République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. Mira Bejaïa
Faculté Des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme Master en informatique

Option : Administration et Sécurité des Réseaux

THÈME

Scénarios et Simulations d'un IoT sécurisé dans NetLogo

(Cas Maison Intelligente et Port Intelligent)

Réalisé par :

Mr DJOUAD Badreddine

Melle GANI Sara

Soutenu le : 22/06/2023

Membre du jury :

Président	Mr	MOKETFI Mohand	M.C.B	U.A/Mira Béjaia.
Examinateur	Mme	BOUADEM Nassima	M.C.B	U.A/Mira Béjaia.
Encadrant	Mme	HOUHA Amel	M.A.A	U.A/Mira Béjaia.

Promotion : 2022/2023

Remerciements

Nous aimerions exprimer notre sincère gratitude et nos chaleureux remerciements au Dieu Tout-Puissant pour les innombrables bénédictions dont nous avons bénéficié tout au long de notre parcours de recherche, sans lesquelles ce projet n'aurait pas été possible.

Un immense merci à notre promotrice HOUHA AMEL, pour son soutien, sa patience inépuisable et son expertise précieuse. Sa présence et son mentorat constant ont été une source d'inspiration et de motivation tout au long de notre travail de recherche et de la rédaction de ce mémoire sans oublier sa bienveillance qui nous a conduits à mener notre travail à bien. Nous lui sommes profondément reconnaissants pour sa guidance éclairée et ses précieux conseils.

Nous tenons également à exprimer notre sincère reconnaissance envers les membres du jury qui ont consacré leur temps et leurs compétences à évaluer et juger notre travail. Leurs commentaires constructifs et leur expertise ont grandement enrichi notre réflexion et contribué à l'amélioration de ce mémoire.

Un grand merci à nos parents qui ont été d'un soutien infaillible, non seulement pendant la réalisation de ce mémoire, mais tout au long de notre parcours académique. Leur amour, leurs encouragements constants et leur confiance en nous ont été des moteurs essentiels de notre réussite. Nous leur sommes infiniment reconnaissants et souhaitons qu'Allah les préserve et les bénisse.

Enfin, nous souhaitons exprimer notre profonde gratitude envers nos frères, sœurs, camarades de classe et amis, qui ont contribué de diverses manières à la réalisation de ce projet. Votre soutien moral, vos encouragements et vos précieux conseils nous ont permis de surmonter les obstacles et de progresser vers nos objectifs. Nous sommes reconnaissants de vous avoir à nos côtés et nous apprécions énormément votre présence.

À tous ceux qui ont joué un rôle dans cette aventure, nous vous adressons nos remerciements les plus sincères. Votre contribution, votre soutien indéfectible et votre amitié précieuse ont été des éléments essentiels de notre réussite. Nous sommes honorés et reconnaissants de partager cette étape importante de notre parcours avec vous.

Gani Sara
Djouad Badreddine

Table de matières

Table de figures

Liste des tableaux

Liste des acronymes

A	AT&T	American Telephone and Telegraph
	AES	Advanced Encryption Standard
	ACK	Acknowledgment
B	Big Data	Données massives
	BidCoS	Bidirectional Communication System
C	CoAP	Constrained Application Protocol
D	DoS	Denial of Service (Déni de service)
	DDoS	Distributed Denial of Service (Déni de service distribué)
E	ECG	Électrocardiogramme
	EPB	Entreprise Portuaire de Bejaïa
F	FTTx	Fiber to the x
G	GPS	Global Positioning System (Système de positionnement mondial)
H	HTTP	Hypertext Transfer Protocol
	HTTPS	Hypertext Transfer Protocol Secure
I	IoT	Internet des objets
	IIoT	Industrial Internet of Things
	IP	Internet Protocol
	IPv6	Internet Protocol version 6
	IA	Intelligence Artificielle
	IEEE	Institute of Electrical and Electronics Engineers
	IaaS	Infrastructure as a Service
	ICMP	Internet Control Message Protocol
L	Li-Fi	Light Fidelity
	LoRaWAN	Long Range Wide Area Network
	LTE	Long Term Evolution
M	MIT	Massachusetts Institute of Technology
	M2M	Machine to Machine
	MQTT	Message Queuing Telemetry Transport

