de charges excessives ou autres barrières de fonctionnement [5].

1.3 Vulnérabilités et menaces dans l'internet des Objets

A cause de la forte intégration de l'IOT, les objets du quotidien deviennent des risques potentiels d'attaque sur la sécurité, l'ubiquité de L'IoT amplifiera les menaces classiques de la sécurité qui pèsent sur les données et les réseaux, de plus l'apparition de nouvelles menaces qui toucheront directement à l'intégrité des objets eux-mêmes, les infrastructures et processus et la privacy des personnes [6].

1.3.1 Menaces sur les données et les réseaux

Le manque de surveillance et de protection physique des objets communicants peut en gendres des attaques potentielles portées sur le matérielle telles que le vole, la corruption ou la contrefaçon de ces derniers pour récupération des données qui sont stockées sur ces dispositifs ou pour interrompre le bon fonctionnement des réseaux ou les systèmes complexes les hébergent.

De plus, les transmissions sans fil sont réputées par leur forte vulnérabilité aux attaques de l'écoute passive et de déni de service. Les solutions cryptographiques existantes aujourd'hui ne sont pas adéquates pour tenir faces à ces problèmes cités à cause de la limitation de ressources des objets communicants, de ce fait, l'adaptation de ces dernières ou

la conception de nouveaux modèles est une nécessité a fin d'assurer les services de sécurité [5] .

1.3.2 Menaces sur la privacy

De nombreux objets seront intégrés, portés ou même bien installés dans les lieux privés des personnes, ces objets présentent une potentielle menace pour la vie privée (privacy) de leurs utilisateurs. En effet, ces appareils électrique non seulement sont traçables, mais peuvent filmer, écouter ou même enregistrer leurs rythmes cardiaque ou respiratoire ainsi que la température du corps ou sa cinématique dans le but d'un malicieux [6].

1.3.3 Menaces sur les systèmes et l'environnement physique des objets

Des objets malicieux connectés à un réseau ou intégrés dans un systéme complexe peuvent causer un dysfonctionnement quelconque,, un déni de service ou autres types d'attaques à l'intégrité des données et les informations sensibles du système, ou pire encore prendre le contrôle du système en causant des importants [6].

1.4 La sécurité dans internet des objets

1.4.1 Définition des objectifs de la sécurité

La sécurité informatique d'une manière générale consiste à assurer que les ressources matérielles et logicielles d'une organisation sont uniquement dans le cadre prévu. Elle vise à assurer plusieurs objectifs, dont les cinq principaux sont : L'authentification, L'intégrité, la disponibilité et la non-répudiation [6],[12].

1.4.1.1 Authentification

L'authentification peut être définie comme le processus de prouver une identité revendiquée. La confidentialité, l'intégrité des données, et la répudiation dépendent tous de l'authentification appropriée. Un système sans cette fonctionnalité ne pouvait pas fournir les objectifs de sécurité mentionnée de manière satisfaisante [12].

1.4.1.2 Confidentialité

Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données [12].

1.4.1.3 Intégrité

L'intégrité peut être vue comme un ensemble de mesures garantissant la protection des données contre les modifications et les altérations non autorisées. L'objectif des attaques sur l'intégrité est de changer, D'ajouter ou supprimer des informations ou des ressources [12].

1.4.1.4 Disponibilité

La disponibilité est un service réseau qui donne une assurance aux entités autorisées d'accéder aux ressources réseaux avec une qualité de service adéquate. L'objectif des attaques sur la disponibilité est rendre le système inexploitable ou inutilisable [12] .

1.4.1.5 Non-répudiation

Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire, c'est-à-dire au des correspondants ne pourra nier l'envoi ou la réception du message [12], [6].

1.5 Conclusion

Dans ce premier chapitre nous avons définis L'IOT, Nous avons cité brièvement les domaines d'application de l'internet des objets. Par la suite nous avons parlé de l'architecture de l'IOT, et son fonctionnement ou nous avons cité ses technologie, ses composantes et quelques protocole de fonctionnement, et nous avons cité les axes de recherche et nous avons décrit en détail dans cette partie les menaces et les vulnérabilités relatives à sont déploiement.

Dans le prochain chapitre nous expliquons le principe de l'élection et l'authentification.

2. Introduction

Actuellement, le problème de contrôle d'accès est très important dans plusieurs applications, le contrôle d'accès physique consiste à vérifier si une entité demande d'accéder aux droits nécessaires pour le faire. Les protocoles de vérification d'identité qui permettent l'accès s'appellent les protocoles d'authentification.

Au cours de ce deuxième Chapitre on va expliquer l'essentiel de notre travail , Nous allons expliquer en détail le principe de l'authentification d'un capteur au près d'un serveur, et comment ce fait l'élection entre les capteurs d'un nœud.

Ce chapitre est divisé en deux parties, la première sera consacrée à la présentation, du principe d'authentification dans le but d'établir des clés secrètes dans l'IOT. Pour cela, nous commençons d'abord par l'explication du protocole d'authentification. Par la suite, nous présenterons le protocole utilisé. En fin de cette première partie, La seconde partie est une introduction sur le concept de l'élection et des algorithmes d'élection.

2. 1 Authentification

Plusieurs obstacles importants restent à combler pour la réalisation de la vision de l'IoT dont le principal est la sécurité. La plupart des études et recherches Tendent à rendre leurs solutions applicables et utiles. Dans le domaine de la sécurité, Les chercheurs ont proposé diverses solutions pour permettre des communications Sécurisées entre les objets.

Dans l'IoT, appareils et capteurs communiquent ensemble directement par le world wide web et avec n'importe quelle application. Réduire la surface d'exposition des objets connectés aux attaques est une tache complexe. Elle requiert une Connaissance architecturale de la chaine de valeur qui relie les objets au cloud. Il Faut s'intéresser aux objets eux-mêmes, à leurs capteurs et processeurs, aux réseaux Locaux et distants, aux protocoles de tout niveau, puis aux serveurs, à leurs logiciels Et aux traitements des données qui y sont réalisés. Les besoins sont bien connus depuis des années [7].

Les protocoles de vérification d'identité qui permettent l'accès s'appellent les protocoles d'authentification. Ils répondent aux deux questions suivantes: qui suis-je ? et Suis-je réellement l'entité que je suis en train de procéder ?

La réponse à cette première question est basée sur la reconnaissance ou l'identification de l'entité qui consiste à associer une identité à une entité, telle qu'une carte à puce ou tag. Concernant la deuxième question qui s'articule sur la vérification ou l'authentification de l'entité, elle donne une permission à une identité proclamée. En d'autre terme, elle consiste à identifier une entité à partir d'une ou de plusieurs caractéristiques [13,14].

2.1.1 Protocole d'authentification

2.1.1.1 Cryptographie à courbe elliptique

La différence des algorithmes de chiffrement à base de courbes elliptiques Par rapport aux algorithmes bas´es sur les entiers comme RSA ou El-Gamal est Que, pour les vaincre, il faut résoudre un problème de logarithme discret sur une Courbe elliptique est réputé être un problème plus difficile que le problème similaire Dans les entiers modulos n. C'est pourquoi on n'estime qu'une clé de 200 bits qui Mesure, pour une courbe elliptique, la taille du corps fini K de cette courbe Pour les chiffres basés sur les courbes elliptiques est plus sûre qu'une clé de 1024 Bits pour le RSA. Comme les calculs sur les courbes elliptiques ne sont pas bien Compliqués à réaliser, c'est un gros avantage pour les cartes à puces ou on dispose De peu de puissance, et ou la taille de la clé influe beaucoup sur les performances [7].

2.1.1.2 Echange des clés par courbes elliptiques

Il s'agit d'un échange de clés à la manière de Diffie-Hellman, c'est-à-dire sans les communiquer directement. A et B se mettent d'accord ensemble et publiquement sur une courbe elliptique E (a,b,K), c'est-à-dire qu'ils choisissent un corps fini K par exemple, Z/pZ, et une courbe elliptique $y2=x3+ax2+b$. Ils choisissent aussi ensemble, et toujours publiquement, un point P situé sur la courbe. Ensuite A et B choisissant secrètement KA et KB, A envoie à B le point de la courbe elliptique KAP, et B envoie à A KBP, ils sont capables de calculé kA (kBP)=kB(kAP)=(kAkB)P, ce point de la courbe elliptique consiste la clé secrète ((kAkB)P) [7].

Échange de clés :

