République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Seddik Benyahia Jijel
Faculté des Sciences Exactes et Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option : Réseaux et Sécurité

Thème

Implémentation d'un Protocole d'Élection d'un Serveur d'Authentification dans l'Internet des Objets

Réalisé par

Chabani Rabah

Encadré par

Mme. Bouchaib Fazia

Promotion 2021

Remerciements

Tout d'abord je remercie ***ALLAH****, le tout puissant qui a illuminé mon chemin et qui s'est armé de courage et de patience pour accomplir ce travail.*

Je remercie mon encadreur ***Mme. Bouchaib Fazia****, qui a été très disponible tout au long de la réalisation.*

Je remercie également toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail, sans oublier les membres du jury pour avoir accepté de la juger.

Résumé

L'internet des objets(Ido) 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, qui sont considérés comme la plateforme de base de l'Ido, sont les objets de la vie quotidienne (réfrigérateur, téléviseur, portables, Smartphone, .etc.). Ces objets sont équipés de composants électronique tels que des supports de communication radio, des processeurs pour le traitement, des capteurs et/ou actionneurs, etc.

La grande puissance de l'Ido repose sur le fait que ses objets communiquent, analysent, traitent et gèrent des données d'une manière autonome. Cependant, les problèmes liés à la sécurité freinent considérablement l'évolution et le déploiement rapide de cette haute technologie.

La panne des serveurs dans les systèmes distribués est un autre problème dans l'Ido.

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

Mots clés : *Internet des Objets, Sécurité, Authentification, Election.*

Abstract

The Internet of Things(IoT) means the ubiquity around us of a variety of things, which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to achieve common goals. The objects, which are considered the basic platform of the IOT, are the objects of everyday life (refrigerator, TV, laptops, Smartphone, .etc.). These objects are equipped with electronic components such as radio communication media, processors for treatment, sensors and / or actuators, etc.

The great power of the IoT lies in the fact that its objects communicate, analyze, process and manage data autonomously. However, security concerns are a major obstacle to the development and rapid deployment of this high technology

Server failure in distributed systems is another issue in the IoT. The proposed work is based on an authentication protocol and an election algorithm, the authentication protocol aims to secure communications between the different objects or between the objects and the server, and the election algorithm aims to select another server from a set of objects that can perform this function in the event of a failure.

Keywords : *Internet Of Things, Security, Authentication, Election.*

Table des matières

Table des figures

Listes des acronymes

IdO	Internet des Objets
IoT	Internet of things
ITU	Internation Telecommunication Union
SIdO	le concept d' Internet des Objets social
ERDF	la gestion des réseaux de distribution en France
GPS	global positioning system
WSN	Un réseau de capteurs sans fil
RFID	Identification par radiofréquence
6LoWPAN	réseaux personnels sans fil de faible puissance
LoRaWAN	le réseau étendu à longue portée
BLE	Bluetooth basse énergie
CoAP	protocole d'application contraint
MQTT	transport de télémétrie par file d'attente de messages
HTTP	Hypertext Transfer Protocol
MQTT	est un protocole de messagerie léger
CoAP	protocole d'application contraint
IP	internet protocol
TTP	tiers de confiance
ECC	cryptographie de courbe elliptique
Pin	personal identification number
Id	identificateur
RSA	Rivest-Shamir-Adleman
MD5	message-digest algorithme
IKE	Internet Key Exchange
SSH	Secure Socket Shell
TLS	Transport Layer Security
FIFO	first in first out
WSN	Wireless sensor network
GWN	gateway wireless node

Introduction Générale

L'Internet a subi de graves changements depuis son premier lancement à la fin des années 1960 en tant que résultat de l'ARPANET. Un réseau initial à quatre nœuds s'est rapidement transformé en un réseau fortement interconnecté et auto-organisé qui construit la base quotidienne pour les entreprises, la recherche et l'´économie. Au cours des années 1990, un certain nombre de termes émergeaient pour saisir de nouvelles formes d'interactions personnelles et commerciales. La prochaine révolution sera l'interconnexion entre les objets pour créer un environnement intelligent nommé Internet des Objets (IdO) ou IoT pour Internet of Things en anglais. L'Ido est considéré comme la troisième vague de technologies de l'information juste après Internet et les réseaux de communication mobiles. Il est apparu comme l'un des paradigmes de communication les plus puissants du XXIe siècle [2].

La grande puissance de l'Ido repose sur le fait que ses objets communiquent, analysent, traitent et gèrent des données d'une manière autonome. Cependant, les problèmes liés à la sécurité freinent considérablement l'évolution et le déploiement rapide de cette haute technologie. L'usurpation d'identité, les vols d'information et la modification des données représentent un vrai danger pour ce type des systèmes [4].

La panne des serveurs dans les systèmes distribués est un autre problème dans l'Ido.

L'élection d'un nouveau serveur est une nécessité fondamentale pour les systèmes distribués. Lorsqu'un système est choisi comme serveur, il devrait fonctionner comme un système de gestion, prenez des décisions finales et autres. Il existe plusieurs algorithmes électoraux disponibles dans le système distribué.

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 nœud est dans l'état "gagnant" et tous les autres dans l'état "perdant". Leur but est de choisir un élément d'un ensemble, cet élément est appelé élément élu [3].

A travers ce mémoire, nous proposons une solution de relai en cas de panne du serveur, basé sur un algorithme d'élection (sélectionner un nouveau serveur parmi un ensemble des objets pouvant assurer cette fonction en cas de panne du serveur) et d'un protocole d'authentification qui vise à sécuriser les communications entre les différents objets ou bien entre les objets et le serveur.

Ce mémoire est structuré en trois chapitres encadrés par une introduction générale et une conclusion générale et perspectives :

— 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'Ido.

— Dans le deuxième chapitre, nous commencerons d'abord par la définition de l'authentification et la présentation de quelques méthodes. Ensuite, nous présenterons le principe de quelques méthodes d'élection.

— Dans le troisième chapitre nous l'avons consacré pour la réalisation, c'est-à-dire, l'implémentation d'un algorithme d'élection d'un serveur d'authentification dans l'internet des objets.

CHAPITRE 1
Généralité sur l'Internet des objets

1.1 Introduction

Le terme Internet des Objets (IdO) représente un mécanisme de communication entre des millions d'appareils. Dans l'IdO, des objets physiques, des objets virtuels et des dispositifs informatiques sont connectés les uns aux autres permettant à ces dispositifs d'accéder et de contrôler divers services à distance [5]. L'IdO désigne une informatique qui se fond dans notre quotidien pour nous simplifier la vie. Toutefois, certaines informations dont disposent les objets sont confidentielles, ce qui impose de grands défis en termes de sécurité des individus et des entreprises. Dans ce chapitre, nous présentons l'IDO ou bien IoT (Internet of things) définition, ses domaines d'applications, son fonctionnement, son architecture et les étapes pour la mise en place d'IdO, ainsi que quelques services de sécurité tels que la confidentialité, l'authentification et l'identification.

1.2 Définition

L'Internet des Objets (IdO ou IoT pour l'anglais Internet of Things) est défini comme un réseau mondial pour la société de l'information. Il permet de disposer des services évolués en interconnectant des objets physiques et virtuels grâce aux technologies interopérables de l'information et de la communication existantes ou futures. Ce réseau permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambigüité des entités numériques et des objets physiques. Ainsi, il est possible de récupérer, stocker, transférer et traiter les données sans discontinuité entre les mondes physiques et virtuels [6].

L'expression " Internet of Things " a été introduite pour la première fois par Kevin Ashton durant une présentation en 1999 [7]. En 1999, un groupe de recherche au Massachusetts Institute of Technology (MIT) a établi les premiers prototypes des identificateurs automatiques (RFID : Identification par Radio Fréquence) qui sont considérés comme un élément clé de la technologie de l'IdO. En 2005, L'union internationale de Télécommunications (ITU, Internation Telecommunication Union), un organisme de standardisation dans le domaine TELECOM publie un rapport technique consacré à l'IdO, qu'elle présente comme une nouvelle révolution de l'Internet. Selon l'UIT, l'Internet des Objets est défini comme (une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physique ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution). Au fil du temps, le terme a évolué et il englobe maintenant tout l'écosystème des objets connectés. Cet écosystème englobe, des fabricants de capteurs, des éditeurs de logiciels, des opérateurs historiques ou nouveaux sur le marché, des intégrateurs, etc.

La figure (Figure 1.1) montre l'architecture passée, présente et future de l'IdO.Outre les appareils ou les objets connectés, le concept d'IdO social (SIdO) émerge également. [8]

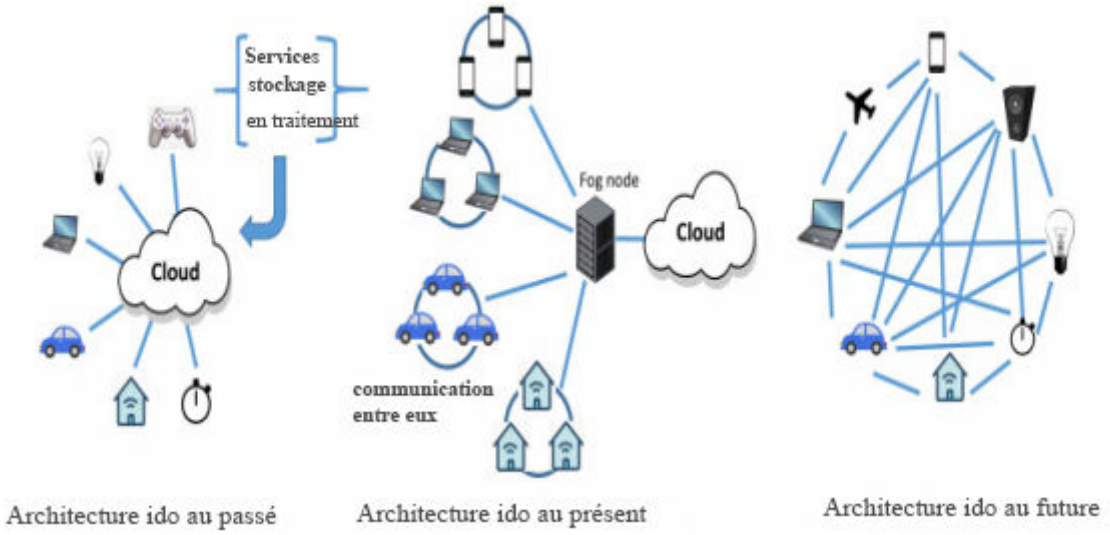

FIGURE 1.1 – Architecture actuelle et future de l' Ido.

1.3 Domaines d'application

Les domaines d'application de l'Ido sont très nombreux, et touchent pratiquement tous les axes de la vie quotidienne des individus, ce qui a permis l'émergence d'espace intelligents autour d'une informatique omniprésente [9]. Parmi ces domaines, nous citons quelques exemples :

1.3.1 Le système de santé électronique

L'internet des objets a rapidement transformé la prestation de soins. Les équipements et les capteurs sont de plus en plus " intelligents " et génèrent toujours plus de données nécessaires aux équipements médicaux, aux professionnels et profitant ainsi aux patients, en réduisant les coûts et en améliorant leur satisfaction. Les données ainsi collectées facilitent, adaptent, améliorent, anticipent ou réorganisent les soins des patients.

Dans le contexte de généralisation du traitement médical électronique, l'Internet des objets est fondamental. En effet, la conception d'un système intelligent de prise de décision clinique, matérialisé par le stockage des données collectées sur les patients et leur accessibilité universelle, procurerait au médecin un excellent appui durant la phase de traitement (voir la figure 1.2). L'internet des objets trouve donc tout son intérêt dans le domaine médical, et qui aussi peut améliorer le développement dans ce dernier. [10]

1.3.2 Les villes intelligentes

Beaucoup de grandes villes ont été soutenues par des projets intelligents, comme Séoul, New York, Tokyo, Shanghai, Singapour, Amsterdam et Dubaï. Les villes intelligentes (voir la figure 1.3) peuvent encore être considérées comme des villes de l'avenir et la vie intelligente, et par le taux d'innovation de la création de villes intelligentes d'aujourd'hui, il sera devenu très faisable pour entrer la technologie Ido dans le développement des villes.

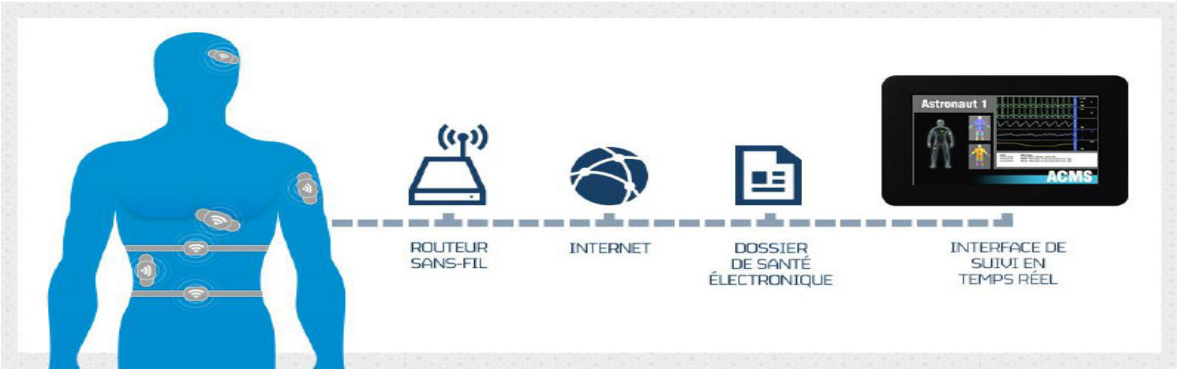

FIGURE 1.2 – Système de santé électronique

La demande exige une planification minutieuse à chaque étape, avec l'appui de l'accord des gouvernements, citoyens à mettre en œuvre la technologie d'Internet des objets dans tous les aspects. Par l'Ido, les villes peuvent être améliorées à plusieurs niveaux, en améliorant les infrastructures, en améliorant les transports dans les lieux de grande affluence, le suivi des caméras de télésurveillance publiques, etc . . . . . [**?**]

FIGURE 1.3 – Une ville intelligente

1.3.3 Le Smart Grid

L'un des domaines d'application de l'Ido est le secteur de la distribution d'énergie intelligente, dit « Smart Grid ». En France, ERDF (la gestion des réseaux de distribution en France) est très actif dans le développement de ce domaine, où un besoin clair en récupération d'information à différents points du réseau électrique est devenue nécessaire pour une meilleure intégration des différentes sources d'énergies et une meilleure gestion de la distribution jusqu'aux utilisateurs finaux [12].

1.3.4 Les Appareils Intelligents

Des appareils intelligents (voir figure 1.5) dans les soins de santé sont utilisés pour stocker et gérer les paramètres de soins clés et pour gérer les données sur les maladies

FIGURE 1.4 – Smart Grid

capturées. Ils sont principalement déployés pour fournir des solutions de conditionnement physique en suivant les activités ciblées et des dispositifs de diagnostic utilisés pour stocker des données de dispositifs. Principalement, ils sont utilisés comme des solutions de fitness pour suivi des activités du patient et des appareils de diagnostic intelligents tels que les dispositifs de tension matérielle, les podomètres, Google verre, etc. utilisé pour capturer les données des capteurs, pour une analyse plus approfondie par le médecin. [13]

FIGURE 1.5 – Des appareils intelligents

1.3.5 L'agriculture

L'agriculture intelligente a pour objet de renforcer la capacité des systèmes agricoles, de contribuer à la sécurité alimentaire en intégrant le besoin d'adaptation et le potentiel d'atténuation dans les stratégies de développement de l'agriculture durable.

Cet objectif a été atteint enfin par l'utilisation des nouvelles technologies, telles que l'imagerie satellitaire et l'informatique, les systèmes de positionnement par satellite de comme GPS, aussi par l'utilisation des capteurs qui vont s'occuper de récolter les informations utiles sur l'état du sol, taux d'humidité, taux des sels minéraux, etc. Et envoyer ces informations au fermier pour prendre les mesures nécessaires garantissant la bonne production [14].

1.3.6 IDO dans le domaine du sport

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 heures 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). [15]

1.3.7 La domotique

La domotique regroupe l'ensemble des technologies informatique, électrotechnique et électronique, qui permettant l'automatisation des équipements d'un habitat et transforment une maison en une mais intelligente. C'est l'ensemble des techniques visant à intégrer à l'habitant tous les automatismes en matière de sécurité (comme les alarmes), de gestion de l'énergie (optimisation de l'éclairage et du chauffage etc.), de communication (contacts et discussion avec des personnes extérieures), etc [16].

1.3.8 Le transport et la mobilité intelligente

Le développement du transport est l'un des facteurs qui indiquent le bien-être de pays.

Une application de surveillance de l'état des routes et d'alerte est l'un des applications les plus importantes de l'Ido. Le processus a besoin de l'identification de l'utilisateur et son trajectoire souhaité dans son application sur son téléphonique intelligents.

Le transport intelligent consiste en : l'analyse des transports, le contrôle des véhicules connectées. L'analyse de transport représente l'analyse de la prédiction de la demande et de détection anomalie. Le routage des véhicules et le contrôle de la vitesse en plus de la gestion du trafic sont tous connu comme le contrôle du transport qu'ils ont réellement étroitement lié aux véhicules connecté, et globalement régie par la diffusion multi-technologie comme montre la figure 1.6. [16]

FIGURE 1.6 – Les aspects de transport intelligent

1.3.9 L'industrie

Le déploiement de l'Ido dans l'industrie sera certainement un support pour le développement de l'économie et du secteur des services, puisque. L'Ido il permettra d'assurer un suivi total des produits, de la production à la distribution, par la gestion automatisée, la surveillance à distance, et le renforcement de la comptabilité. Il compte de développer les techniques de production en entreprises ainsi que le renforcement des capacités de gestion. Donc La technologie Ido permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production et en plus améliorer la sécurité des employés [17].

1.4 Les étapes pour la mise en place de l'IdO

Pour créer un objet connecté, voici 6 étapes incontournables à prendre en compte pour réussir un projet Ido. [18]

1.4.1 L'élément central du projet Ido : l'objet

Boitier inséré dans un véhicule pour surveiller les déplacements, capteur permettant de mesurer les éléments de température ou de pression d'un équipement industriel, ou encore pour gérer des matériels médicaux dans les hôpitaux (maintenance, taux d'utilisation...). L'objet connecté peut être représentatif d'éléments extrêmement différents et diversifiés. La première étape est donc d'acquérir, ou de construire le cas échéant, l'objet adapté aux contraintes physiques du cas d'usage de l'entreprise. [18]

1.4.2 La connectivité pour la communication des objets connectés

L'objectif est de le rendre communiquant. Si l'objet capte les données, elles n'ont aucun sens si elles ne sont pas transférées. Un ensemble de solutions de connectivité existe pour faire 'parler' l'objet. En fonction de la nature de l'objet et des données qu'il capte, il faudra choisir le bon réseau : 2G/3G/4G. [18]

1.4.3 La collecte de l'ensemble des données

Face à la multitude des objets, la collecte et la modélisation de l'ensemble des données produites est un point crucial. Pour les traiter, toutes les données doivent être collectées et traitées afin d'être exploitable et ce à travers un seul outil simple et ergonomique. [18]

1.4.4 L'hébergement et le stockage des données

Les données doivent être stockées, gérées et administrées en toute sécurité. Face à la criticité des données (exemple données de santé ou de géolocalisation), il est important de bénéficier d'une infrastructure qui garantit la sécurité des données et qui soit en mesure de s'adapter à la montée en charge du projet.[18]

1.4.5 Le développement de logiques applicatives

Pour donner un sens aux données collectées et en dégager toute la valeur (optimisation de l'activité de l'entreprise, fidélisation de ses clients ou encore proposition de nouveaux services innovants), il faut pouvoir les utiliser et les lier entre elles. Cela se traduit par le développement et la mise en œuvre d'une application Ido. Au travers d'une telle application, l'entreprise peut utiliser au mieux ces données et piloter les objets ou les processus. [18]

1.4.6 La restitution des données captées par les objets connectés

Pour proposer ces nouveaux services innovants à ses clients, l'entreprise doit mettre une interface à leur disposition pour interagir avec eux. Cette application Ido, proposée sous forme d'interface web, d'application mobile permet de partager les données avec ses clients ou ses fournisseurs, en toute simplicité et d'améliorer l'expérience client par exemple. [18]

1.5 Architecture de l' IDO

L'architecture de l' Ido n'est pas standardisée, l'architecture typique de l'Ido a trois couches : perception, réseau et application comme le montre la figure 1.7. [19]

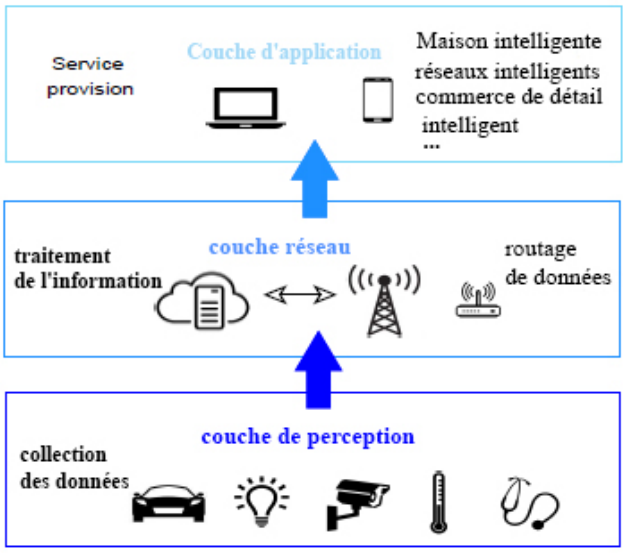

FIGURE 1.7 – Les trois couches d' Ido

1.5.1 Couche de perception

La couche de perception comprend différents dispositifs Ido physiques ; elle est responsable de l'interaction entre les dispositifs et la collecte de données Ido. La collecte de données est effectuée en utilisant des dispositifs intelligents tels que des identificateurs de radiofréquence étiquettes et **capteurs de cation** (RFID). [19]

1.5.1.1 Les capteurs sans fil

Les capteurs sans fil jouent un rôle essentiel dans l' Ido en fournissant des services de détection et de communication. Un réseau de capteurs sans fil (WSN) se compose d'un grand nombre de capteurs intelligents déployés dans des environnements éloignés pour détecter et recueillir des données telles que la température, l'humidité, les vibrations, etc. Les données détectées sont transmises par un ou plusieurs-se rendre à une passerelle/station de base, comme le montre la figure 1.8.

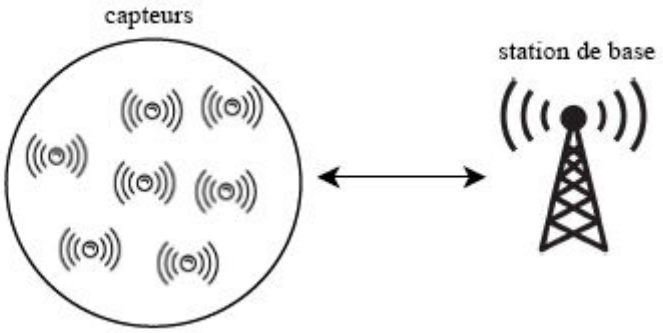

FIGURE 1.8 – Capteur sans fil

1.5.1.2 Identification par radiofréquence (RFID)

La technologie RFID est un élément majeur de l' Ido en raison de son identification, de son suivi et de sa surveillance des objets [20]. Un système RFID se compose d'un transpondeur de signal radio (tag) qui stocke une identité d'objet unique et un lecteur d'étiquettes qui identifie l'objet à travers les ondes radio. Le lecteur d'étiquettes transfère le numéro d'identification à un ordinateur pour suivre et surveillez l'objet comme le montre la figure 1.9.

FIGURE 1.9 – Le system de RFID

1.5.2 Couche réseau

La couche réseau traite les données collectées fournies par la couche perception et stocke ou envoie les données à la couche application. C'est la couche la plus importante d'architecture Ido car elle intègre diverses technologies de communication qui permettent la connectivité des appareils Ido. Les technologies de communication largement utilisées comprennent : Zig Bee, Bluetooth basse énergie (BLE), IPv6 sur les réseaux personnels sans fil de faible puissance (6LoWPAN) et le réseau étendu à longue portée (LoRaWAN). [19]

1.5.2.1 Zig Bee

Zig Bee est une technologie de communication sans fil conçue pour les communications de courte portée [**?**]. Il peut être utilisé dans les maisons intelligentes, les compteurs intelligents et les soins de santé intelligents. La pile de protocoles Zig Bee comprend des couches de contrôle d'accès physiques et moyennes basées sur la norme IEEE 802.15.4, une couche réseau et une couche application.

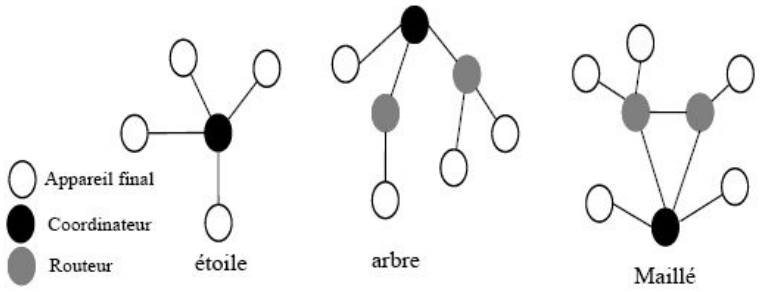

FIGURE 1.10 – La technologie Zig Bee

1.5.2.2 BLE

BLE est une technologie de communication à courte portée qui réduit la consommation d'énergie comparé au Bluetooth classique [22]. Il est largement utilisé dans les systèmes de véhicules Ido. BLE dispose d'une pile de protocoles composée de couche physique, couche de contrôle d'accès moyen, contrôle de liaison logique et protocole d'adaptation et protocole d'attribut. Le BLE adopte une topologie étoile, y compris les dispositifs maîtres et esclaves, comme le montre la figure 1.11. Chaque nœud esclave est associé à un seul nœud maître. Le nœud maître est responsable de lancer la communication et fournir un tableau de planification en fonction de la répartition du temps multiple accès.

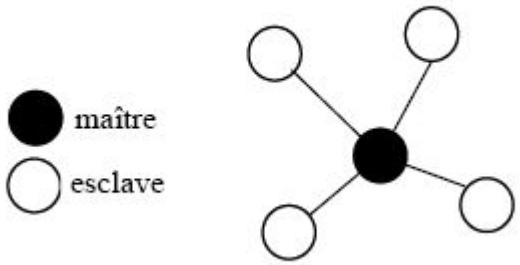

FIGURE 1.11 – La technologie BLE

1.5.2.3 6LoWPAN

6LoWPAN combine la dernière version du protocole Internet (IPv6) et réseau personnel sans fil faible puissance [23]. Il permet aux appareils de transmettre des

données via des canaux sans fil utilisant IPv6. Il est adapté pour les dispositifs à ressources limitées parce qu'ils réduisent les coûts de transmission, favorisent la mobilité, etc. Les cas d'utilisation les plus courants de 6LoWPAN sont la maison intelligente, l'agriculture intelligente et l'Ido industriel. Par rapport à Zig Bee, un appareil 6LoWPAN peut communiquer avec un autre appareil 6LoWPAN ou IEEE 802.15.4. Il peut également communiquer avec un réseau basé sur IP tel que le Wi-Fi comme présenté dans la figure 1.12.

La spécification du défi 6LoWPANnes une pile de protocoles complète composée de couches PHY et MAC basées sur la norme IEEE 802.15.4, la couche NWK, la couche transport et la couche APP [24].

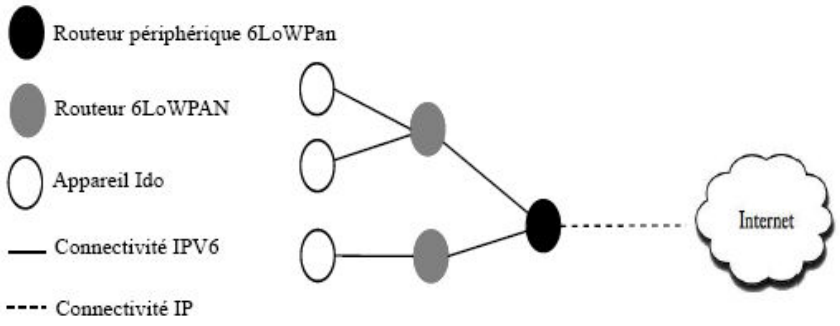

FIGURE 1.12 – L'architecture de 6LoWPAN

1.5.2.4 LoRaWAN

LoRaWAN est un protocole de communication longue portée conçu pour les applications Ido à faible puissance et évolutives de l'Ido [25]. Comme l'illustre la figure 1.13, un réseau LoRaWAN est constitué d'appareils finaux, de passerelles et d'un serveur unique dans une topologie en étoile ou en étoile de l'étoile.

Les périphériques finaux peuvent communiquer avec une ou plusieurs passerelles en utilisant le schéma ALOHA par le biais des liens à un saut. Les passerelles sont connectées au serveur du réseau via le protocole Internet. Les communications sont bidirectionnelles et initiées par le dispositif d'extrémité.

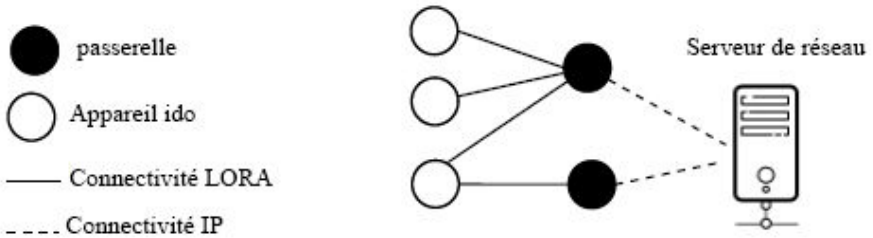

FIGURE 1.13 – architecture LORAWAN

1.5.3 La couche application

La couche application reçoit les données de la couche réseau et fournit les services requis aux utilisateurs Ido. Il prend en charge une grande variété d'applications telles

que la maison intelligente, la vente au détail intelligente, les grilles intelligentes, etc. Les protocoles d'application les plus courants sont le protocole d'application contraint (CoAP) et le transport de télémétrie par file d'attente de messages (MQTT).[19]

1.5.3.1 CoAP

Les appareils Ido étant limités en ressources, le protocole HTTP n'est pas adapté aux appareils à faible consommation en raison de sa complexité. CoAP a été conçu pour inclure les caractéristiques de HTTP dédiées aux dispositifs Ido. Comme le montre la figure 1.14, CoAP est un protocole de messagerie basé sur l'architecture REST. Il comporte quatre types de messages : confirmable, non confirmable, accusé de réception et réinitialisation. Il offre des fonctionnalités qui ne sont pas disponibles sur HTTP, comme la notification push.