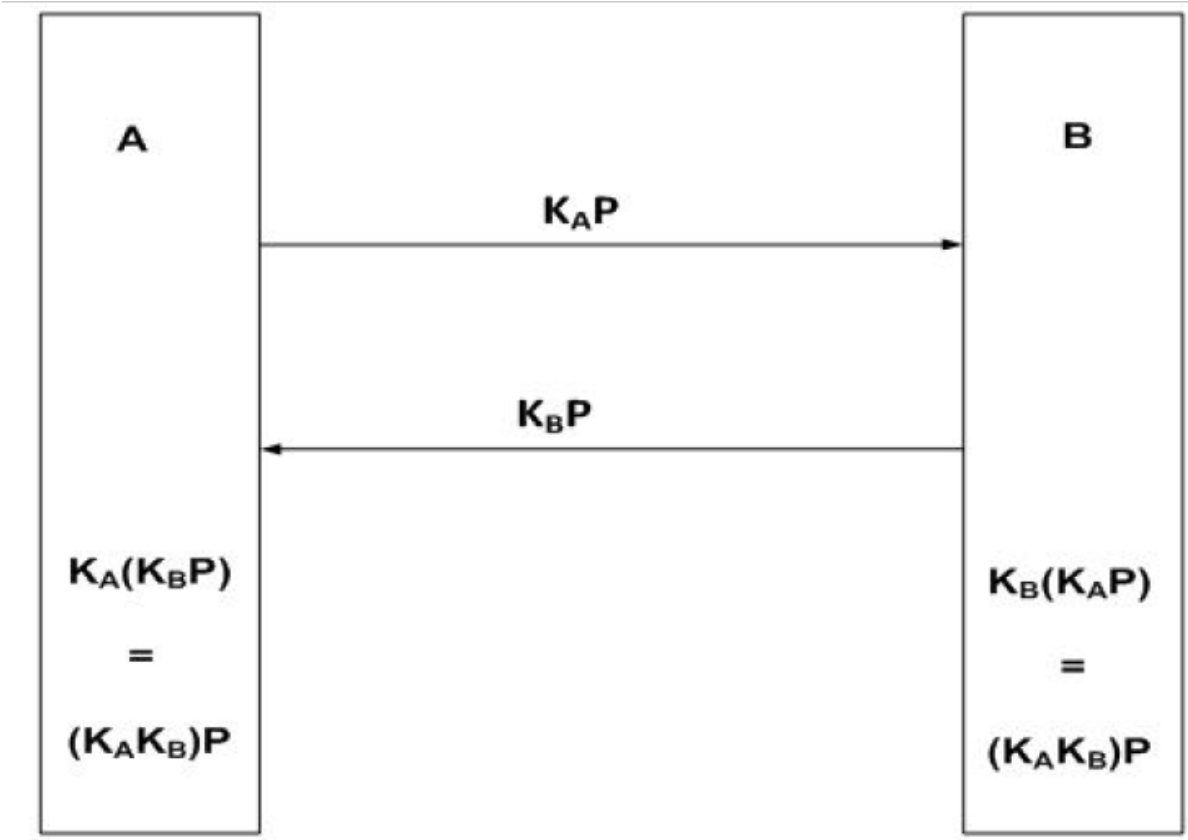


Figure 2.1 échanges de clés

Clusturing dans un réseau de capteur :

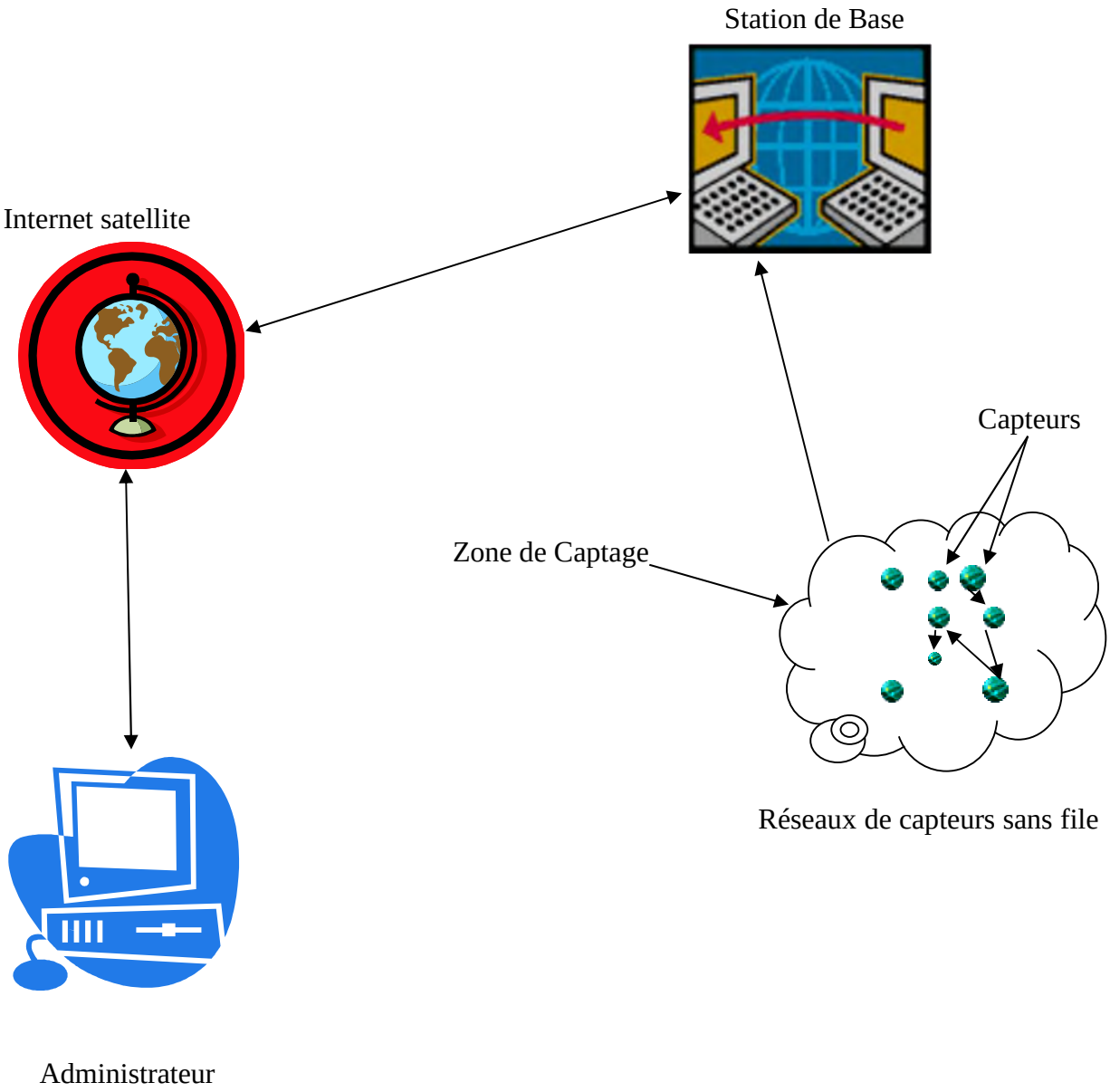


Figure 2.2 le Clusturing dans un réseau de capteurs [15].

Notre proposition

Nous avons opté pour une architecture non définit et aléatoire ou nous déploierons notre proposition, et ce, afin de tester notre solution dans un environnement ou les nœuds ne connaissent pas l'architecture et n'ont aucune notion du chemin à prendre pour leur routage, et doivent donc explorer l'environnement afin de pouvoir communiquer et ainsi construire un chemin.

Dans le cadre de travail présenté par notre camarade ACHOUR RAOUF en Recherche, entant que des professionnelles, 'Nous admettons que l'IoT est un réseau dense composé d'objets hétérogènes déployés aléatoirement et regroupés en communautés [12]. Chaque objet peut jouer le rôle de fournisseur ou demandeur de service. Chaque objet a une identité unique et appartient à une seule communauté gérée par un serveur de confiance. Un objet sollicité pour la réalisation d'un service peut soit accepter ou refuser de le fournir.'

Nous supposons aussi dans cette étude que la panne du serveur est déjà survenue, et on va tenter de chercher un nouveau candidat temporaire pour prendre le relai afin que le système ne tombe jamais en panne, de cette façon les activités sur le réseau ne cesseront pas et le système demeurera fonctionnel jusqu'à la réparation ou le remplacement dudit serveur. La première étape de notre proposition débutera juste après la panne. [7]

- **Etape 1**

  Dans cette première étape, le nœud qui détecte la panne, envoie au autre nœud de sont champ de captage :

  - Son Id
  - Id des autres Nœuds dans sont champ de captage
  - Sa Position
  - Sa Capacité
  - Ressources restante (batterie)
  - Une requête qu'une panne à étais détecté dans le serveur, comme nous avons dit juste précédemment, nous supposons que la panne est déjà survenue dans le serveur.

- **Etape 2**

Dans cette deuxième étape, Les nœuds qui on reçue la requête qu'une panne est survenue dans le serveur, avec l'Id du nœud qui la détecter plus Les Id des nœuds de sont champ, vérifie si tous les autres nœuds on reçue la requête, et cela ce fait grâce au Id des nœuds. A fin de minimiser les messages échanger entre les nœuds (capteurs), et économiser l'énergie.

- **Etape 3**

L'étape 3 consiste à lancer l'algorithme d'élection, a fin de désignée un leader. Une fois le leader est choisie, lui a sont Toure procède avec les contrainte de l'étape 4.

- **Etape 4**

  Maintenant le scénario est le suivant :

  – Un Nœud demande à s'authentifier auprès du nouveau serveur

  – Il envoie son chiffre, sa clé et l'envoie au serveur.

  – le serveur vérifie si la clé et bien chiffré.

  – Si c'est le cas, il envoie un ok au Nœud.

  – Sinon l'authentification échouera.

Pour le routage de la clé d'authentification, nous avons utilisé le protocole Leach qui calcule le meilleur chemin afin d'économiser le maximum d'énergie.

2.2 L'élection

L'IOT est un système distribué composé d'un grand nombre d'objets intelligents (Ordinateurs, Smartphone, etc.). Ces objets peuvent fonctionner ensemble, mais tous les systèmes sont indépendants. L'´election d'un leader est une nécessité fondamentale pour les systèmes distribués. Lorsqu'un système est choisi comme leader, il devrait fonctionner comme un système de gestion, prenez des décisions finales et autres. Il existe plusieurs algorithmes électoraux disponibles dans le système distribué.

2.2.1 Introduction sur l'élection

Le problème d'élection est l'un des grands paradigmes de l'algorithmique distribuée. Il a été présenté pour la première fois par LeLann [16,7]. Ce problème est de partir d'une configuration dans laquelle tous les Nœuds sont dans le même état pour arriver dans une configuration dans laquelle un seul Nœuds est dans l'état "gagnant" et tous les autres dans l'état "perdant" [17, 7, 19]. Leur but est de choisir un élément d'un ensemble, cet élément est appelé élément élu. Il peut être utilisé pour prendre des décisions dans un système réparti, il peut également centraliser des informations [16,7].

Donnons deux exemples de l'intérêt de l'élection [18,7] :

– Dans une application de type maitre-esclave, tous les serveurs sont redondants pour le traitement des requêtes de lecture des clients. Cependant, les requêtes d'écriture ne sont traitées que par un seul serveur, qui transmet ensuite les modifications aux autres sites (les esclaves). On pourra, par exemple, imaginer une gestion de mots dépasse qui permet d'ouvrir une session sans passer par le réseau.