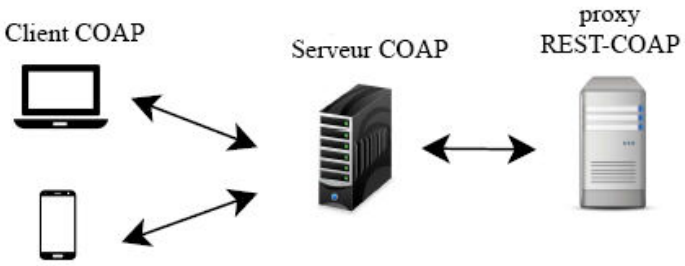

FIGURE 1.14 – architecture CoAP

1.5.3.2 MQTT

MQTT est un protocole de messagerie léger qui assure la connectivité des réseaux et des utilisateurs avec des applications. Il est basé sur une architecture de publication/abonnement où le système se compose de trois éléments principaux : les éditeurs, les abonnés et un courtier, comme le montre la présenté à la figure 1.15. Dans le contexte de l' Ido, les éditeurs sont des dispositifs intégrés qui envoient des données au courtier. Envoient des données au courtier et les abonnés sont des serveurs d'applications.

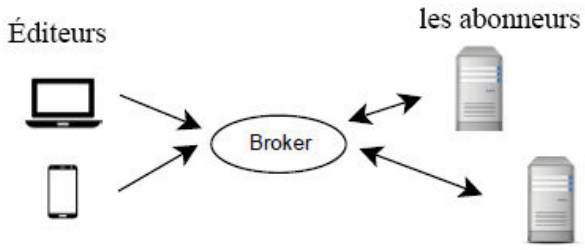

FIGURE 1.15 – architecture de MQTT

1.6 La sécurité dans internet des objets

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 [15], [26].

1.6.1 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 [26].

1.6.2 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 [26].

1.6.3 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 [26].

1.6.4 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 [26].

1.6.5 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 [15].

1.7 Conclusion

L'Ido a suscité une attention considérable ces dernières années, car il a apporté des changements révolutionnaires dans la vie humaine.

L'Ido permet l'échange d'informations dans une grande variété d'applications telles que les bâtiments intelligents, la santé intelligente, le transport intelligent, etc.

Dans ce chapitre, nous avons présenté l'Ido, ses domaines d'application ainsi que son fonctionnement. En outre, nous avons passé en revue différentes applications offertes par le paradigme de l'Ido et discuté des principaux éléments et protocoles intégrés dans l'architecture Ido à trois couches.

Dans le chapitre suivant, nous nous concentrons sur le principe de l'élection et l'authentification.

CHAPITRE 2

Authentification et élection dans l'Internet des objets

2.1 Introduction

Dans un monde où «les choses» et les dispositifs sont interconnectés à tous les niveaux, la sécurité joue un rôle central sans marge d'erreur ou de pénurie en matière d'approvisionnement. La sécurisation, y compris l'authentification de ces dispositifs, deviendra la priorité de tous, des fabricants aux fournisseurs de silicium (ou développeurs IP), aux développeurs de logiciels et d'applications, et au consommateur final, les bénéficiaires de la «recette» de sécurité qui accompagnera ces produits Ido. Ensemble, tous les consommateurs de ces produits doivent s'adapter aux exigences du marché, innover et améliorer les processus, saisir de nouvelles compétences et apprendre de nouvelles méthodes, accroître la sensibilisation et adopter de nouveaux programmes de formation et de programmes.

Ce chapitre est divisé en deux parties. La première sera consacrée à la présentation de quelques solutions d'authentification afin d'établir des clés dans l'Internet des Objets. La deuxième partie introduit le concept d'élection et ses algorithmes.

2.2 L'élection

L'Ido 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'élection d'un leader est une nécessité fondamentale pour les systèmes distribués.

2.2.1 Introduction sur l'élection

Le problème de l'élection est de partir d'une configuration dans laquelle tous les processus sont dans le même état pour arriver dans une configuration dans laquelle un seul processus est dans l'état "gagnant" et tous les autres dans l'état "perdant". [34]

2.2.2 Priorité et vocabulaire

Un algorithme d'élection est un algorithme qui satisfait les trois propriétés suivantes :

— Chaque processus exécute le même algorithme : symétrie complète.

— L'algorithme est décentralisé : une exécution peut être commencée par un nombre quelconque de processus.

— L'algorithme atteint une configuration terminale dans laquelle il existe exactement un processus "gagnant" et tous les autres processus sont "perdants".

La dernière propriété est quelquefois relâchée en : il existe un seul processus gagnant. Le processus 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 processus gagnant diffuse le résultat aux autres processus.

Dans les algorithmes que nous étudions, chaque processus possède un nom unique qui peut être compare ($=$, $>$, $<$, $\leq$ ou $\leq$) avec les identifiants des autres processus du

système reparti. Enfin, chaque processus possède une variable *statep* pouvant contenir les valeurs *gagnant* et *perdant*.

Certaines fois, la variable statep est égale a dormant avant que le processus n'ait exécute une étape de l'algorithme et candidat lorsque le processus participe à l'algorithme mais ne sait pas encore s'il est gagnant ou perdant. [12]

2.2.3 Algorithmes d'élection de leader dans les systèmes répartis

2.2.3.1 Election sur un anneau

Algorithme de LeLann :

Cet algorithme a été proposé par Le Lann en 1977 pour des anneaux unidirectionnels FIFO. L'algorithme possède une complexité en nombre de messages en O(n2), avec n le nombre de processus. Chaque initiateur calcule l'ensemble des identifiants des processus de l'anneau, l'initiateur avec l'identifiant le plus petit est 'gagnant'. Chaque initiateur p émet un message ⟨jeton, p⟩ contenant son identifiant, le message ⟨jeton, p⟩ est propage sur l'anneau. Les canaux sont supposés FIFO et un initiateur p doit générer son message ⟨jeton, p⟩ avant qu'aucun autre message ⟨jeton, q⟩ ne soit reçu. Lorsqu'un initiateur p reçoit son message ⟨jeton, p⟩, les messages ⟨jeton, q⟩ de tous les autres processus ont visité p. p peut alors connaitre l'identifiant du processus 'gagnant'. Avant qu'un processus ne reçoive le premier message ⟨jeton, p⟩, s'il veut participer à l'élection en étant candidat, il doit avoir commencé à exécuter l'algorithme en se considérant comme un initiateur.[34]

Algorithme 1: Algorithme LeLann

```
Var   Listep sous-ensemble de P init{p}
etap(init, leader, perdu, sleep) ;
Debut
    si (p est intiateur) alors
        etap := init ;
        envoie <tok, p> à Suivantp ;
        reçoit < tok, q> ;
        tant que q ≠ p faire
            Listep := Listep ∈ {q} ;
            envoie <tok, p> à Suivantp ;
            reçoit <tok, p> ;
            si (p = max(Listep)) alors
                etap := leader ;
            sinon
                etap := perdu ;
            fin
        fin
    sinon
        tant que Vrai faire
            reçoit <tok, q> ;
            envoie <tok, q> à Suivantp ;
            si etap = sleep alors
                etap := perdu ;
            fin
        fin
    fin
Fin
```

Algorithme de Chang et Robert (1979)

Cet algorithme est une évolution de l'algorithme de Lelan, il supprime les jetons des processus qui ne sont pas élus : ceux qui ont un numéro de processus plus petit.[41]

Algorithme 2: Algorithme de Chang et Robert

```
Var  etap
Debut
    si (p est intiateur) alors
        etap := cand ;
        envoie <tok, p> à Suivantp ;
        tant que etap ≠ leader faire
            reçoit <tok, q> ;
            si (q = p) alors
                etap := leader ;
            sinon
                si (q > p) alors
                    si (etap = cand) alors
                        etap := perdu ;
                        envoie <tok, q> à Suivantp ;
                    fin
                fin
            fin
        fin
    sinon
        tant que Vrai faire
            reçoit <tok, q> ;
            envoie <tok, q> à Suivantp ;
            si etap = sleep alors
                etap := perdu ;
            fin
        fin
    fin
Fin
```

2.2.3.2 Election sur un réseau complet

- **Algorithme de Bully (Garcia-Molina) :** [41]

— **Déclenchement :** quand un processus P 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 P :** P envoi un message ELECTION à tous les autres processus dont le numéro est plus grand que le sien

— Réception d'un message ELECTION depuis P par un processus Q.

— Le processus Q envoie un message ACK à P lui signant qu'il est actif.

— A son tour Q, lance une élection si ce n'est pas déjà fait.

- **Sur le processus P**

— Si aucun processus ne lui répond avant TEMPO, P gagne l'élection et devient le coordinateur.

— Si un processus de numéro plus élevé répond, c'est lui qui prend le pouvoir.

— Le rôle de P est terminé.

— **Annonce de l'élu :** le nouveau coordinateur envoie un message à tous les participants pour les informer de son rôle. L'application peut alors continuer à s'exécuter réveil d'un processus inactif.

— 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.

2.2.3.3 Election sur un arbre

- **L'algorithme général d'élection** [3]

— Un (ou plusieurs) processus détecte la panne du coordinateur.

— Il informe l'ensemble de processus 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 l'arbre, l'élection commence.

— Les feuilles émettent un message.

— Le processus ayant le plus grand numéro est élu.

Var wsp : booléen init faux (wsp est vrai si p est réveillé)
wrp : integer init 0 (compte les messages de reveil reçus) reqp[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

Algorithme 3: Partie Réveil

```
Debut
    si (p est intiateur) alors
        WSp := vrai ;
        pour q ∈ Neighq faire
            Envoie <wakeup> à q ;
        fin
    fin
    tant que wrp < Vp faire
        Recoit <wakeup> ;
        si (wsp = faut) alors
            wsp := vrai ;
            pour q ∈ Neighq faire
                envoie <wakeup> à q ;
            fin
        fin
    fin
Fin
```

Algorithme 4: Partie élection

```
Debut
    tant que #((q : reqp[q]) = faux) > 1 faire
        Reçoit <tok, r> de q ;
        reqp[q] := vrai ;
        vp := max(vp, r) ;
        Envoie <tok, vp> à q_0 tel que reqp[q_0] est faux ;
        Reçoit <tok, vp> de q_0 ;
        vp := max(vp, r) ;
        si (vp = p) alors
            Statep := leader ;
        sinon
            Statep := lost ;
        fin
        pour q ∈ Neighp, q ≠ q_0 faire
            envoie <tok, vp> à q ;
        fin
    fin
Fin
```

2.2.3.4 Election sur topologie du réseau quelconque [42]

— Le réseau est modélisé par un graphe connexe.

— Les liaisons sont unidirectionnelles.

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

— Un processus ne connaît que ses voisins et n'apprend jamais la structure globale

du réseau.

```
Debut
| Lors de décision de lancer une élection faire
  si état i = initial alors
  | lancer-exploration
  fin
| fait
| Lors de réception de explorer(7c, z, s) depuis Pi faire
  cas
      Pgvu i > k :
      si étatt = initial alors
      | lancer-exploration
      fin
      Pgvu i < k : étatt := battu ;
      Pgvu i := k ;
      Pgvu i := j ;
      Soit y = voisins i z ;
      Cas y = ∅ -> succi := 0 ;
      Cas s = ∅ -> envoyer conclure à Pi
          s ≠ envoyer rebrousser (k, z U i, s) à Pi
      fcas
      y ≠ ∅ -> soit x = maximum(y) ;
          succ i := x ;
          envoyer explorer (k, z U i, s U y-x) à Px
      fcas
  fcas
| fait
Fin
```

```
Debut
| Lors de réception de rebrousser(k, z, s) depuis Pi faire
  si pgvut = k alors
  |   soit y = voisin Si ∩ s ; (a 3)
  |   cas j := ∅ -> envoyer rebrousser (k, z, s) à Pi
  |     y ≠ ∅ -> soit x = maximum(y) ;
  |     succi := succi i ∪ x ;
  |     envoyer explorer (k, z, s-x) à Px
  |   fcas
  fin
| fait
| Lors de réception de conclure depuis Pi faire
  si pgvui = i alors
  | étatt := élu ;
  fin
  V x£ (succ i ∪ pred i)-j : envoyer conclure à Px
| fait
Fin
```

2.3 L'Authentification

2.3.1 Définition

L'authentification est le processus de vérification de l'identité d'une entité. L'authentification est la première phase de toute mécanisme de contrôle d'accès qui peut déterminer l'identité exacte de la partie accédant afin d'établir la confiance du système.

Dans la plupart des cas, l'authentification est initiée entre un humain et une machine dans un processus pour se connecter au portail bancaire Internet en entrant les identifiants. Toutefois, dans ce scénario, l'entité qui sollicite l'accès n'a pas de garantie quant à l'identité de l'entité qui accorde l'accès. Afin de surmonter cette préoccupation, l'authentification mutuelle doit être établie entre les entités, en vérifiant l'identité de l'entité octroyant l'accès avec la participation d'un TTP (tiers de confiance), tel qu'une autorité de certification. [27]

2.3.2 L'authentification mutuelle

L'authentification mutuelle ou l'authentification bidirectionnelle (à ne pas confondre avec l'authentification à deux facteurs) désigne le fait que deux parties s'authentifient en même temps dans un protocole d'authentification. C'est un mode d'authentification par défaut dans certains protocoles (IKE, SSH) et optionnel dans d'autres (TLS).

L'authentification mutuelle est une caractéristique souhaitée dans les schémas de vérification qui transmettent des données sensibles, afin d'assurer la sécurité des données. L'authentification mutuelle peut être effectuée avec deux types d'identifiants : les noms d'utilisateur et les mots de passe, et les certificats de clé publique.

L'authentification mutuelle est souvent utilisée dans l'Internet des objets (Ido). La rédaction de schémas de sécurité efficaces dans les systèmes Ido peut devenir difficile, en particulier lorsque les schémas doivent être légers et avoir des coûts de calcul faibles. L'authentification mutuelle est une étape de sécurité cruciale qui peut se défendre contre de nombreuses attaques antagonistes, qui autrement peuvent avoir de grandes conséquences si les systèmes Ido (tels que les serveurs de soin e-médecine) sont piratés. Le manque d'authentification mutuelle a été considéré comme une faiblesse des schémas de transmission des données. [28]

2.3.3 Étapes de base pour l'authentification

Les étapes de base courantes pour l'authentification sont les suivantes [29] :

— Étape 1 : le demandeur n'est pas authentifié.

— Étape 2 : étape de connexion : le demandeur d'asile demande au système d'information d'utiliser une fonction qui nécessite une authentification. Le système d'information demande au contrôleur d'authentifier le demandeur.

— Étape 3 : étape d'authentification, le demandeur est authentifié et une session est ouverte. Le système d'information fournit à l'utilisateur les fonctions requises.

— Étape 4 : étape de déconnexion, l'utilisateur se déconnectée du moniteur et l'état revient à l'étape initiale. Cette étape peut être initiée sur un temps mort ou par une action de l'utilisateur.

2.3.4 Les types d'authentification

2.3.4.1 Authentification par mot de passe :

ce type d'authentification exige que le fournisseur se rappelle ce qu'il sait. Il y a deux parties dans cette méthode. Premièrement, le fournisseur entre le nom d'utilisateur et, deuxièmement, le mot de passe. Le mot de passe est la combinaison secrète de mots et de chiffres que le fournisseur connaît. [30]

2.3.4.2 Authentification par carte à puce :

l'authentification par carte à puce est un facteur qu'un utilisateur a. Une carte à puce est une carte de la taille d'une carte de crédit qui a un certificat intégré utilisé pour identifier le titulaire. L'utilisateur peut insérer la carte dans un lecteur de carte à puce pour authentifier l'individu. Les cartes à puce sont couramment utilisées avec un NIP fournissant l'authentification multifactorielle. En d'autres termes, l'utilisateur doit avoir quelque chose (la carte à puce) et savoir quelque chose (le PIN) [31], [32].