– Certaines applications nécessitent une phase d'initialisation exécutée par un seul site. L'exemple le plus simple est celui de la circulation d'un jeton unique entre les sites. Dans ce cas l'initiateur est le premier possesseur du jeton.

2.2.2 Algorithmes d'élection

Un algorithme d'´election est un algorithme qui satisfait les trois propriétés suivantes [17,7] :

– chaque Nœuds exécute le même algorithme : symétrie complète,

– l'algorithme est décentralisé : une exécution peut être commencée par un nombre quelconque de Nœud.

– l'algorithme atteint une configuration terminale dans laquelle il existe exactement un Noeud "gagnant" et tous les autres Nœud sont "perdants".

La dernière propriété est quelquefois relâchée en :

Il existe un seul Nœud gagnant. Le Nœud gagnant est alors au courant qu'il a gagné l'élection, mais les autres ne savent pas encore qu'ils ont perdu. Dans ce cas, le Nœud gagnant diffuse le résultat aux autres Nœuds. Dans les algorithmes que nous étudions, chaque Nœud possède un ID unique qui peut être comparé (=, <, >, ≤,≥) avec les identifiants des autres Nœuds du système réparti. Enfin, chaque Nœud possède une variable state pouvant contenir les valeurs gagnant et perdant. Certaines fois, la variable state est égale à dormant avant que le Nœud n'ait exécuté une étape de l'algorithme et candidat lorsque le Nœud participe à l'algorithme, mais ne sait pas encore s'il est gagnant ou perdant [17,7].

2.2.2.1 Algorithme de Dolev, Klawe et Rodeh

Dans ce cas, Dolev, Klawe et Rodeh ont mis au point un algorithme d'élection de leader. L'idée est de choisir parmi les différentes Nœud ce lui dont l'id est le plus grand. Initialement, chaque Nœud est dans état actif (c.a.d participant au protocole). Dés qu'un Nœud découvre qu'il n'est pas ce lui dont l'id est le maximum global, il passe en mode passif, et n'agit plus alors que comme un relai pour les messages.

L'algorithme utilise pour chaque Nœud deux variables entières : left et max, ainsi que deux types de messages : <1, i> et <2, i> ou i est un entier. Notons que la variable max contient initialement l'identificateur du Nœud. L'algorithme, tel que présenté dans l'article original [20].

2.2.2.2 Hypothèses et principe

– Calcul du plus grand numéro Id du Nœud.

– Initialement tous les Nœuds sont actifs à chaque round chaque Nœud compare son numéro avec ses voisins.

– Si son numéro est plus petit que l'un de ses voisins, passe à l'état passif.

– A moins la moitié des identités actives ne survivent pas à un round ! Après au Plus log N round l'élection est finie [20,7].

2.2.3 Election sur réseau complet

2.2.3.1 Algorithme de Bully (Garcia-Molina)

Déclenchement

– Quand un Nœud N s'aperçoit que le coordinateur ne répond plus à ses requêtes (time-out sur TEMPO), il lance l'algorithme d'élection.

Lancement de l'élection par N

– n envoi d'un message ELECTION à tous les autres nœuds dont le numéro est plus grand que le sien Réception d'un message ELECTION depuis P par un Nœud N+1.

– le Nœud N+1 envoie un message ACK à N lui signant qu'il est actif.

– a son tour N+1, lance une élection si ce n'est pas déjà fait.

Sur le Nœud n

– Si aucun Nœud ne lui répond avant TEMPO, N gagne l'élection et devient le coordinateur.

– si un Nœud de numéro plus élevé répond, c'est lui qui prend le pouvoir. le rôle de N est terminé.

Annonce de l'élu

– le nouveau leader (coordinateur) envoie un message à tous les participants pour les informer de son rôle.

– déclenche une élection.

– S'il détient le plus grand numéro de processus en cours de fonctionnement, il gagne l'élection et devient le nouveau coordinateur (leader) [20].

2.2.3.2 Algorithme général d'élection 2 [16,7].

Principe

– Un ou plusieurs nœuds détecte la panne du coordinateur.

– Ils informent l'ensemble des nœuds du début de l'algorithme avec un message <wakeup > car la seconde partie de l'algorithme doit être initié par toutes les feuilles.

– Lorsque le message < wakeup > a parcouru tout Nœuds, l'élection commence.

– les Nœuds émettent un message.

– le nœud ayant le plus grand numéro est élu.

Variables

– wsp : booléen ini faux (wsp est vrai si p est réveillé).

– wrp : integer init 0 (compte les messages de réveil reçus) req[q] ; 8q 2

Neighp : booléen init faux (vrai si p a reçu un message de q).

– vp : numéro de processus init p (plus grand processus) etatp : (sleep, leader

, lost) init sleep.

– Vp : voisins du processus.

2.2.4 Election sur topologie du réseau quelconque

2.2.4.1 Election dans le cas de la diffusion séquentielle [21].

Hypothèses

– Une topologie du réseau quelconque est supposée.

– Les messages ne se perdent pas et sont délivrés au bout d'un temps fini après leur émission.

– Un nœud ne connait que ses voisins et n'apprend jamais la structure globale du réseau.

2.2.4.2 Principe d'élection

– Un nœud détecte la panne du serveur.

– il informe l'ensemble des nœuds du période d'élection avec un message « non message ».

– Lorsque le message parcourt tous nœuds, l'élection commence.

– Les nœuds lancent l'élection et émettent un second message contenant leur propre ID ainsi que les ressources restantes et disponibles.

2.3 Conclusion

Dans ce chapitre nous avons vu différents protocoles d'authentifications utilisant différentes techniques et méthodes, ainsi que quelques algorithmes d'élection, et nous avons soulevé certains points importants dans un système IOT.

Notre modèle regroupe différentes techniques et méthodes qui sont l'élection d'un leader afin d'élire un nouveau candidat, un protocole d'authentification qui sert a sécurisé les communications entre les nœuds à base ' d'Elliptic Curve Cryptography ' ce qui permet d'économiser des ressources surtout dans notre domaine d'étude, l'IoT, ou on doit sauvegarder et économiser un maximum, et en dernier, un protocole de routage, Leach, qui optimise le chemin par lequel transitent les messages dans le but d'économiser un maximum d'énergie.

3.1 Introduction

Après avoir réalisé la conception appropriée à notre projet, nous allons dans ce chapitre décrire le processus de la réalisation de notre simulation. Ceci en spécifiant l'environnement de développement, et une présentation de quelques interfaces de notre simulation

3.2 Les outils de développement

3.2.1 cooja

Cooja est le simulateur de réseau contiki, cooja permet de simuler de grands et petits réseaux de motos contiki, les mutations peuvent être émulées au niveau du matériel, ce qui est plus lent, mais permet une inspection précise du comportement du système, ou réseau plus important.0

Nous compilerons maintenant et commencerons cooja, le simulateur de réseau contiki.

Pour commencer cooja, ouvrir une fenêtre de terminal, et accéder au répertoire cooja. Cd contiki/tools/cooja.

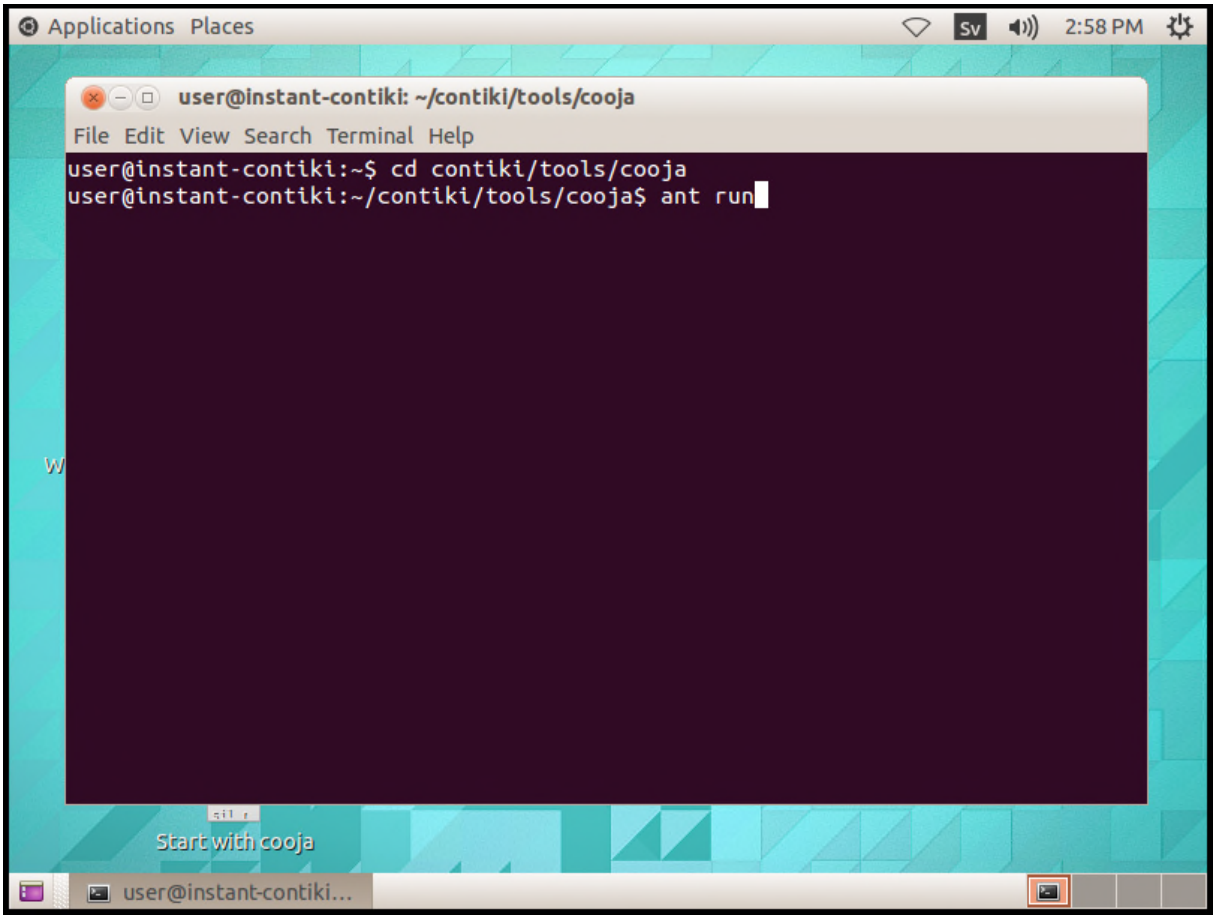


Figure 3.1 lancement de cooja

Commencer cooja avec la commende : Ant run , attendez que cooja commence, il se compile tout d'abord, ce qui peut prendre du temps. Lorsque cooja est compilé, il commencera par une fenêtre vide bleue.

Maintenant que cooja est opérationnel, nous pouvons l'essayer avec un exemple de simulation.

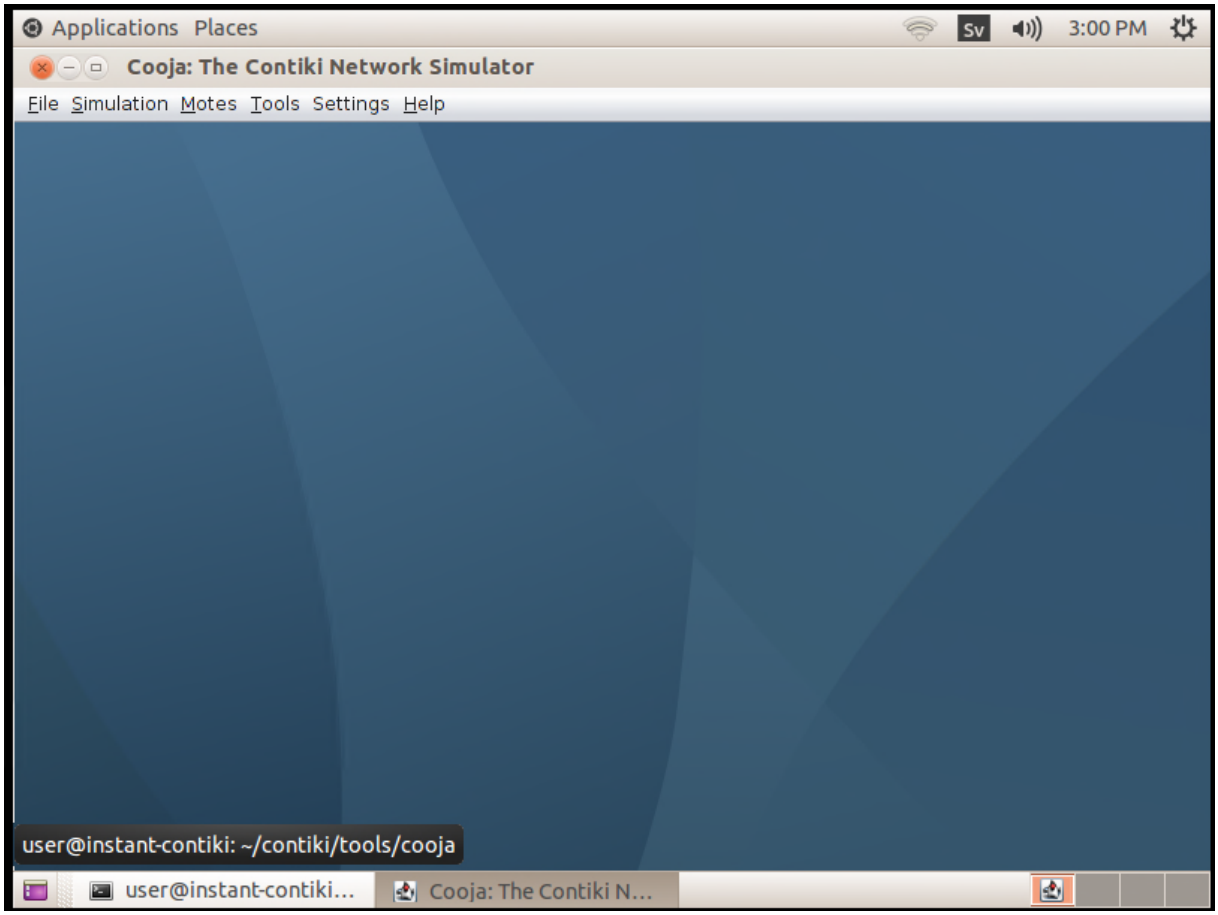


Figure 3.2 cooja simulateur

3.2.2 A propos des simulations de cooja

Cooja est un outil très utile pour le développement de contiki il permet aux développeurs de tester leur code et leurs systèmes longtemps avant de l'exécuter sur le matériel cible.

Les développeurs établissent régulièrement de nouvelles simulations à la fois pour déboguer leur logiciel et pour vérifier le comportement de leurs systèmes.

Cliqué sur le menu fichier et cliqué sur nouvelle simulation.

Cooja ouvre maintenant le nouveau dialogue de simulation, dans ce dialogue, nous pouvons choisir de donner à notre simulation un nouveau nom, mai pour cet exemple, nous nous contenterons simplement de ma simulation.

Cooja fait apparaitre la nouvelle simulation, La fenêtre du réseau, en l'écran affiche toute la piste dans le réseau simulé.

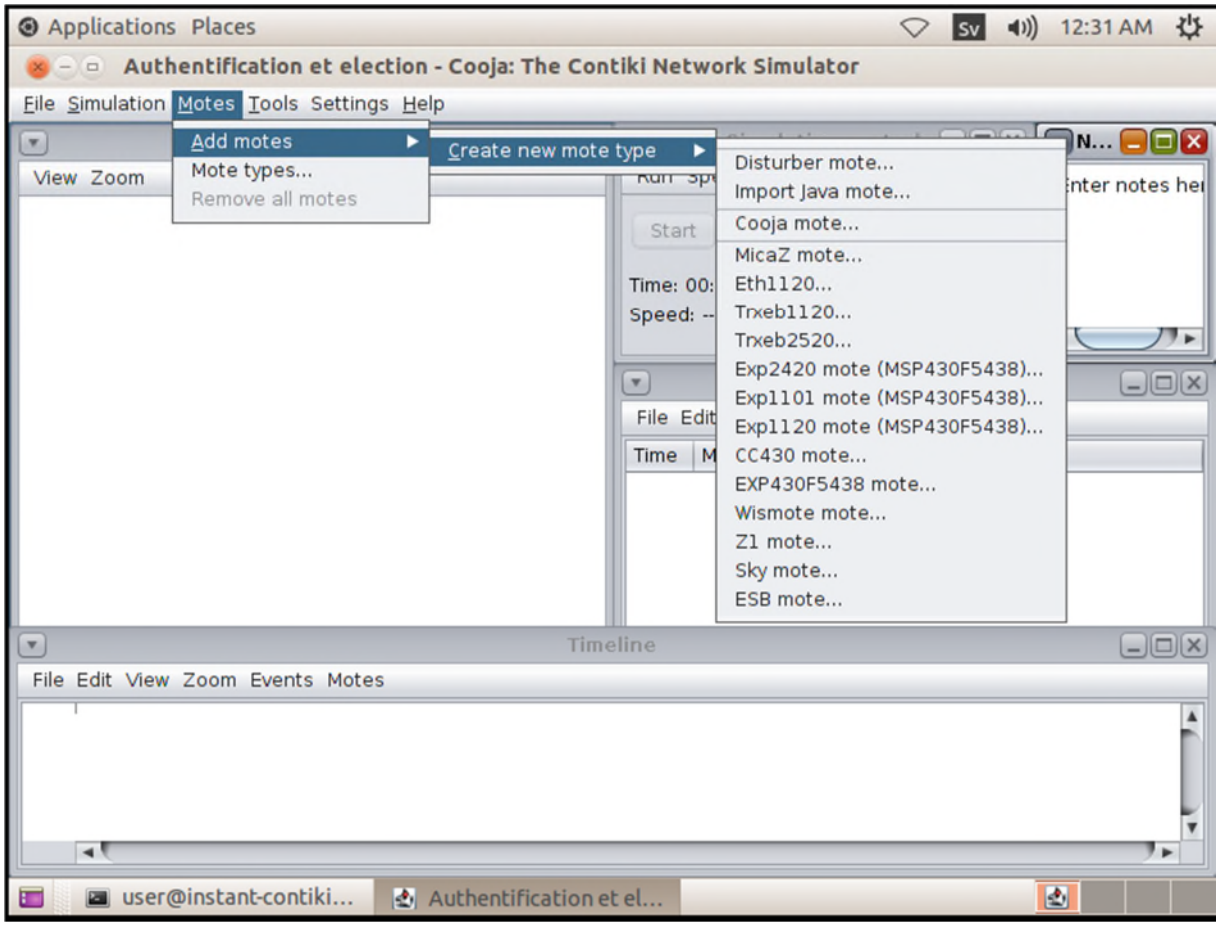


Figure 3.3 cooja simulateur « création des Nœuds (capteurs) »

3.3 contiki

Contiki est un système d'exploitation léger et flexible pour capteur miniatures en réseau. Ces dernières années, le monde scientifique a porté une attention importante au réseau de capteurs sans fil. La miniaturisation des capteurs et leur prix relativement faible, permettant d'imaginer des applications très variées dans les domaines scientifiques, militaires, industriels et domotiques.

Contiki propose malgré tout les principales caractéristiques et fonctionnalités d'un système d'exploitation tout en favorisant une empreinte mémoire minimales. Ses principaux

Atouts sont le support des protocoles IPv6 et 6LoWPAN, sa flexibilité et sa portabilité disponible gratuitement sous licence BSD, contiki peut être utilisé et modifier même a des fins commerciales.