2.3.4.3 Authentification biométrique :

les méthodes biométriques fournissent ce que vous êtes facteur d'authentification. L'authentification biométrique est une méthode qui identifie un utilisateur et/ou vérifie son identité en fonction de la mesure de ses caractéristiques physiologiques ou comportementales uniques. La biométrie physiologique est l'empreinte digitale, la reconnaissance faciale, la géométrie de la main. La biométrie comportementale est la reconnaissance vocale, la démarche et le balayage de la signature. Les empreintes digitales et les empreintes de mains sont la méthode biométrique la plus utilisée aujourd'hui.[33]

2.3.4.4 Authentification par certificat numérique :

un certificat numérique est une technologie de chiffrement qui fonctionne comme la version Internet d'un passeport. À l'aide d'une clé publique et d'une clé privée, les certificats numériques permettent essentiellement de s'assurer que le message provient d'une personne en particulier. Le certificat numérique authentifie l'identité de l'expéditeur pour assurer une communication plus sûre et prévenir la fraude sur Internet. Les plus grands avantages de l'authentification numérique basée sur les certificats sont la confidentialité. En cryptant vos communications, courriels, ouvertures de session ou transactions bancaires en ligne, les certificats numériques protègent les données privées et empêchent les renseignements d'être vus par des yeux involontaires. Les systèmes de certificats numériques sont également conviviaux, fonctionnent généralement automatiquement et nécessitent un minimum d'action ou de participation de la part des expéditeurs ou des destinataires. [34]

2.3.5 Protocoles d'authentifications

Chaque protocole d'authentification a sa propre méthode pour authentifier un utilisateur ou une machine. Ils utilisent différents algorithmes et différentes techniques. Cependant, ils ont tous presque le même principe de fonctionnement (basé sur la clé).

On va classer les protocoles étudiée à deux catégories principales. D'un côté y'a des protocoles base sur la cryptographie symétrique qui utilise un seul clé pour le chiffrement et le déchiffrement ; et dans l'autre côté nous avons des protocoles basée sur la cryptographie asymétrique qui utilise deux clé (le premier est public pour le chiffrement et le deuxième est privée pour le déchiffrement).

2.3.5.1 Protocoles basés sur la cryptographie symétrique utilisant une carte à puce

Protocole d'authentification et d'accord clé basé sur la cryptographie symétrique et une carte à puce [35]

Ce protocole comprend quatre phases : phase d'enregistrement, phase de connexion, phase d'authentification et phase de changement de mot de passe.

- **La phase d'enregistrement :** dans cette phase l'utilisateur Ui s'enregistre sur le serveur Si. Ui choisit d'abord son identifiant ID et son mot de passe Pwi.
- **La phase de connexion :** Lorsqu'un utilisateur enregistré Ui veut accéder aux services de Si, il insère sa carte à puce SCi dans un terminal et saisit son identité et son mot de passe Pwi.
- **La phase d'authentification :** Si et Ui procèdent à des calculs pour s'authentifier mutuellement, âpres ils avoir une clé de session commune.
- **La phase de changement de mot de passe :** cette phase est réalisée lorsque Ui souhaite remplacer son ancien mot de passe PWi par un nouveau, la carte SCi décide si la demande de changement de mot de passe est acceptable ou non.

Un système d'authentification et d'accord clé basé sur une carte à puce et un noeud de passerelle pour l'Ido [36]

Ce protocole est composé de quatre phases :

- **La phase de pré-déploiement :** pendant la phase de pré-déploiement, chaque nœud de capteur régulier est prédéfini avec son identité SID et une clé de mot de passe sécurisée XGWN générée au hasard, qui est partagé avec le GWN et stocké dans la mémoire du noeud. Le GWN est prédéfini avec une clé de mot de passe hautement sécurisée générée de manière aléatoire Xgwn.
- **La phase d'enregistrement :** deux phases d'enregistrement distinctes sont nécessaires après le déploiement. La première est une phase d'enregistrement entre GWN et un nœud de capteur régulier correspondant Sj, et après le déploiement. La deuxième phase d'enregistrement est entre une interface utilisateur et le GWN, et est initié par l'utilisateur sur demande.

— **La phase de connexion :** Après la phase d'enregistrement, l'utilisateur peut se connecter à un nœud de capteur désiré du réseau en lançant une phase d'authentification. Dans l'ordre de la phase d'authentification pour être lancé, l'utilisateur doit d'abord se connecter. Comme mentionné, le système utilise une carte à puce (SC) pour l'utilisateur de s'inscrire et s'authentifier. Tout autre système de sécurité pour l'enregistrement sécurisé des données d'un utilisateur pourrait être utilisé à la place.

— **La phase d'authentification :** cette phase est initiée par l'utilisateur avec une authentification message à la fin d'une phase de connexion exécutée avec succès.

L'utilisateur envoie le message d'authentification à un nœud de capteur souhaité du réseau et non le GWN. L'objectif de cette phase est de négocier une clé de session secrète entre l'utilisateur et le nœud du capteur d'une manière qui contribuera individuellement à la clé de la session avec un nonce secrètement choisi. Après avoir négocié avec succès la clé de session, ils peuvent l'utiliser pour communiquer en toute sécurité dans toute matière cryptée. Afin de réaliser la session sécurisée négociation clé, une méthode d'accord clé légère est proposée qui implique une authentification mutuelle entre toutes les parties.

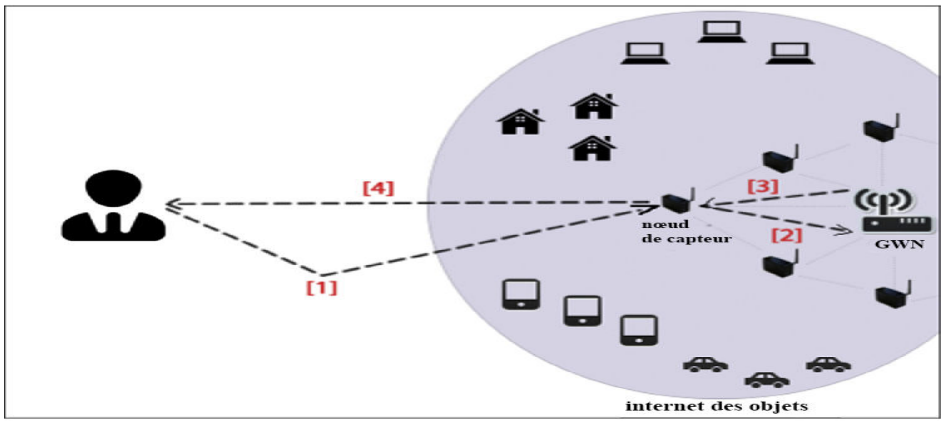

FIGURE 2.1 – Un système d'authentification et d'accord clé basé sur une carte à puce et un noeud de passerelle pour l'Ido

Un système d'authentification et d'accord clé basé sur une carte à puce et un noeud de passerelle pour l' Ido (UAKAS) [37]

Ce Système d'authentification des utilisateurs et d'accord clé (UAKAS) basé sur le modèle de Turkanov'c où résoudre et éliminer toutes les lacunes et vulnérabilités.

Il comprend trois phases :

— **La phase de pré-déploiement :** pour qu'un WSN(Wireless sensor network) puisse être activé, une phase de pré-déploiement est nécessaire. Selon le schéma de Turkanovi'c, cette phase est effectué hors ligne par un administrateur réseau. Chaque nœud de capteur du WSN est prédéfini avec son identité SIDj et un mot de passe sécurisé XGWN-Sj qui est partagé avec le GWN. Les deux variables sont stockées dans la mémoire d'un nœud de capteur Sj.

— **La phase d'enregistrement :** cette phase est divisée en deux parties : la phase d'enregistrement de l'utilisateur et la phase d'enregistrement du nœud de capteur. Le processus d'enregistrement de l'utilisateur ce fait via le canal protégé par le GWN, et le résultat est que l'utilisateur utilise une carte à puce pour s'inscrire. Avant de commencer l'authentification, l'utilisateur Ui doit se connecter. Cela se fait hors ligne via la carte à puce SC.

— **La phase de connexion et d'authentification :** après une connexion réussie, SC prépare le processus d'authentification. Le but de la phase d'authentification est de permettre l'utilisateur négocie la clé de session secrète avec un nœud de capteur spécifique sans contacter le GWN. La clé de session sera ensuite utilisée pour une communication sécurisée (requête, réponse) entre l'utilisateur et le nœud capteur, et sera construite par les deux parties.

2.3.5.2 Protocoles basés sur la cryptographie asymétrique basés sur ECC

Un système d'authentification et d'établissement de clé utilise des certificats implicites (CA) basés sur ECC [38]

Le schéma d'authentification proposé pour les applications WSN dans l' Ido distribué comprend deux phases.

— **La phase d'enregistrement :** les dispositifs de bordure du réseau (p. ex., nœuds de capteurs) et les utilisateurs finaux demandent des justificatifs de sécurité et des certificats à l'autorité de certification (AC). Le rôle de la phase d'enregistrement est d'établir une communication authentifiée, où le nœud capteur et l'utilisateur final doivent avoir un certificat implicite d'une suite de chiffrement spécifique, et le nœud capteur demande des informations de sécurité et un certificat de sécurité.

  Dans un premier temps, le client envoie une suite de chiffrement de message, qui inclut un certificat implicite Appelez le serveur. Le serveur accepte la suite de chiffrement et répond par un message, ou supprime la poignée de main.

— **La phase d'authentification :** Afin d'établir une communication authentifiée, les nœuds de bordure et les utilisateurs finaux devraient posséder des certificats implicites pour des suites de chiffrement particulières. Plusieurs transferts de message de la phase d'authentification entre le nœud client et le nœud serveur est considérée.

Le client envoie son certificat accompagné d'un nonce cryptographique aléatoire et la valeur MAC. Si la vérification MAC réussit, le serveur calcule la clé publique du client (QU) à l'aide du certificat CertU reçu et de la clé publique de l'AC (QCA). Semblable au côté serveur, le client vérifie MAC, calcule la clé publique du serveur, et dérive la clé commune en utilisant sa propre clé privée et la clé publique du serveur : KUV = dUQV .

À la fin, les deux nœuds de bord (clients) peuvent s'authentifier, et établir une clé secrète commune et une liaison de communication pouvant être utilisée pour sécuriser d'autres acquisitions de données entre le client et le serveur.

Protocole d'authentification basé sur le hashing et l'extraction des fonctionnalités [39]

Ce protocole est basé sur l'algorithme de hachage SHA et l'extraction de fonction et la cryptographie de la courbe elliptique ECC. Il contient trois parties principales :

— **La phase d'installation :** dans cette phase, certains facteurs nécessaires sont pré-distribués au nœud de la plateforme et du terminal. De la figure 2.2 nous pouvons voir que les facteurs dans le côté du nœud de terminal y compris ID, compte, etc... Et les facteurs du côté de la plateforme, y compris toutes les informations concernant le nœud terminal. Afin de comprendre clairement le schéma, nous besoin de faire quelques explications.

— **Vérification AC :** Comme nous l'avons expliqué dans la partie précédente, il existe un centre CA peut être utilisé en toute sécurité pour vérifier les certificats des deux plateformes et le nœud terminal. L'authentification du certificat méthode est la même que celles existantes.

— **L'authentification mutuelle :** Le système d'authentification mutuelle proposé est asymétrique pour les nœuds de plateforme et de terminal. En général, la plateforme a des structures relativement plus complexes et des capacités de processus plus élevées par rapport au nœud terminal, il est donc très difficile pour l'attaquant de prétendre être une fausse plate-forme pour communiquer avec le nœud terminal.

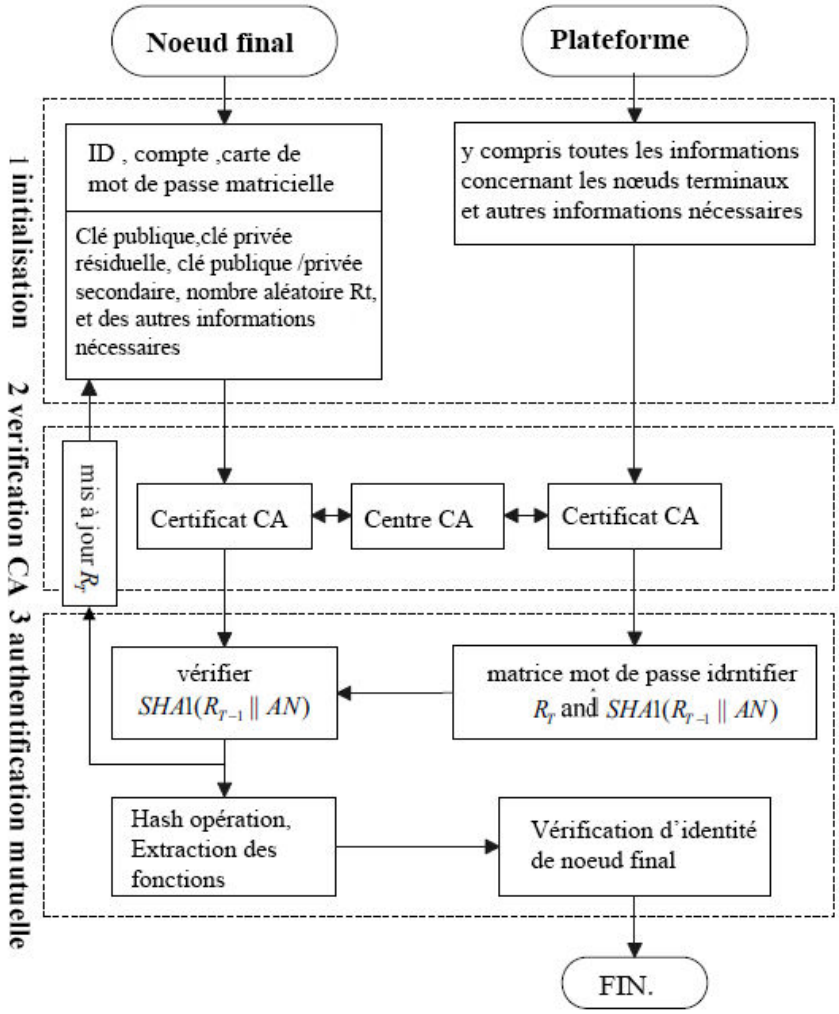

FIGURE 2.2 – Les étapes de protocole de hashage.

Une méthode efficace d'authentification basée sur ECC pour la couche de perception

YE Ning et al [40] ont proposé une méthode efficace d'authentification mutuelle établissant des paires de clés public-privé, basée sur la cryptographie de courbe elliptique (ECC) pour la couche de perception de l'Ido. Cette méthode peut confirmer l'identité des deux côtés de la communication et établir une clé de session.

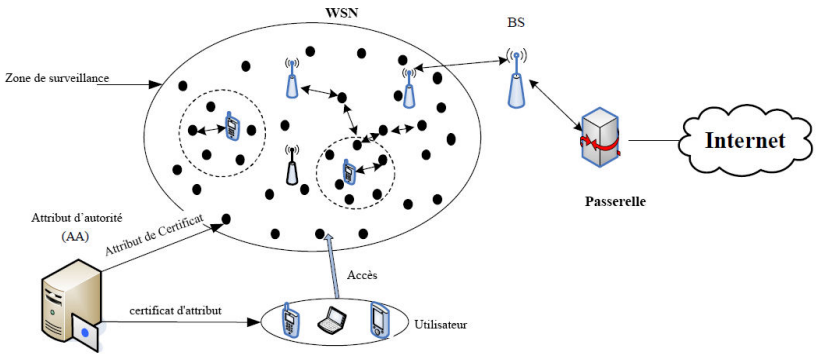

FIGURE 2.3 – la structure de la couche de perception.