3.3.1 Fonctionnement et théorie

Contiki est constitué d'un noyau, de bibliothèques, d'un ordonnanceur et d'un jeu de processus. Comme tout systéme d'exploitation, son rôle est de gérer les ressources physiques telles que le processeur, la mémoire, les périphériques informatiques (d'entré/sorties). Il fournit ensuite au applications informatique des interfaces permettant d'utiliser ces ressources. Conçu pour les modules de capteurs sans-fil miniatures, il occupe peu d'espace en mémoire et permet une consommation électrique très fiable.

Contiki **offre deux types de connectivités :**

- La couche Rime, elle permet un dialogue vers les captures voisin ainsi que le routage.
- La couche UIP, orientée Internet, elle offre les services essentiels du protocole IP mai nécessite plus de ressources que Rime.

Contiki gère les standards multi-threads 6LoWPAN, RPL CoAP. Le système de fichier coffee permet des opération sur des fichiers stockés sur une mémoire flash externe.

3.3.1.1 Les caractéristiques :

Un système d'exploitation pour capteur en réseau a différentes caractéristique :

- **Empreinte mémoire**

  L'espace mémoire utilisé par le système d'exploitation et par l'application doit être suffisamment faible pour être contenu dans la mémoire du capteur. Une configuration typique de contiki (le noyau et le chargeur de programmes)

  Consomme 2 kiloctets de RAM et 40 kilooctets de ROM.

- **Consommation energétique**

  L'énergie électrique, souvent apportée par une batterie de piles, peut être problématique à renouveler. Si des systèmes de captage, comme des éléments photovoltaïques, éoliens, ou autres peuvent être utilisée dans certains cas, les recherches scientifiques explorent les possibilités de réduire la consommation des capteurs. L'élément le plus consommateur est le module radio. La réduction de temps de transmission

3.4 Les différentes interfaces de la simulation

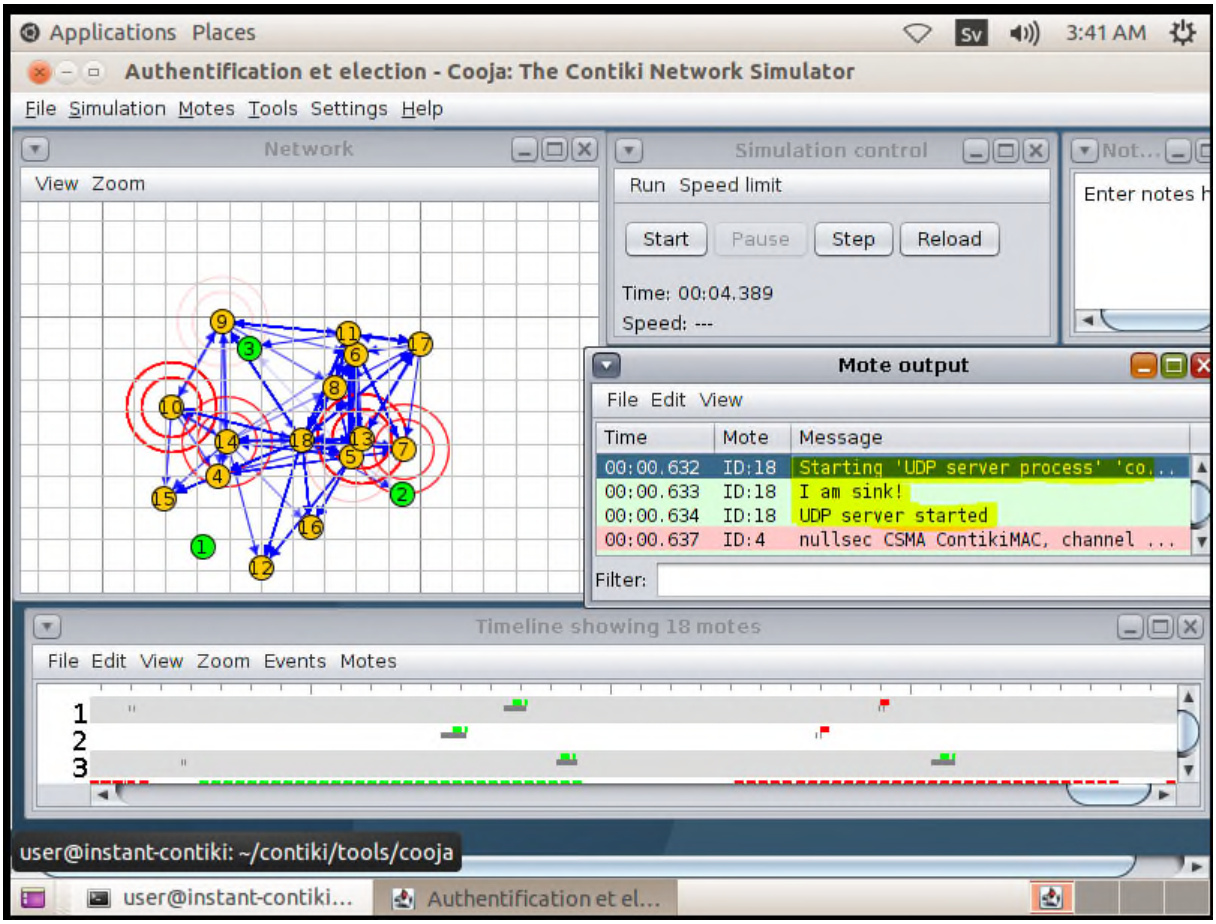


Figure 3.4 échanges de messages « une panne c'est produite le serveur »

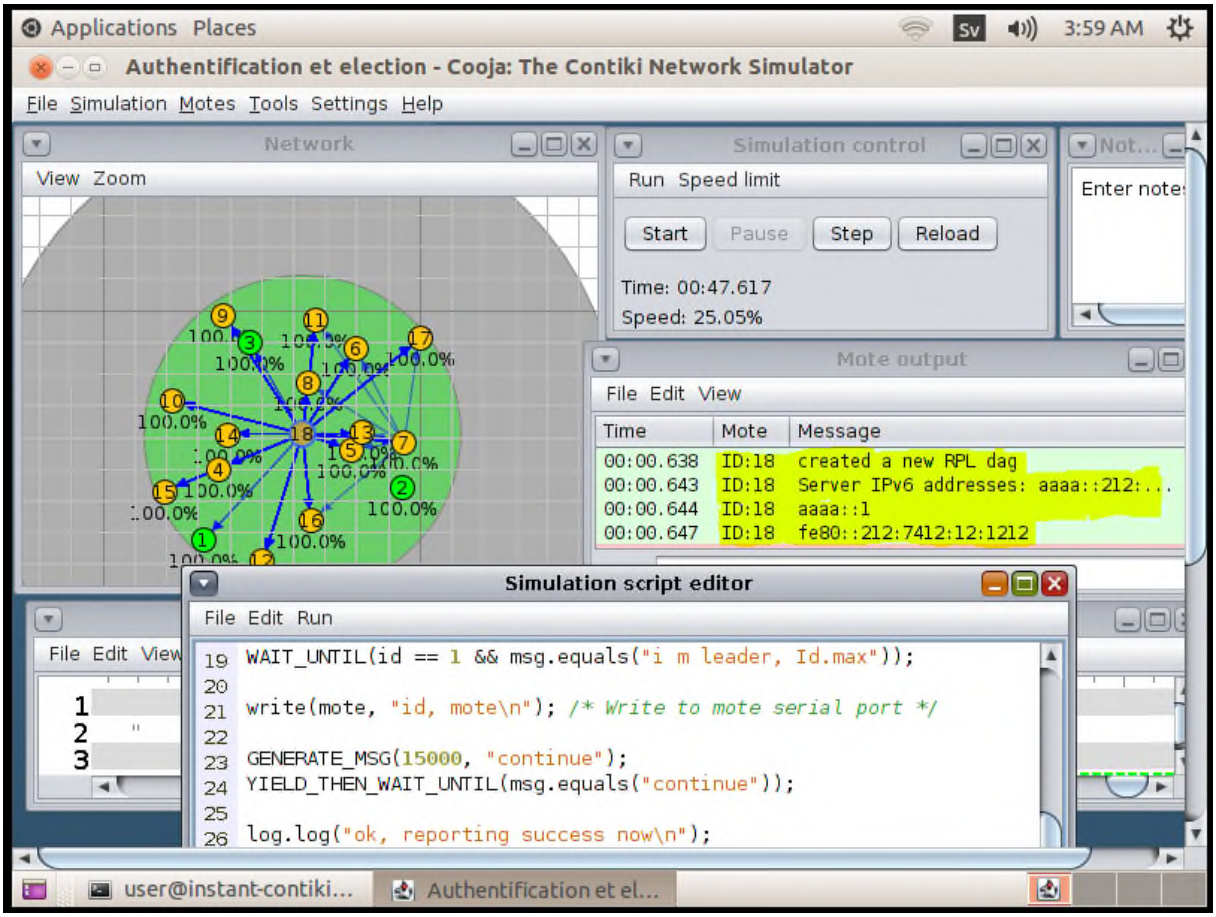


Figure 3.5 le lancement de l'élection

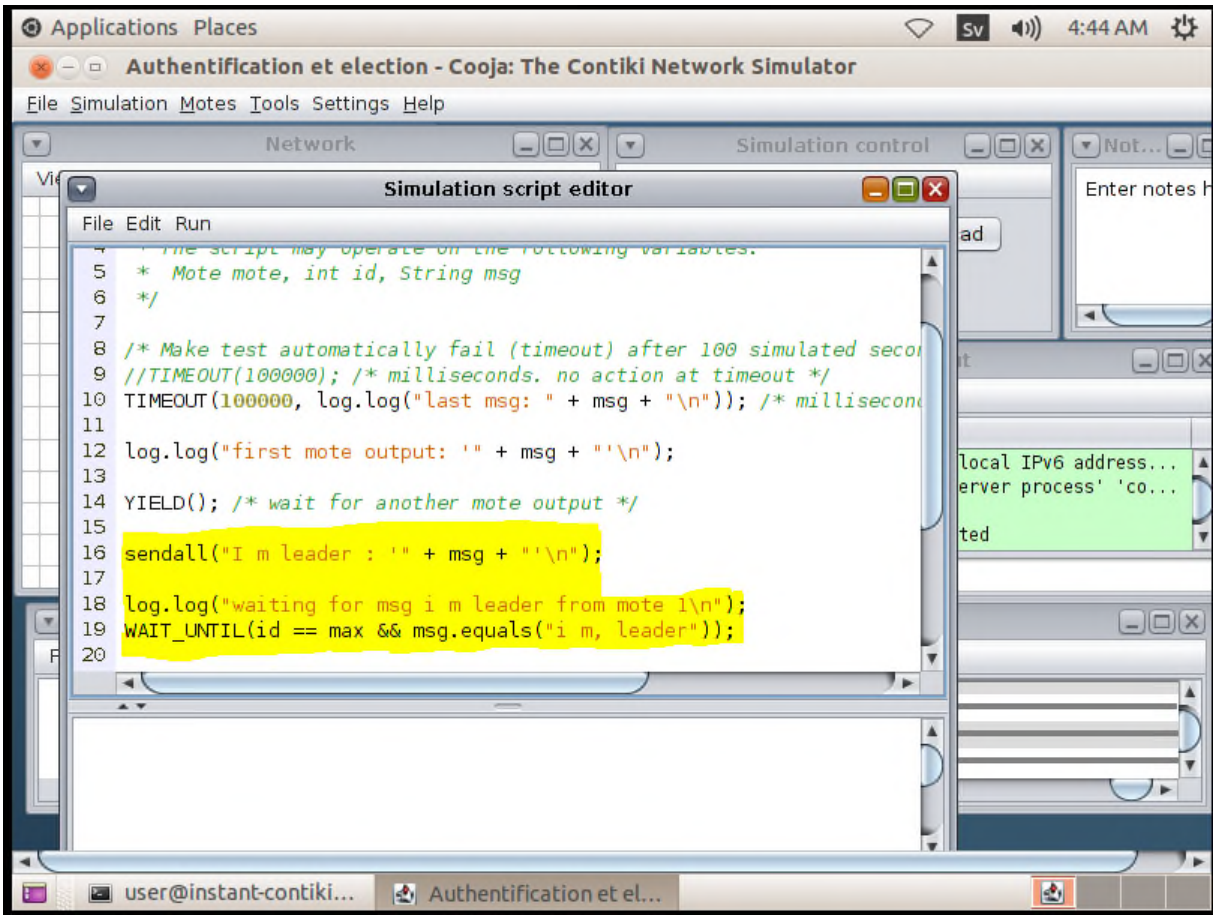


Figure 3.6 le scripte de désignation du leader

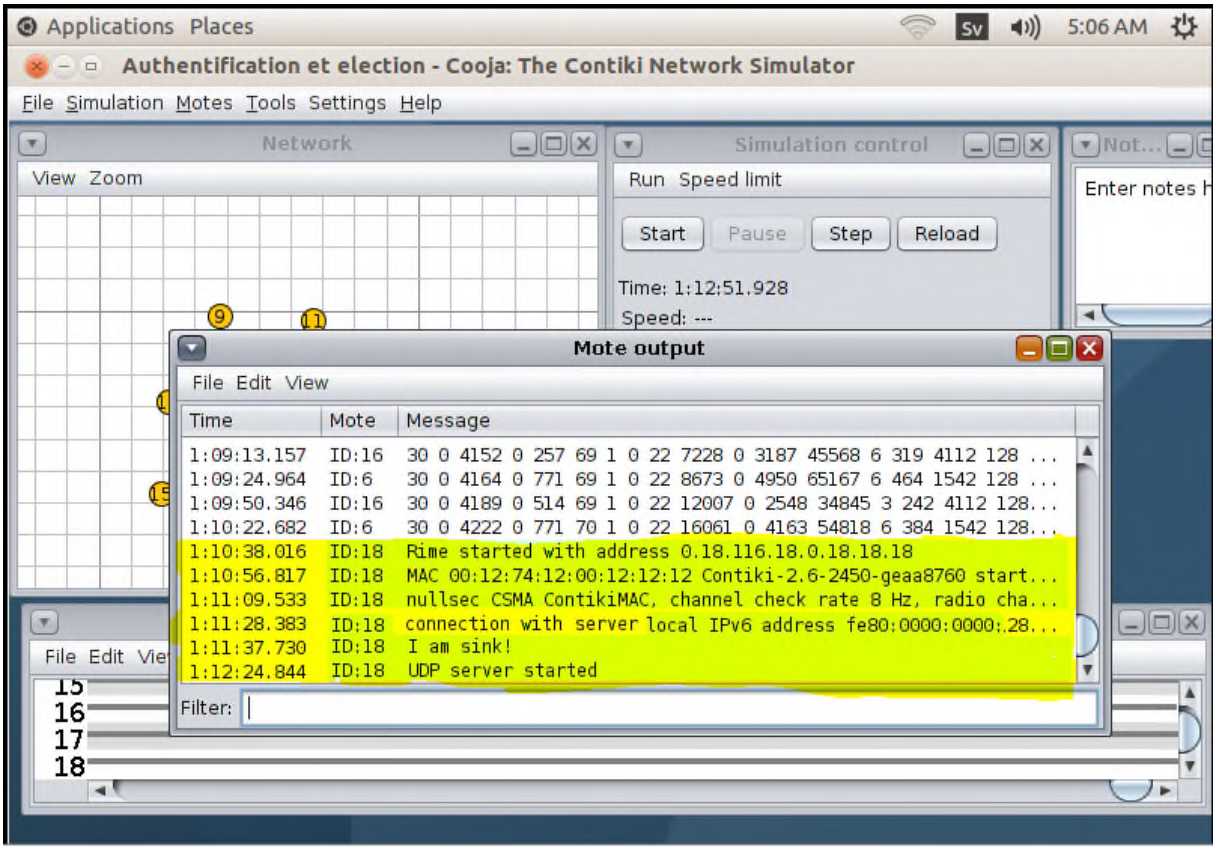


Figure 3.7 L'authentification avec le serveur

3.4.1 Code source de l'authentification

```
<projectAuthentification>
        <name>FormatS1</name>
        <comment></comment>
        <projects>
        </projects>
        <buildSpec>
            <buildCommand>
                <name>org.eclipse.jdt.core.javabuilder</name>
                <arguments>
                </arguments>
            </buildCommand>
        </buildSpec>
        <natures>
            <nature>org.eclipse.jdt.core.javanature</nature>
        </natures>
</projectAuthentification>
```

```
<classpath>
	<classpathentry kind="src" path="src"/>
	<classpathentry kind="con"
path="org.eclipse.jdt.launching.JRE_CONTAINER/org.eclipse.jdt.internal.debug.ui.launcher.
StandardVMType/JavaSE-1.8"/>
	<classpathentry kind="output" path="bin"/>
</classpath>
public class A extends Thread {

	public static int p=233; //
	public static int a; //
	public static int y1; //
	private int x1; //
	int k; //

	/**
	 * les instructions qui s'execute dans le thread
	 */
	public void run(){

	    /*
	     * avoir un nombre aléatoire entre [1, p-1]
```

```
 * la valeur retourné de la méthode random(Uniforme) est entre [0, 1] (Type
Real)
 * random_number = (uniforme * (borne_sup - borne_inf)) + 1
 * Hichem
 */
a = (int) (Math.random()*((p-1)-1)) + 1;

/*
 * générer un nombre aléatoire entre [1, 1000]
 *
 */
x1 = (int) (Math.random()*(999)) + 1;

/*
 * calculer y = (a^x1) mod p
 */
y1=(int) (Math.pow(a,x1) % p);

/**
 * créer un objet de type B pour récuperer y2
 */
B bo = new B ();

/*
 * calculer la clé K = (y2^x1) mod p
 *
 */
```

```
public class B extends Thread {

 public int k; //
 public static int y2; //
 private int x2; //

/**
 * les instructions qui s'execute dans le thread
 */
 public void run(){

     //Récupération des variables
     A al = new A;
     int a = al.a; //
     int p = al.p; //

     /*
      * générer un nombre aléatoire entre [1, 1000]
      *
      */
     x2 = (int) (Math.random()*(999)) + 1;

     /*
      * calculer y = (a^x1) mod p
      */
     y2=(int) (Math.pow(a,x2) % p);
```

```
                /*
                 * calculer la clé K = (y2^x1) mod p
                 */
        k=(int) (Math.pow(al.y1,x2) % p);
                // Afficher le résultat
        System.out.println("B # La clé publique est : " + k);

            }
        }
        public class MainClass {

            public static void main(String[] args) {

                A proc1 = new A();
                B  proc2 = new B();
                proc1.start();
                proc2.start();

            }
}
```