L'authentification comprend deux phases : une phase d'initialisation, authentification mutuelle où l'utilisateur doit négocier avec BS l'information secrète utilisée pour l'authentification lorsqu'il accède au réseau du capteur. Et une phase d'établissement de clés. Le schéma suivent décrit les différentes étapes.

2.4 Conclusion

Dans ce chapitre nous avons vu quelques protocoles d'authentifications qui servent à sécuriser les communications entre les objets, ainsi que quelques algorithmes d'élection d'un nouveau serveur.

Le chapitre suivant fera l'objet de notre travail qui est basée sur l'élection d'un nouveau serveur capable d'authentifier les objets dans un système Ido.

CHAPITRE 3
Conception et Implémentation

3.1 Introduction

Dans le chapitre précèdent, nous avons étudié quelques travaux publiés sur l'authentification et l'élection.

Dans ce chapitre, on va présenter l'essentiel de notre travail. Nous allons expliquer en détail le principe d'élection d'un nouveau serveur entre plusieurs nœuds candidats, et comment ce fait l'authentification d'un nœud au près du nouveau serveur.

Ensuite, on va présenter l'implémentation, la phase la plus importante après celle de la conception. C'est une traduction pratique de notre solution théorique afin de la rendre opérationnelle. Pour cela, nous allons décrire l'environnement de travail puis donner une description des différentes interfaces graphiques de l'application développée.

3.2 Algorithme et protocole utilisés

3.2.1 L'algorithme d'élection

L'élection d'un serveur est une nécessité fondamentale pour les systèmes distribués. Elle partit d'une configuration dans laquelle tous les processus exécutent l'algorithme d'élection pour arriver dans une configuration dans laquelle un seul processus est élu comme serveur.

Pour que notre solution soit générale, nous admettons les hypothèses suivantes :

- Nous avons opté pour une architecture aléatoire et non définit, c'est-à-dire les nœuds ne connaissent pas l'architecture, donc, l'IdO est un réseau composé d'objets hétérogènes, déployés aléatoirement.
- Chaque objet peut jouer le rôle de fournisseur ou de demandeur de service.
- Un objet sollicité pour un service, peut soit accepter, soit refuser de le fournir.
- Nous supposons aussi, que le serveur est déjà en panne, et on va chercher un nouveau candidat pour prendre le relai afin d'assurer le bon fonctionnement du système jusqu'à la réparation ou le remplacement du serveur en panne.
- Chaque objet est définit par un id 'une identité unique'.
- Chaque nœud de réseau (objet) a deux états (actif, passif). Au début tous les nœuds sont dans l'état passif.

Notre solution passe par les étapes suivantes :

a. Le premier nœud N qui détecte la panne du serveur, démarrer l'exécution de l'algorithme d'élection. Il envoie aux autres nœuds voisins : son identificateur (id), une requête qu'une panne à était détecté dans le serveur. C'est le nœud qui commence à la construction d'un arbre dont celui est la racine.

b. Les nœuds qui ont reçu la requête qu'une panne est survenue dans le serveur, avec l'id du nœud qui la détecter, ils participent aussi à l'élection. Ils envoient aux autres nœuds voisins qui n'ont pas encore informés, et cela grâce à la variable état (actif), afin de minimiser les messages échanger entre les nœuds, et économiser l'énergie.

c. L'étape b est répétées jusqu'à arriver aux nœuds feuilles.

d. Chaque nœud feuille envoi son id à son père, qui est à son tour envoie l'id le plus grand (parmi ses fils) à son père et ainsi de suite jusqu'à arriver à la racine (le nœud qui détecte la panne).

e. Le nœud racine compare son id avec les ids reçus.

f. Maintenant, le nœud avec l'identificateur le plus grand est le nœud gagnant (processus élue). Ce résultat est disponible chez la racine.

g. Le nœud racine diffuse un message d'information du nouveau serveur.

h. Tous les nœuds passent dans l'état passif.

Maintenant le scénario est le suivant :

— Un nœud demande à s'authentifier auprès du nouveau serveur,

— Il envoie ses informations au serveur, qui est à son tour les vérifies.

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

— Sinon l'authentification échouera.

Les variables utilisées dans l'algorithme d'élection :

— Chaque processus a une variable nommé **état**=actif si il participe à l'élection, passif sinon.

— **Voisinsp** : l'ensemble des processus voisins de p selon une distance d voir les sections 3.2.2 et 3.2.3.

— **Idp** est l'identificateur du processus p.

— **Idg** est l'identificateur le grand.

Les messages utilisés dans l'algorithme d'élection :

— **message élection (idp)** : c'est un message envoyé par le processus p qui a l'identificateur id pour informer les autres processus à participer à l'élection.

— **message id(q)** : c'est un message envoyé par un processus fils q à son parent étiqueté par son identificateur.

— **message (serveur, idg)** : c'est message diffusé par l'initiateur de l'élection pour informer l'ensemble des processus par le nouveau serveur d'identificateur idg.

Algorithme 5: Algorithme d'élection

```
Debut
    si le processus p est initiateur alors
        Étatp=actif
        pour tout processus q ∈ voisinsp faire
            Envoie message élection (idp) aux processus q
        fin
    fin
    Lors de la réception de q d'un message d'élection (id)
     pour chaque processus q faire
        Etatq=actif
        si voisinq = ∅ alors
            # (q c'est une feuille)
            Envoie message id(q) au nœud père
        sinon
            tant que voisinsq ≠ ∅ faire
                si état voisinq = passif alors
                    Envoie message élection (idq) aux voisinsq
                    etat voisinq=actif
                fin
            fin
        fin
     fin
    Lors de la réception d'un message id(q) par un processus k
     pour chaque processus k faire
        Choisir parmi les id reçus, l'idg le plus grand et envoi message (id) au
        processus père
     fin
     si processus k = processus p alors
        Serveur=processus avec idg
        Diffuse message (serveur, idg)
        pour tout processus p faire
            Etatp=passif
        fin
     fin
Fin
```

3.2.2 Algorithme choix des voisins

Nous avons utilisé le principe de l'arbre couvrant minimal.

- Le nœud père choisir les plus proches voisins en calculant la distance entre lui-même et tous les autres nœuds qui sont dans l'état passif.
- Si un nœud est choisi comme voisin, son état passe de l'état passif à actif.
- Après le père sélectionne les r plus proches voisins. r est choisis aléatoirement entre 1 et 5.

3.2.3 Algorithme distance minimale

Algorithme 6: Algorithme distance minimale

Debut
| Distance = racine carré $((x_1 - x) * (x_1 - x) + (y_1 - y) * (y_1 - y))$
Fin

3.2.4 Le protocole d'authentification

Vu le manque du temps, nous avons choisi le protocole basés sur la cryptographie asymétrique RSA. Alors que au début, c'était de travailler avec 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'Ido, ou on doit sauvegarder et économiser le maximum.

Comme pour tout système de chiffrement, l'authentification à clé publique est basée sur un algorithme. Il existe plusieurs algorithmes bien documentés, sécurisés et dignes de confiance, le plus commun étant les types de RSA. Contrairement aux algorithmes de chiffrement communément connus (symétriques ou clés secrètes), les algorithmes de chiffrement à clé publique fonctionnent avec deux clés distinctes. Ces deux touches forment une paire spécifique à chaque utilisateur. [43]

Les clés viennent par paires d'une clé publique et d'une clé privée. Chaque paire de clés est unique, et les deux clés travaillent ensemble. [44]

L'authentification à clé publique fonctionne comme ceci [44] :

- Générer une paire de clés.
- Envoyer la clé publique au serveur.
- Plus tard, chaque fois qu'un client (nœud) veut authentifier, le serveur vous demande de prouver que vous avez la clé privée qui correspond à la clé publique on envoyant un message chiffré par la clé publique.
- Le client reçoit le message et le déchiffré avec sa clé privée.
- Le client hash le résultat obtenu avec la méthode MD5 et envoyer le hash au serveur.
- Le serveur fait une comparaison entre le message reçu avec le hash du mot "actif"

Debut
  si *(MD5 (actif)) = message reçu* **alors**
    Le nœud appartient au réseau
  sinon
    Le nœud n'appartient pas au réseau
  fin
Fin

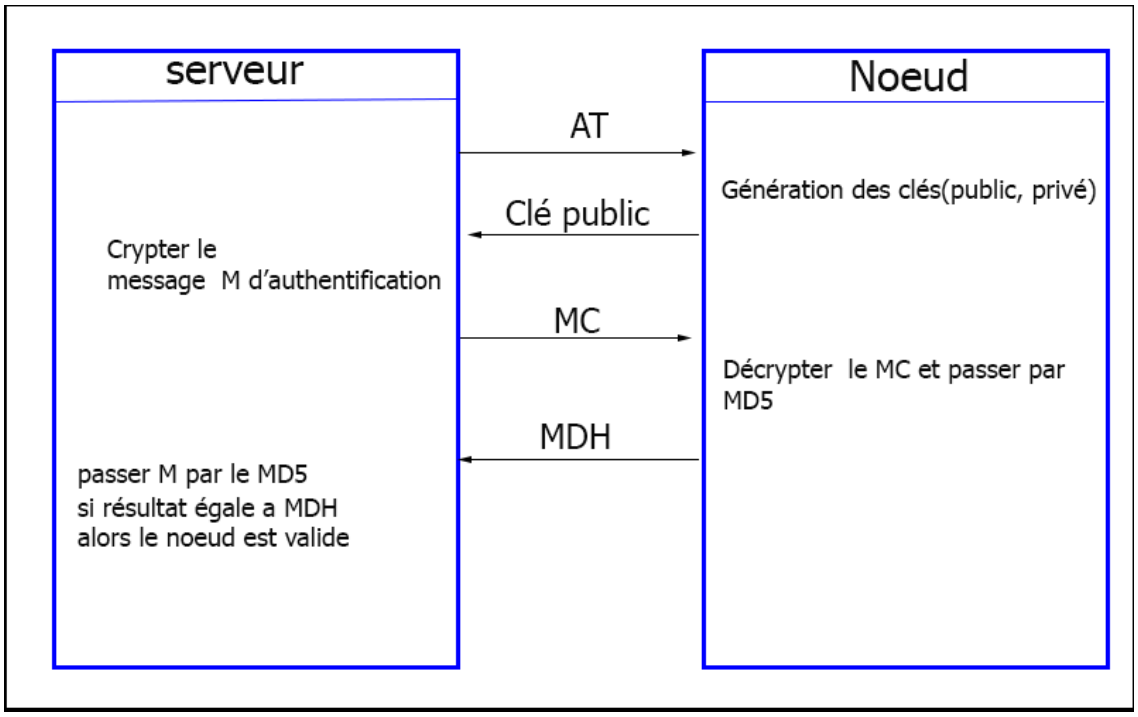

FIGURE 3.1 – protocole d'authentification.

3.3 Environnement de développement

L'environnement de travail est constitué par deux parties nommées environnement matériel et environnement logiciel.

3.3.1 Environnement matériel

Le développement de l'environnement matériel est caractérisé par :

- Système d'exploitation : Windows 10 Professionnel.
- Processeur : Intel(R) Core(TM) i5-2520U CPU @ 2.50GHz 2.19
- Mémoire installée (RAM) : 8.00 GB.
- System type : 64-bit operating system, x64-based processor.

3.3.2 Environnement logiciel

- **NetBeans 8.2** : Netbeans est un environnement de développement intégré(EDI), placé en open source par Sun en juin 2000.

  En plus de Java, NetBeans permet également de supporter différents autres langages, comme Python, C, C++, JavaScript, XML, Ruby, PHP et HTML.

  Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, éditeur graphique d'interfaces et de pages Web . . .). Conçu en Java, NetBeans est disponible sous Windows, Linux, Mac OS X etc ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java).

  Un environnement Java Développement Kit (JDK) est requis pour les développements en Java. NetBeans constitue par ailleurs une plate forme qui permet le développement d'applications spécifiques (bibliothèque Swing (Java)).

  L'IDE Netbeans s'appuie sur cette plateforme Ainsi L'IDE Netbeans s'enrichit à l'aide de plugins.

- **Le langage de programmation JAVA** : C'est un langage de programmation orienté objet, développé par Sun Microsystems en 1995. Il permet de créer des logiciels compatibles avec de nombreux systèmes d'exploitation (Windows, Linux, Macintosh, Solaris). Java donne aussi la possibilité de développer des programmes pour téléphones portables et assistants personnels. Enfin, ce langage peut être utilisé sur internet pour des petites applications intégrées à la page web (applet) ou encore comme langage serveur (jsp).

  Enfin, nous rappelons que le Java, étant un langage de programmation orienté objet utilisable sur divers systèmes d'exploitation, est un langage assez robuste, portable et à hautes performances.

3.3.3 Bibliothèques utilisé

3.3.4 Cipher

Cette classe fournit la fonctionnalité d'un chiffrement cryptographique pour le chiffrement et le décryptage. Il constitue le cœur du Framework Java Cryptographique Extension (JCE).

Afin de créer un objet Cipher, l'application appelle la méthode getInstance de Cipher et lui passe le nom de la transformation demandée. Optionnellement, le nom d'un fournisseur peut être spécifié. Une transformation est une chaîne qui décrit l'opération (ou un ensemble d'opérations) à effectuer sur l'entrée donnée, pour produire une sortie. Une transformation inclut toujours le nom d'un algorithme cryptographique (par exemple, RSA), et peut être suivie d'un mode de rétroaction et d'un schéma de remplissage. [45]

3.3.4.1 Graphic 2D

Cette classe Graphics2D étend la classe Graphics pour fournir un contrôle plus sophistiqué sur la géométrie, les transformations de coordonnées, la gestion des couleurs et la mise en page du texte. Il s'agit de la classe fondamentale pour le rendu de formes bidimensionnelles, de texte et d'images sur la plateforme Java(TM). [46]

Java 2D étend les mécanismes AWT précédents pour dessiner des graphiques 2D, manipuler du texte et des polices, charger et utiliser des images, et définir et traiter des couleurs et des espaces de couleur. Nous examinerons ces nouveaux mécanismes dans cette rubrique et dans les prochaines. [46]

Toutes les coordonnées passées à un objet Graphics2D sont spécifiées dans un système de coordonnées indépendant de l'appareil appelé Espace utilisateur, qui est utilisé par les applications. L'objet Graphics2D contient un objet AffineTransform dans le cadre de son état de rendu qui définit comment convertir les coordonnées de l'espace utilisateur en coordonnées dépendantes de l'appareil dans l'espace périphérique.[46]

3.4 Présentation des interfaces graphiques de l'application

3.4.1 Interface principale

Une exécution de notre application, nous donne l'interface principale suivante (figure 3.2) :

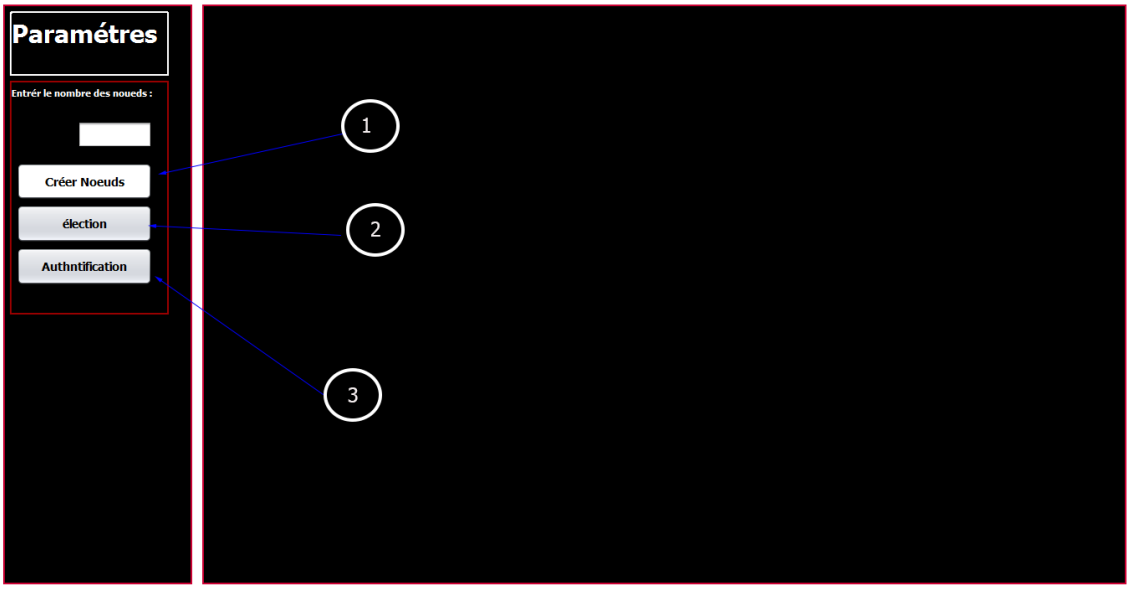

FIGURE 3.2 – Iterface principale

L'interface principale contienne trois boutons, tel que :

- **Créer réseaux** : ce bouton sert à générer une topologie quelconque du réseau, c'est à dire créer les nœuds de réseaux, et cela après avoir entré le nombre de nœuds désirés.
- **Élection** : ce bouton sert à exécuter l'algorithme d'élection après avoir choisir un nœud aléatoire qui détecte la panne, et afficher le résultat d'élection.
- **Authentification** : cliquer sur ce bouton pour afficher le résultat de l'application de l'algorithme d'authentification.
- Et bien sûre, l'espace pour l'affichage des résultats.