3.4.2 Autres capture de la simulation

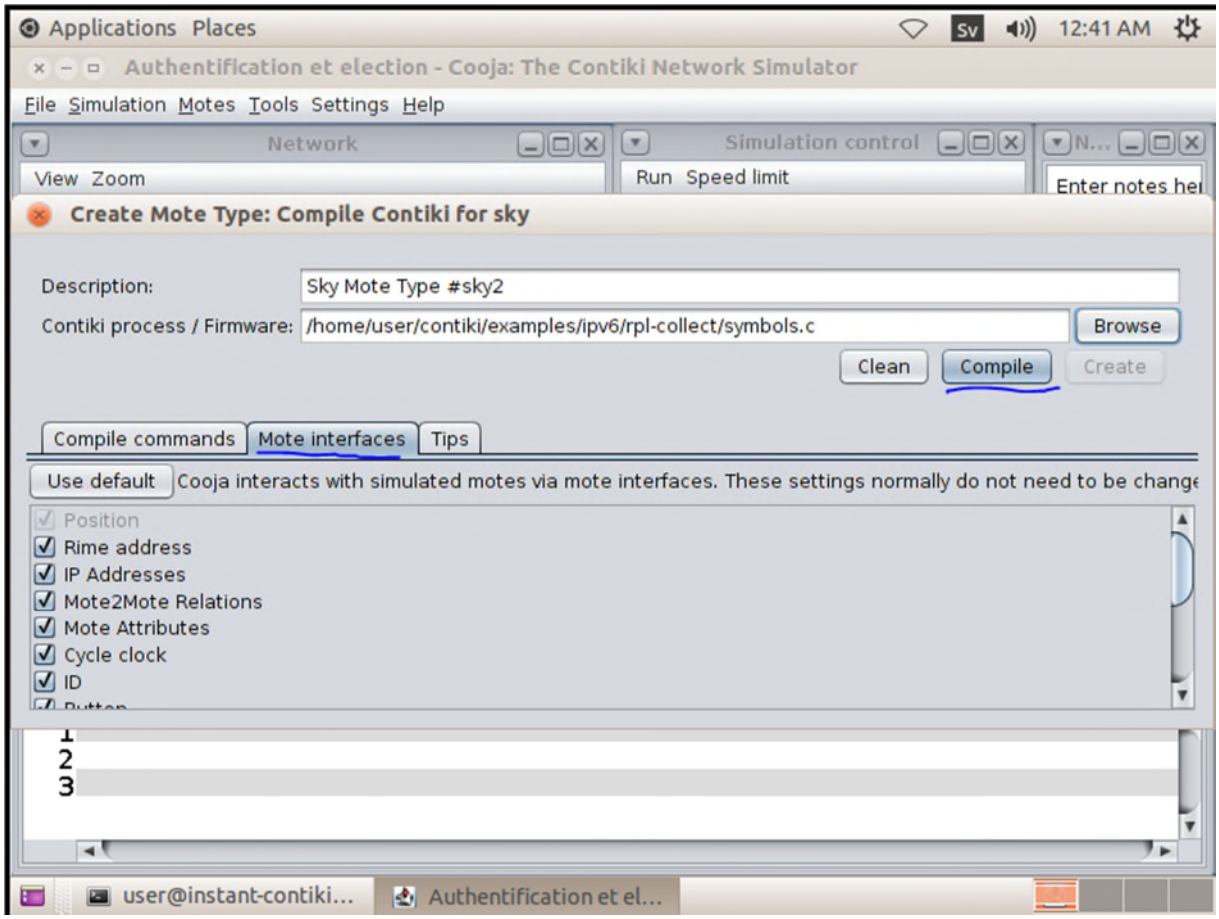


Figure 3.8 création des capteurs

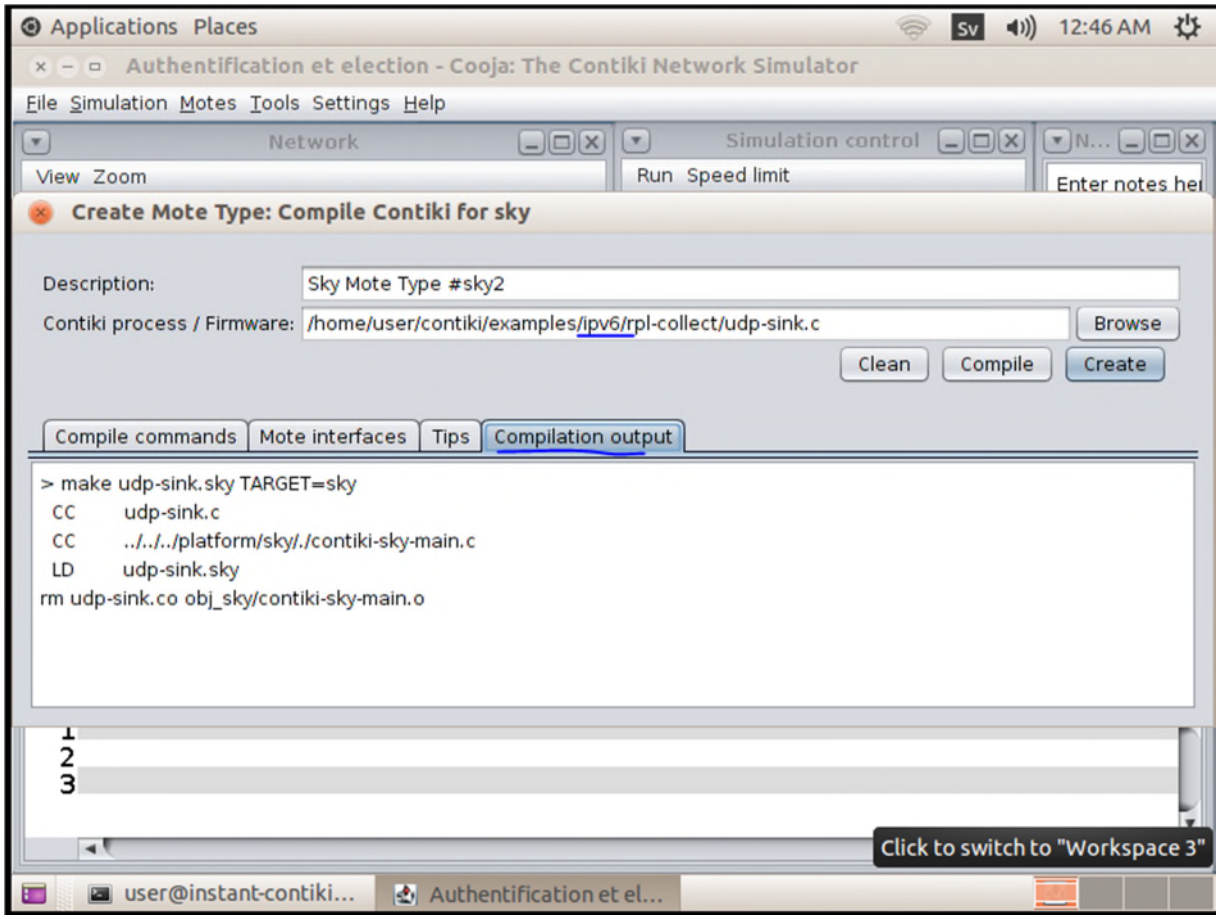


Figure 3.9 compilation de type de capteur

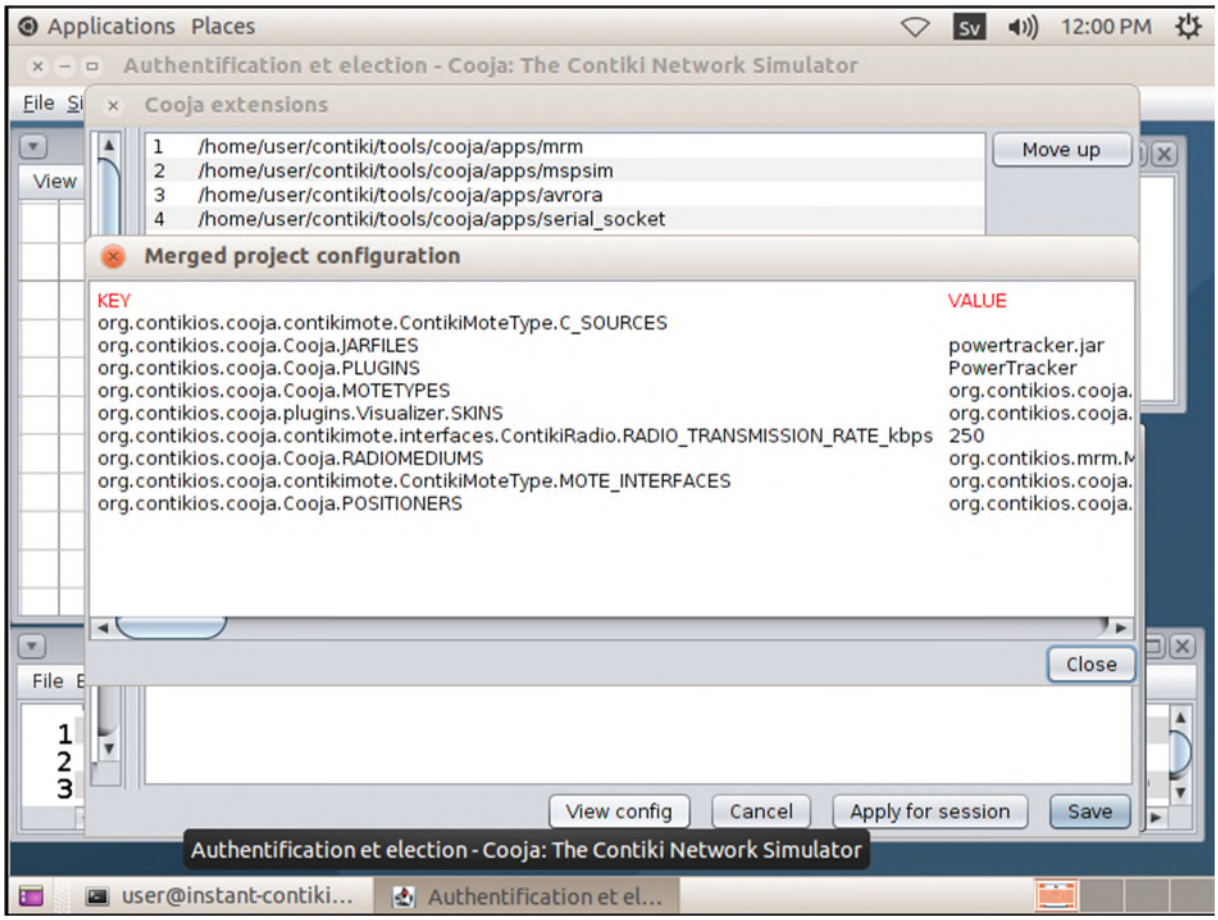


Figure 3.10 Extensions de cooja

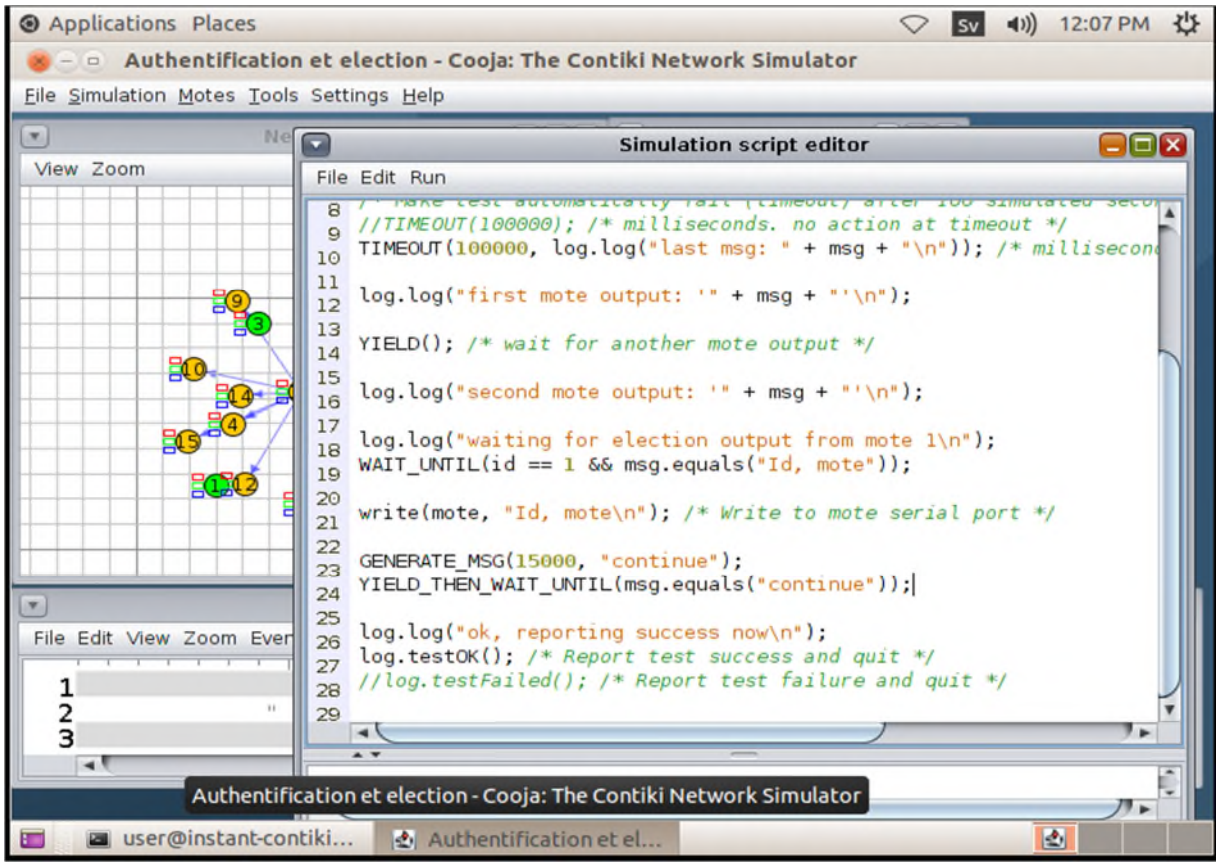


Figure 3.11 Scripte de l'élection

3.4.3 L'algorithme d'élection choisie

Vu le manque du temps nous avons choisie . Nous l'avons mentionné dans la partie 2.2.3.1 du deuxième chapitre, avec la contrainte, le nœud qui as le plus grand Id seras élu comme leader.

3.5 Conclusion

La phase de la réalisation est l'étape la plus importante. Dans ce chapitre nous avons présenté cette étape cruciale de notre projet par une brève description des outils nécessaires pour réaliser notre simulation, nous avons implémenté un protocole d'élection d'un serveur d'authentification dans IOT.

L'internet des objets est un concept qui repose sur l'idée que tous les objets seront connectés un jour à l'internet de l'information et éventuellement de recevoir des commandes. En quelques années seulement depuis son apparition, il est fut adopté dans divers secteurs et cela à grâce à son potentiel énorme. Cependant, sa forte intégration soulève plusieurs interrogations dont le principal est « comment assurer la privacy et instaurer une sécurité robuste pour cette nouvelle technologie fortement hétérogène et ubiquitaire.

Dans ce travail, nous avons mis en avant les concepts essentiels de l'IOT, ainsi que les besoin et les défis de la sécurité dans l'IOT. Nous avons étudié quelques schémas d'établissement de clé qui permettent d'offrir le service d'authentification et de sécurité. Nous avons aussi recensé quelque algorithmes d'élections qui servent à élire un processus parmi plusieurs dans le but de prendre des décisions dans un système informatique.

Notre proposition se base sur un protocole d'authentification et un algorithme d'élection, le protocole d'authentification vise à sécurisé les communications entre les différentes objets ou bien entre les objets et le serveur, et l'algorithme d'élection vise sélectionner un autre serveur parmi un ensemble de dispositifs pouvant assurer cette fonction en cas de panne.

Le but de l'élection de leader et d'élire un chef unique parmi plusieurs processus qui sont candidats à l'élection. Le but du leader est de synchroniser les différents processus présents dans un réseau. Pour cela, nous avons choisie et étudier un algorithme qui permet de faire l'élection dans les réseaux de capture (nœud).

Finalement, en guise de perspective, nous souhaitons proposer une amélioration au protocole implémenté, dans notre travail afin d'améliorer l'élection et d'approfondir la simulation

Ce travail nous à été bénéfique sur le plan théorique et pratique, avec lequel on a amélioré nos connaissances déjà acquises, et acquérir de nouvelles connaissances.

Bibliographie

[1](books.openedition.org\editionsmsh\8u?lang=Fr#tocFrom2n1.)

Consulté le: http://fr.slideshare.net/mobile/mousski/9-linternet-des-objets. [2].

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things : A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4) :2347–2376, 2015. [3]

P.J . Benghozi,S. Bureau,and F. Massit-Folea. L'Internet des objets. Quels Enjeux Pour les Européens ? Technical report, Orange Ecole Polytechnique et TELECOM Paris Tech,2008.[4]

Y. Challal. Sécurité de l'internet des objets : Vers une Approche Cognitive et Systémique.

PHD thesis, Université de technologie de Compiègne, 2012 [5]

Y.ait mouhoub, F.Bouchebbah . Propotion d'un modèle de confaince pour l'internet des Objets, Université A/MIRA de Bejaia . 2015 [6]

R.ACHOUR, N.Makhloufi, Authentification dans l'internet des objets . Université A/MIRA de Bejaia, 2017 [7] .

Livre Blanc Préparer la Révolution de l'internet des Objets . 2016

Consulté le: https://www.itu.int/rec/T-RREC-E.164-201011-1/fr [8].

P. Benghazi, S. Bureau, and F. Massit-Folea. L'internet des objets. quels enjeux Pour les européens ? 2008.[9]

R. Saad. *Modèle collaboratif pour l'Internet of Things (IoT).* PhD thesis, Université du Québec a Chicoutimi, 2016.[10] .

S. Feng, J. Cerles, H. Dalmas, T. Dˆo-Khac, and B. Paulin. *Sécurité des objets Connectés*. Institut national des hautes études de la sécurit´e et de la justice, 2014. [11].

C.Llorens, L.Levier and D.Valois. Tableau de bord de la sécurité réseaux. Eyrolles. 2006 [12].

SmartCard Alliance, "Smart Cards and Biometrics," available to: Consulté le: wwww.smartcardalliance.org , Mars 2011. [13]

M.Benmohammed, Conception et Vérification d'un Protocole d'Authentification de Système Combiné RFID-Biométrique [14]

N.Bounegta ingénieurs D'état en informatique, Mémoire en ligne approche distribuée pour la sécurité d'un réseaux sans file RCSF , Université Bechar 2010 . [15]

Bibliographie

A. Zemmari. *Présentation et analyse de quelques algorithmes distribués probabilistes*. PhD thesis, Université Bordeaux 1, 2009. [16]

D. Conan. Initiation ´a l'algorithmique répartie. 2017. [17]

H. Serge. *L'ELECTION*. PhD thesis, Université de Paris-Dauphine, 2014. [18]

Cosulté le : http://www.lirmm.fr/~lafourca/ML-enseign/CNAM/mps.pdf, (Consulte le 22 juin 2017). [19]

P. Laurent. *Algorithmique Distribuée, Election distribuée*. PhD thesis, Université de franche-comté, 2014. [20]

J. Hélary, A. Maddi, and M. Raynal. *Calcul distribué d'un extremum et du routage associé dans un réseau quelconque*. PhD thesis, INRIA, 1986. [21]

Résumé

Internet of Things relie des objets à Internet, ce qui permet d'obtenir des idées jamais obtenues auparavant. L'IoT est un vaste réseau de périphériques qui comprend différents dispositifs intelligents et capteurs. Ces "Objets" collectent et échangent des données. Leurs contraintes matérielles ainsi que celle des environnements hostiles dans lesquels ils pourraient être déployés rendent l'IoT vulnérable et nécessitent des mécanismes de sécurité efficaces et peu couteux. La panne des serveurs dans les systèmes distribués est un autre problème dans l'IoT.

Mots clés : Internet des Objets (IdO), authentification, sécurité, élection.

ABSTRACT

Internet of Things connects objects to the Internet, making it possible to get ideas that have never been available before. The IoT is an extensive network of devices that includes various intelligent devices and sensors. These "Objects" collect and exchange data. Their physical constraints as well as hostile environments in which they could be deployed make IoT vulnerable and require effective and inexpensive security mechanisms. Another problem in the IoT is the failure of servers in distributed systems. In this brief, we present a state of the art of some existing key management protocols, some election algorithms.

Key words: Internet of Things (IoT), Authentication, security, election.