3.4.2 Architecture du modèle

La simulation de notre solution se faite sur un réseau peer to peer voir la figure 3.3. Tel que chaque nœud du réseau a deux modèles, boite de réception et modèle pour l'envoie de message.

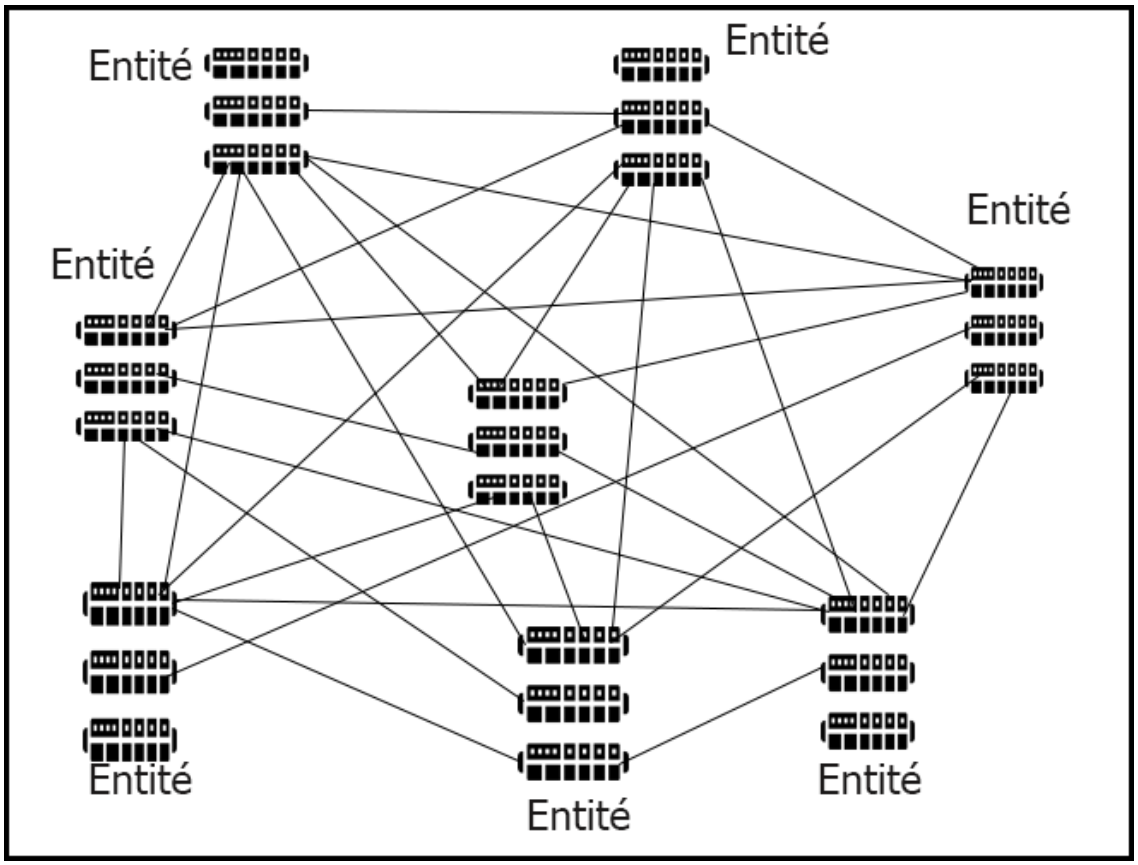

FIGURE 3.3 – Architecture de réseau Peer to Peer.

3.4.3 Exemple de simulation

Dans cette partie, nous allons présenter les différentes interfaces de simulation :

3.4.3.1 Générer un réseau

Après avoir entré le nombre de nœuds désirés (exemple 12), et cliquer sur le bouton générer réseau, un réseau quelconque est généré (figure 3.4)

— Chaque nœud a quatre information (le nom, le port, position(x, y), état), ces informations sont enregistrée dans un fichier texte.

— Chaque nœud de réseau a deux état (actif, passive) ; au début tous les nœuds sont dans l'état passive.

— Chaque nœud a un id qui est générée aléatoirement entre 1 et 100.

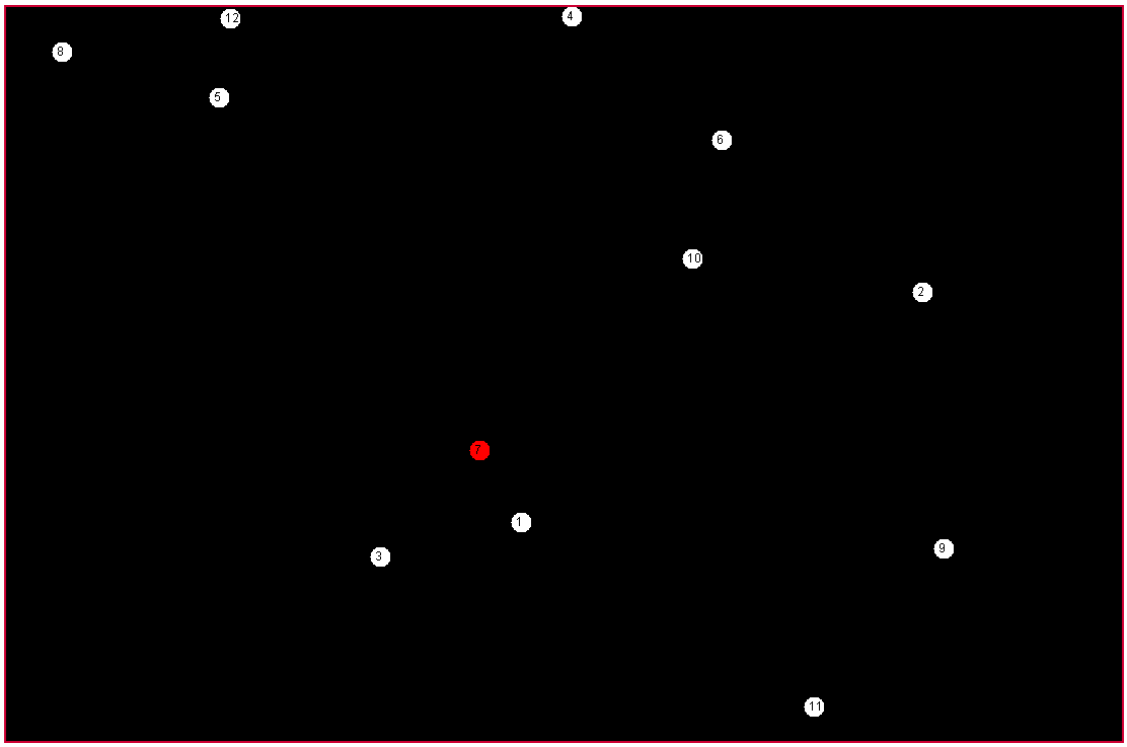

FIGURE 3.4 – création des nœuds (objets).

Le nœud (7) en couleur rouge, c'est le nœud qui détecte la panne du serveur, il est choisi aléatoirement.

3.4.3.2 Election

Après avoir générer un réseau :

- **Etape 1 :** cliquer sur le bouton élection pour démarrer l'exécution de l'algorithme d'élection. Un arbre couvrant va construit dont le nœud (7) est sa racine.
- **Etape 2 :** le nœud racine choisi deux plus proches voisins 1 et 3 (Figure 3.5) en se basant sur la distance entre ces nœuds et la racine.

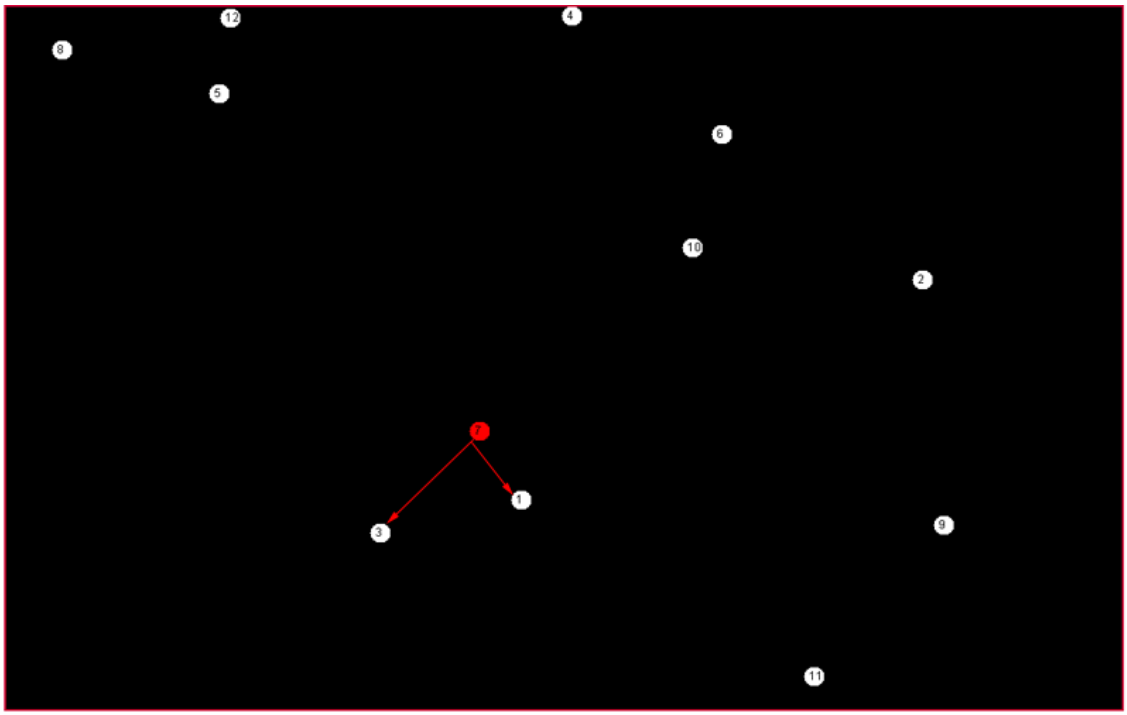

FIGURE 3.5 – étape 1 de la construction de l'arbre

- **Etape 3 :** L'algorithme continué à s'exécuter, maintenant :
  - Le nœud 1 choisi deux plus proches voisins 10 et 11.
  - Le nœud 3 choisi le proche voisin, le nœud 9 (figure 3.6)

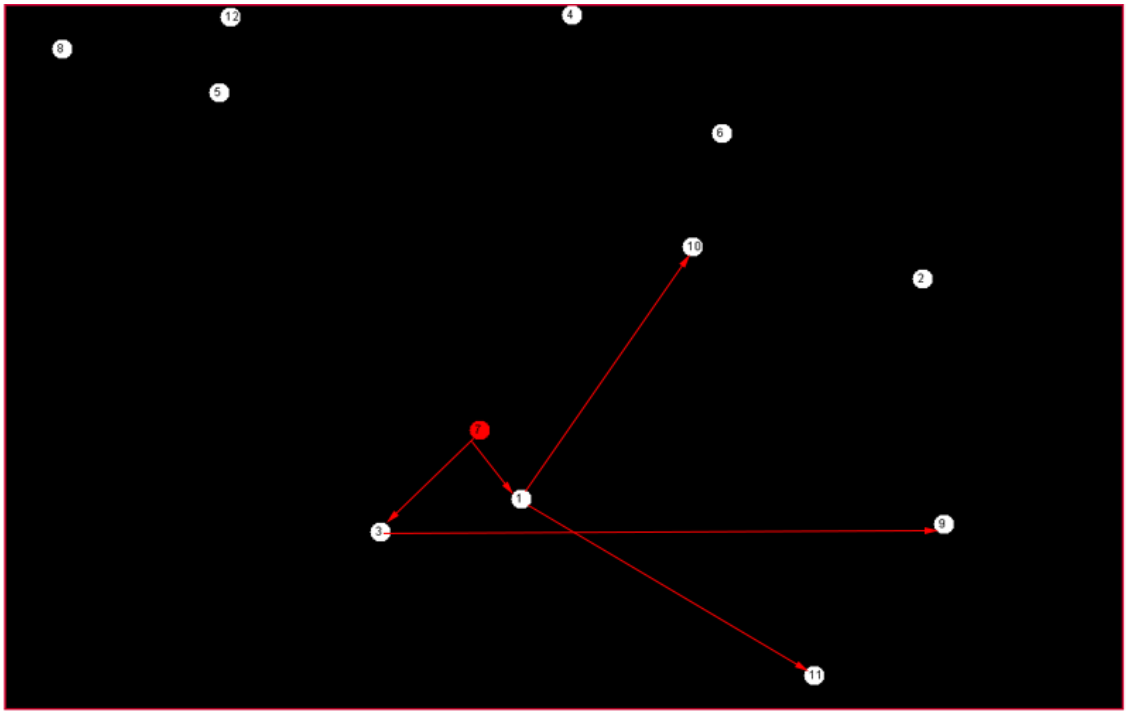

FIGURE 3.6 – étape 2 de la construction de l'arbre

Et ainsi de suite, c'est-à-dire chaque nœud informe ses voisins du début d'élection, jusqu'à la construction de l'arbre finale (figure 3.7)

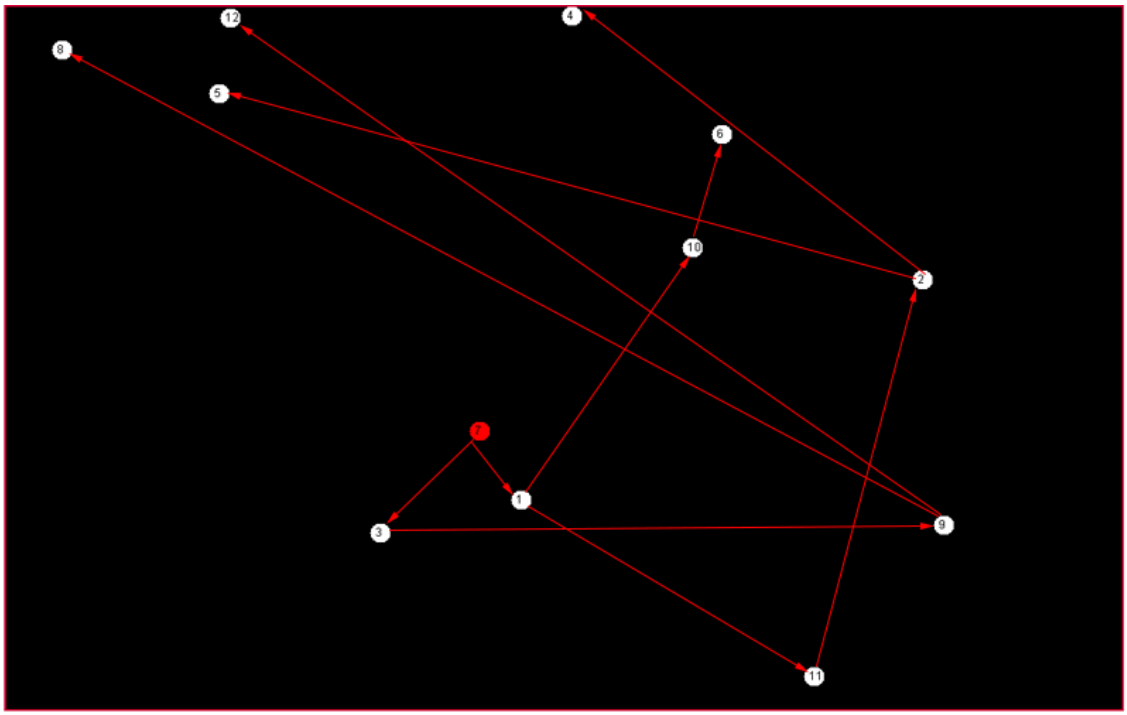

FIGURE 3.7 – L'arbre finale.

- **Etape 4 :** les nœuds feuilles (4, 5, 12, 9, 6) informes leurs parents de leurs ids. (figure 3.8).

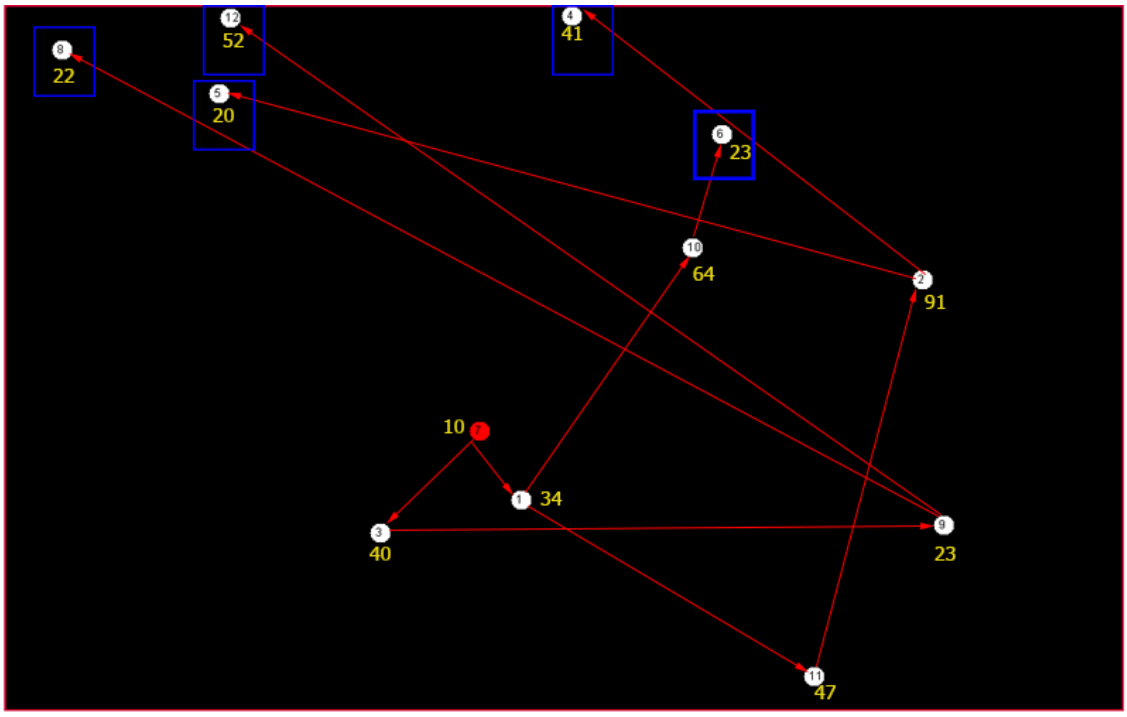

FIGURE 3.8 – Nœuds feuilles.

— Le nœud feuille 6 envoie son id(23) à son nœud père 10.

— le nœud feuille 4 envoie son id(41) à son nœud père 2.

— **Remarque :** dans ce cas, le nœud 2 doit attendre la réponse de nœud 5 pour répondre à son père (nœud 11).

— Le nœud 5 envoie son id(20) à son nœud père 2.

— Le nœud 10 envoyé le max id=64 entre (23 et 64) à son nœud père 1.

— **Remarque :** dans ce cas le nœud 1 doit attendre la réponse de nœud 11 pour répondre à son père (nœud 1).

— Le nœud 2 envoyé le max id=91 entre (41 et 20 et 91) à son nœud père 1 (figure 3.9).

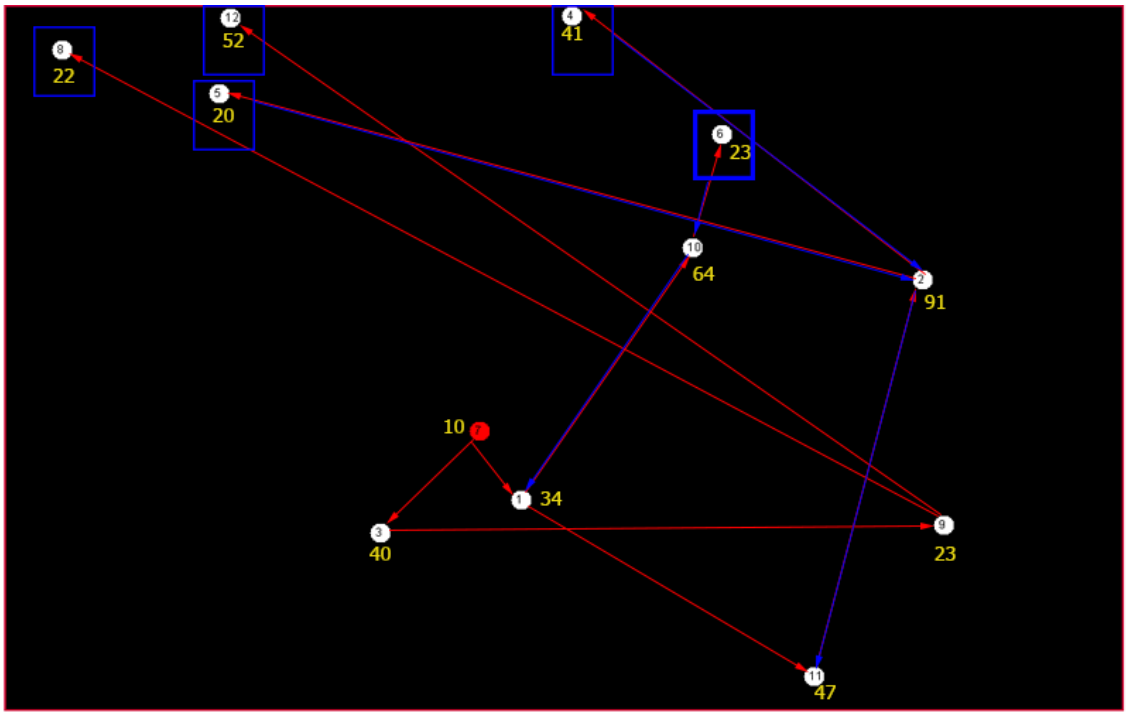

FIGURE 3.9 – messages des nœuds fils aux parents.

— Le nœud 11 envoyé le max id=91 entre (41 et 91) à son nœud père 1, et dans ce cas le nœud 7 doit attendre la réponse du nœud 3.

— Et ainsi de suite jusqu'à le nœud 3 envoie le max id=52 entre (52, 40) à son nœud père 7.

— Maintenant, le nœud 7 (la racine) choisi le max entre (91, 40, 52) (voit la figure 3.10)

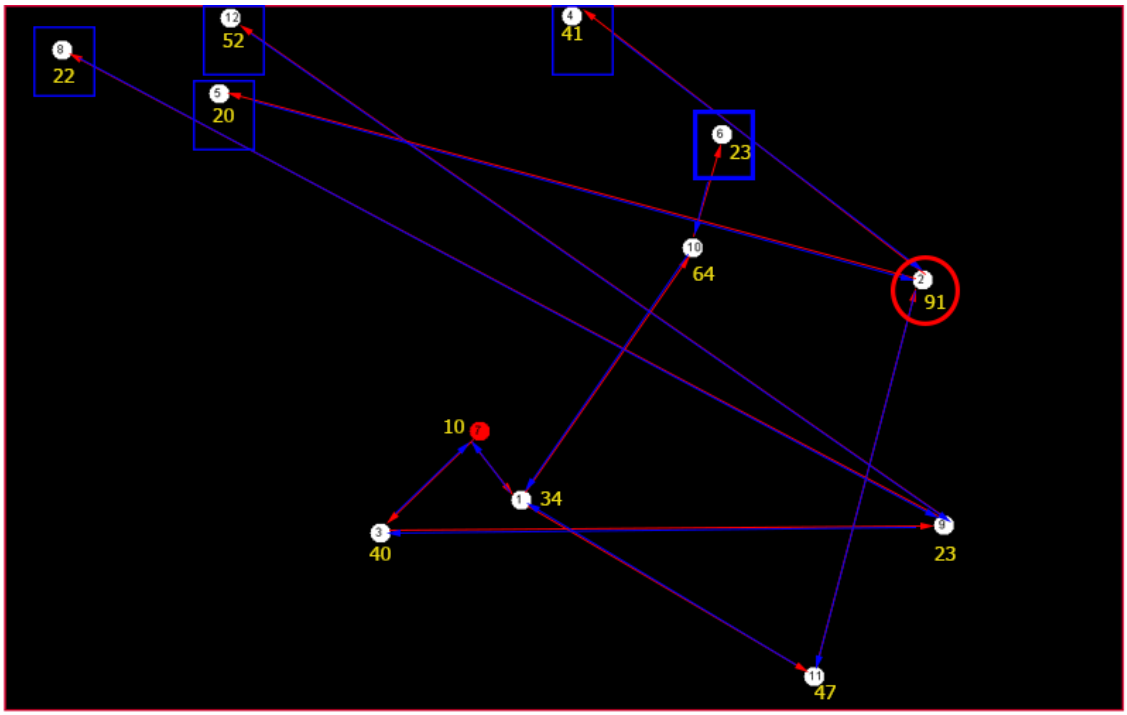

FIGURE 3.10 – résultat de l'élection (nœud 2 est le nouveau serveur).

— Maintenant, le nœud racine 7 savoir que le nœud 2 qui a le plus grand identificateur est le processus élu (gagnant), il diffuse un message dans le réseau pour informer les autres nœuds que le nœud 2 avec l'identificateur 91 est le nouveau serveur (voir la figure 3.11).

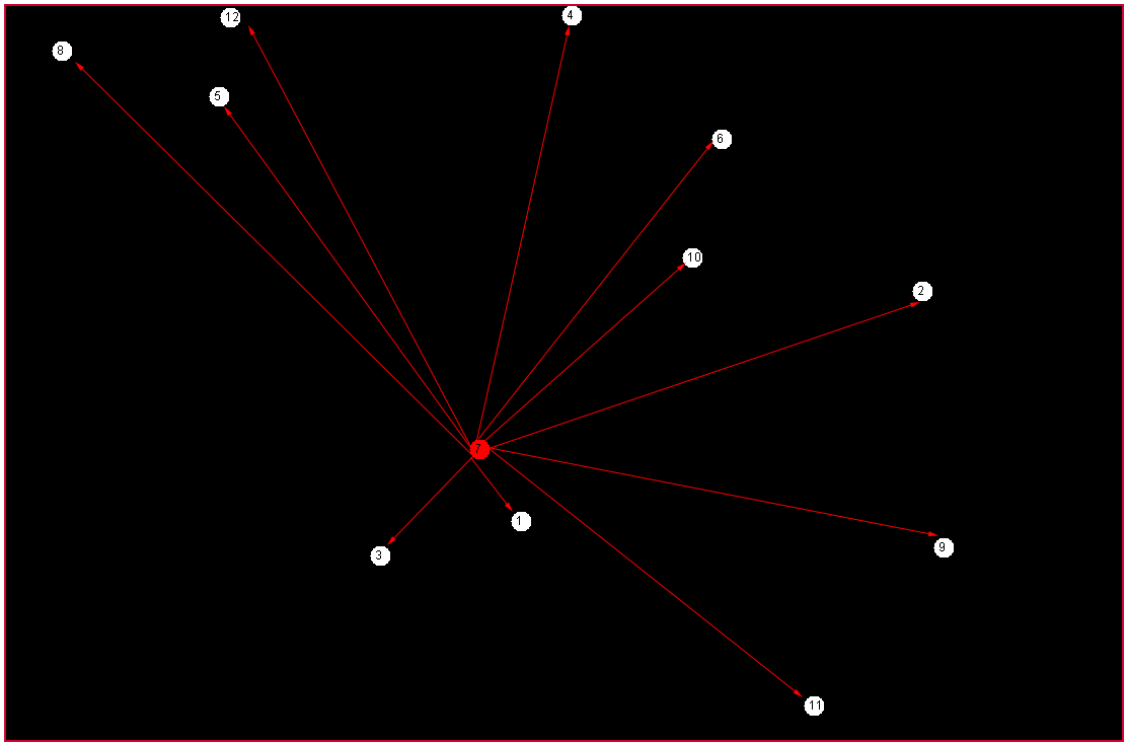

FIGURE 3.11 – Diffusion du message résultat de l'élection.

L'interface suivante représente le nouveau serveur avec le couleur bleu.

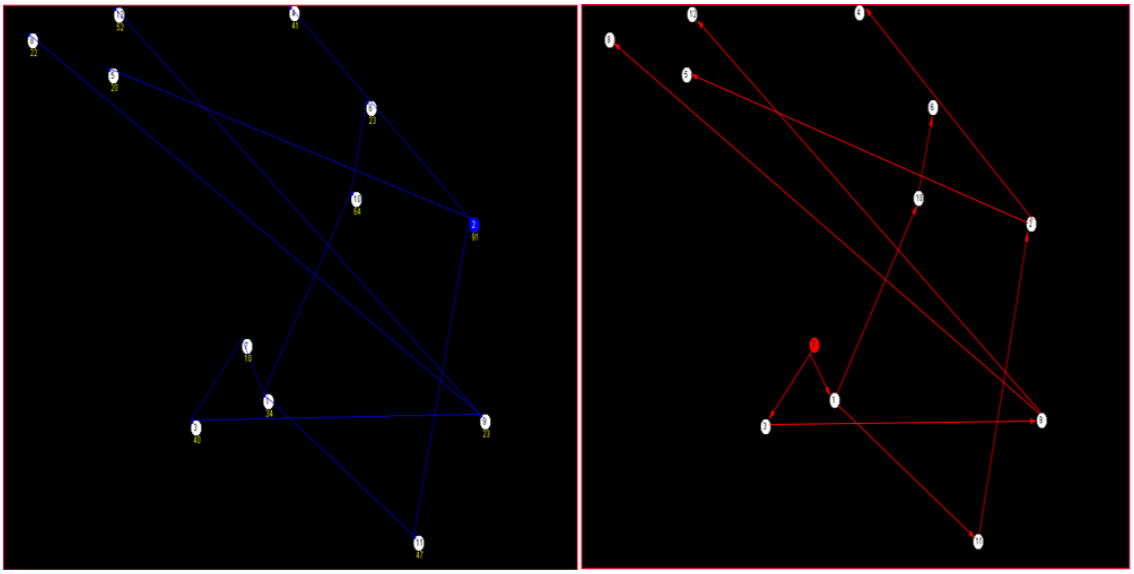

FIGURE 3.12 – comparaison entre début et fin d'élection.

3.4.3.3 L'authentification

— Le nouveau serveur est élu. Donc, il sera capable d'authentifier les différents nœuds.

— les nœuds demandent à s'authentifier auprès du nouveau serveur,

— Ils envoient ses informations au serveur, qui est à son tour les vérifies.

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

— Sinon l'authentification échouera.

— Un clique sur le bouton authentification donne les interfaces suivantes (figure 3.13, figure 3.14)

— Une attaque homme aux milieux (man in the middle) est modélisée.

— Les nœuds en couleur verte sont bien authentifier, alors que ceux en couleur orange sont non authentifiés.

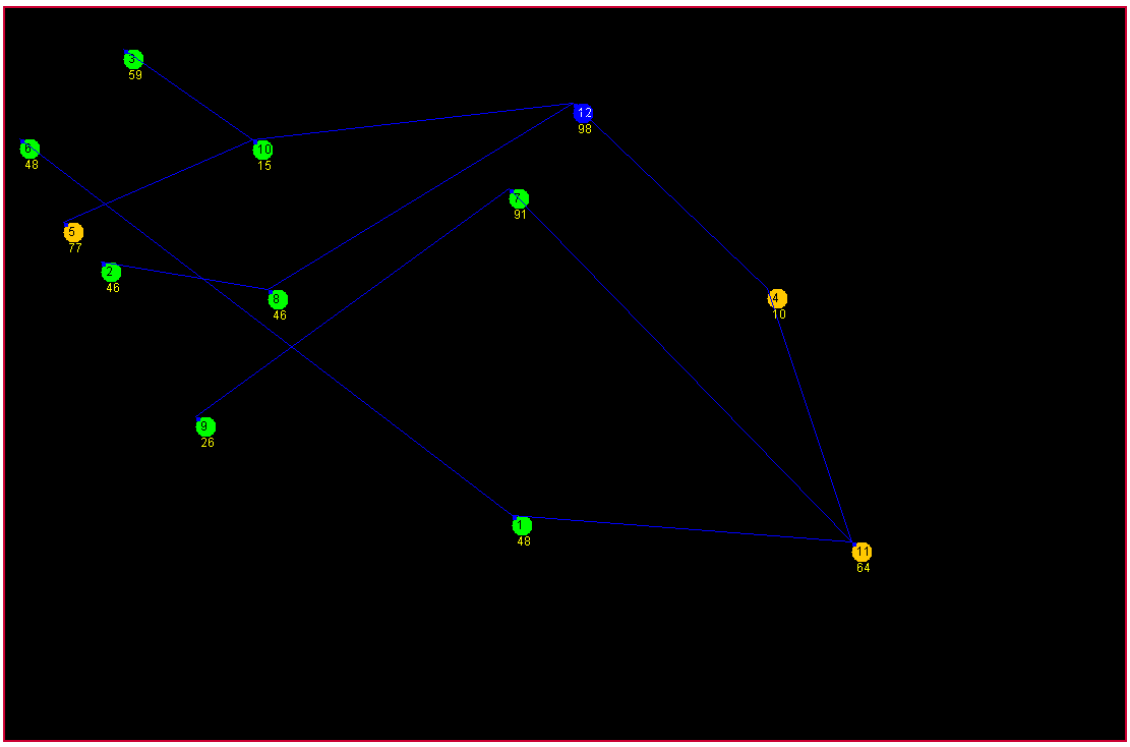

FIGURE 3.13 – résultat de l'étape d'authentification.

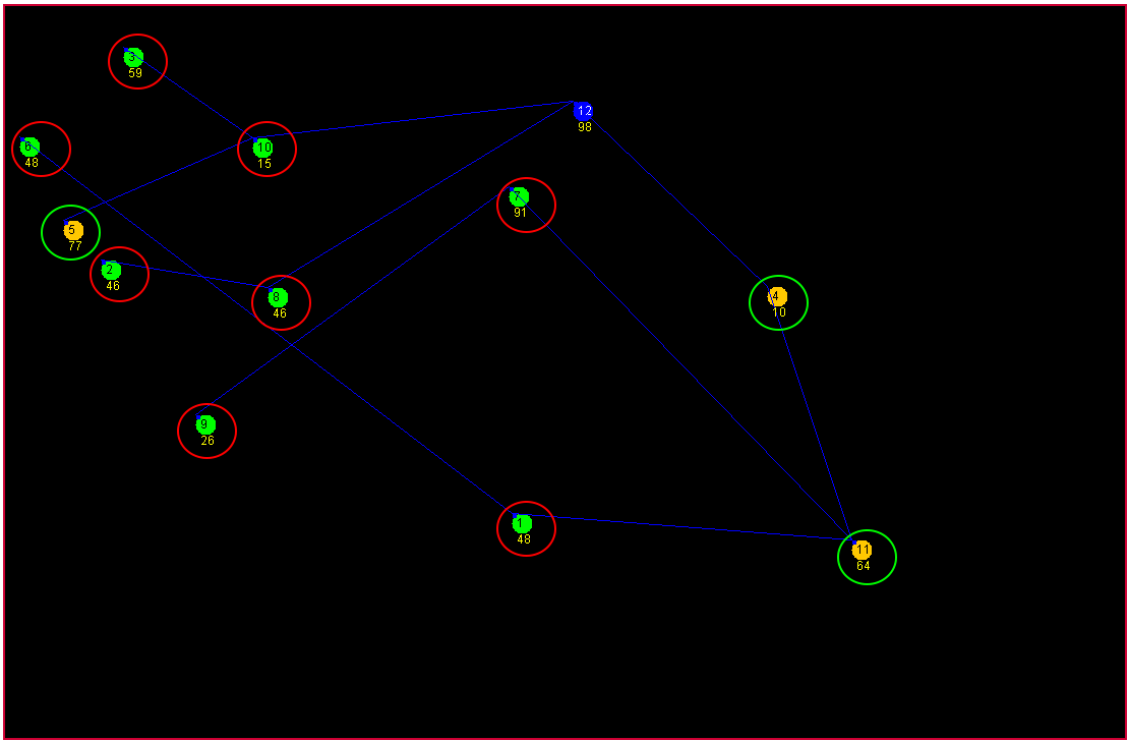

FIGURE 3.14 – Démonstration du résultat de l'étape d'authentification..

3.5 Conclusion

Ce chapitre a été consacré à la présentation de notre solution. Elle regroupe un algorithme d'élection afin d'élire un nouveau serveur, un protocole d'authentification qui sert à sécuriser les communications entre les nœuds à base de RSA.

Ensuite, nous avons présenté l'implémentation de notre solution. Nous avons donné en brève description des outils nécessaires pour réaliser notre simulation. Enfin, nous avons testé et présenté les différentes interfaces de l'application.

Conclusion Générale

La prospérité de l'IoT ne peut être réalisée que lorsqu'on assure une bonne sécurité aux objets et un bon fonctionnement du système de communication utilisés. Il est primordial de mettre en place une politique de sécurité qui empêche tout objet malicieux ou non autorisé d'avoir accès aux systèmes IoT, de lire leurs données ou de les modifier. Pour qu'un objet ait la possibilité d'exploiter un service ou de s'associer à un réseau, il doit d'abord prouver son identité et avoir les droits d'accès nécessaires. Il doit aussi assurer un bon fonctionnement du système en cas de panne de serveur.

Dans ce travail, nous avons mis en avant des généralités essentielles sur l'IOT, ainsi que les besoin et les défis de la sécurité dans l'IOT. Nous avons étudié quelques méthodes d'authentification. Nous avons aussi recensé quelque algorithmes d'élections qui servent à élire un processus parmi plusieurs dans le but de prendre des décisions dans le système.

Notre proposition se base sur un protocole d'authentification et un algorithme d'élection, le protocole d'authentification vise à sécuriser les communications entre les différents objets ou bien entre les objets et le serveur, et l'algorithme d'élection vise sélectionner un nouveau serveur parmi un ensemble d'objets qui sont candidats à l'élection pouvant assurer cette fonction en cas de panne.

Vu le manque du temps, en perspective, nous souhaitons faire des comparaisons avec d'autres algorithmes d'élections afin d'approfondi la simulation. Nous souhaitons aussi d'authentifier les objets à base de la cryptographie à courbe elliptique (ECC) qui a un grand avantage à l'IOT par rapport à la cryptographie sur les entiers comme RSA.

Bibliographie

[1] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on iot security : application areas, security threats, and solution architectures. *IEEE Access*, 7 :82721–82743, 2019.

[2] Nadim El Sakaan, Ali Hidjeb, et al. *Implémentation d'un protocole d'élection d'un serveur d'authentification dans l'internet des objets.* PhD thesis, Université abderrahmane mira béjaia, 2017.

[3] Akka Zemmari. *Présentation et analyse de quelques algorithmes distribués probabilistes.* PhD thesis, Université de Bordeaux, 2009.

[4] Karim Terir et al. *Gstion de la con dentialité des données pour les dispositifs IOT (Internet of Things).* PhD thesis, University of Jijel, 2020.

[5] KEVIN ASHTON. That 'internet of things' thing. *In the real world, things matter more than ideas.*, 2009.

[6] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, 1(2) :99–109, 2015.

[7] Jan Holvast. History of privacy. In *The History of Information Security*, pages 737–769. Elsevier, 2007.

[8] HLM Kerivin, Mathieu Lacroix, Ali Ridha Mahjoub, and Alain Quilliot. The splittable pickup and delivery problem with reloads. *European Journal of Industrial Engineering*, 2(2) :112–133, 2008.

[9] Nuttapong Attrapadung, Benoît Libert, and Elie De Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *International workshop on public key cryptography*, pages 90–108. Springer, 2011.

[11] Hadjadj Walid, ''étude de cas sur un système médical domotique contrôle par un SMA '', mémoire de fin d'étude en vue de l'obtention du diplôme de Master en Informatique Spécialité : Architecture distribué , Université Larbi Ben M'hidi Oum El Bouaghi

[13] `https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-healthcare-solutionbrief-fr.pdf`.

[15] Y Ait Mouhoub, Fatah Bouchebbah, Mawloud Omar, et al. Proposition d'un modele de confiance pour l'internet des objets. *Mémoire master de l'université Abderrahmane Mira Bejaia*, 21, 2015.

[16] Ryangsoo Kim, Hyuk Lim, and Bhaskar Krishnamachari. Prefetching-based data dissemination in vehicular cloud systems. *IEEE Transactions on Vehicular Technology*, 65(1) :292–306, 2015.

[19] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A survey on internet of things : Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal*, 4(5) :1125–1142, 2017.

[20] Abel C Lima-Filho, Ruan D Gomes, Marceu O Adissi, Tássio Alessandro da Silva, Francisco A Belo, and Marco A Spohn. Embedded system integrated into a wireless sensor network for online dynamic torque and efficiency monitoring in induction motors. *IEEE/ASME transactions on mechatronics*, 17(3) :404–414, 2012.

[21] Yasmine Harbi. *Security in Internet of Things*. PhD thesis, Ferhat Abbas University Setif 1, 2021.

[22] Philip Koopman. Embedded system design issues (the rest of the story). In *Proceedings International Conference on Computer Design. VLSI in Computers and Processors*, pages 310–317. IEEE, 1996.

[23] Gabriel Montenegro, Nandakishore Kushalnagar, Jonathan Hui, David Culler, et al. Transmission of ipv6 packets over ieee 802.15. 4 networks. *Internet proposed standard RFC*, 4944 :130, 2007.

[24] Geoff Mulligan. The 6lowpan architecture. In *Proceedings of the 4th workshop on Embedded networked sensors*, pages 78–82, 2007.

[25] LoRa Alliance. Lorawan 1.1 specification. 2017, 2017.

[26] Cédric Llorens, Laurent Levier, Denis Valois, and Benjamin Morin. *Tableaux de bord de la sécurité réseau*. Editions Eyrolles, 2011.

[27] Hokeun Kim and Edward A Lee. Authentication and authorization for the internet of things. *IT Professional*, 19(5) :27–33, 2017.

[29] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, and Jean-Jacques Schwartzmann. A review on authentication methods. *Australian Journal of Basic and Applied Sciences*, 7(5) :95–107, 2013.

[30] Mohammed Farik and AS Ali. Algorithm to ensure and enforce brute-force attack-resilient password in routers. *International Journal of Technology Enhancements and Emerging Engineering Research*, 4(10) :184–188, 2015.

[35] Saru Kumari, Muhammad Khurram Khan, and Xiong Li. An improved remote user authentication scheme with key agreement. Computers & Electrical Engineering, 40(6) :1997–2012, 2014.

[36] Muhamed Turkanović, Boštjan Brumen, and Marko Hölbl. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad Hoc Networks*, 20 :96–112, 2014.

[37] Mohammad Sabzinejad Farash, Muhamed Turkanović, Saru Kumari, and Marko Hölbl. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. *Ad Hoc Networks*, 36 :152–176, 2016.

[38] Pawani Porambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Mika Ylianttila. Two-phase authentication protocol for wireless sensor networks in distributed iot applications. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2728–2733. Ieee, 2014.

[39] Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long, and Ting Hu. A novel mutual authentication scheme for internet of things. In *Proceedings of 2011 International Conference on Modelling, Identification and Control*, pages 563–566. IEEE, 2011.

[40] Ning Ye, Yan Zhu, Ru-chuan Wang, Reza Malekian, and Qiao-min Lin. An efficient authentication and access control scheme for perception layer of internet of things. 2014.

[41] P Laurent. *Algorithmique Distribuée, Election distribuée*. PhD thesis, PhD thesis, Université, 2014.

[42] Jean-Michel Hélary, Aomar Maddi, and Michel Raynal. *Calcul distribué d'un extremum et du routage associé dans un réseau quelconque*. PhD thesis, INRIA, 1986.

[10] https://moodle.insa-rouen.fr/?lang=fr.

[12] https://www.fun-mooc.fr/c4x/MinesTelecom/04013/asset/S4-5_-Objets-communicants.pdf.

[14] https:wikimemoires.net/2019/09/domaines-d-applications-de-l-iot/.

[17] https://www.i-scoop.eu/internet-of-things-iot/industrial-internet-things-iiot-saving-costs-innovation/.

[18] https://www.sfrbusiness.fr/room/internet-des-objets/les-etapes-projet-iot.html.

[28] https://stringfixer.com/fr/Mutual_authentication.

[31] https://pdfs.semanticscholar.org/3733/2607f7a7ac8284c514845957fd0 0583e5614.pdf.

[32] https://en.wikipedia.org/wiki/Multi-factor_authentication.

[33] bioelectronix, biometricsecurity.http://www.bioelectronix.com/what_is_biometrics.html.

[34] https://www.techwalla.com/articles/what-are-the-advantages-disadvantages-of-a-digital-certificate

[43] `https://www.ssh.com/academy/ssh/public-key-authentication`.

[44] `serverpilot.io/docs/how-to-use-ssh-public-key-authentication`.

[45] `docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html`.

[46] `docs.oracle.com/javase/7/docs/api/java/awt/Graphics2D.html`.