	MANET	Mobile Ad hoc Network
	MiTM	Man in the Middle (Homme du milieu)
	MABS	Simulation a Base Multi-Agents
P	PaaS	Platform as a Service
Q	QoS	Quality of Service
R	RFID	Radio Frequency Identification (Identification par radiofréquence)
	RedTacton	Technologie de communication sans fil
S	SOA	Architecture Orientée Service (Service-Oriented Architecture)
	SOS	Système de Systèmes
	SaaS	Software as a Service
	SYN	Synchronize
T	TCP	Transmission Control Protocol
	TLS	Transport Layer Security
U	UDP	User Datagram Protocol
V	VMWare	Virtual Machine softWare
W	Wi-Fi	Wireless Fidelity
Z	Zigbee	Protocole sans fil basé sur le standard IEEE 802.15.4
	Z-Wave	Protocole de communication pour les maisons intelligentes

Introduction Générale

L'internet des objets (IoT) est une révolution technologique qui transforme notre manière d'interagir avec le monde qui nous entoure, elle représente aujourd'hui l'avenir de l'informatique et des communications. La planète compte aujourd'hui davantage d'objets connectés que de personnes. Jusqu'alors, internet se concevait comme la capacité des personnes à communiquer à tout moment et en tout lieu ; avec les objets connectés, le monde physique peut désormais communiquer, que ce soit pour des relations de personnes à personnes, de personnes à objets ou d'objets à objets.

L'IoT a le potentiel de transformer de nombreux aspects de la vie quotidienne, de plus en plus de capteurs, de puces, de caméras embarquées permettent de créer des données à partir d'objets, auparavant inertes et isolés les uns des autres pour rendre notre environnement plus intelligent. Ce réseau d'objets connectés a un impact significatif sur de nombreux secteurs, tels que la santé, la domotique, la ville intelligente, l'agriculture, la manufacture et la logistique [1]. C'est un concept dans lequel le monde virtuel des technologies de l'information s'intègre de manière transparente au monde réel.

Cependant, cette interconnexion généralisée présente également des défis majeurs en matière de sécurité. Alors que de plus en plus d'objets sont connectés à Internet, des vulnérabilités potentielles se créent. Ces objets peuvent être sujets à des attaques telles que le piratage, le vol de données ou les dénis de service. Les conséquences de ces attaques peuvent être graves, allant de la violation de la vie privée des utilisateurs à la compromission de la sécurité physique.

En veillant attentivement sur l'IoT, il est possible d'identifier et détecter les activités suspectes et de répondre rapidement aux menaces de sécurité minimisant ainsi les risques potentiels et assurant un déploiement plus sûr et plus fiable.

L'objectif de notre mémoire est de fournir une compréhension approfondie du concept de l'Internet des objets (IoT) dans son ensemble, tout en se concentrant spécifiquement sur la conception d'une maison et d'un port intelligent. Nous souhaitons explorer comment le monitoring peut être utilisé pour assurer une surveillance efficace des dispositifs connectés et renforcer la sécurité dans une maison intelligente, et comment adapter le langage de simulation NetLogo et l'utiliser pour modéliser et simuler ces interactions.

Organisation du mémoire :

Ce mémoire est structuré en quatre chapitres :

Le premier chapitre intitulé " **Généralités sur l'Internet of Things** " offre un aperçu détaillé de l'Internet des objets (IoT). Il présente une définition claire de l'IoT, examine son architecture, met en évidence ses domaines d'application et souligne les enjeux et les défis auxquels il est confronté.

Le deuxième chapitre intitulé " **Monitoring et sécurité dans l'IoT** " couvre deux aspects essentiels : le monitoring et la sécurité dans l'Internet des objets. Il explique le concept du monitoring, son importance dans l'IoT, les domaines de surveillance et les outils associés. Il aborde également la sécurité dans l'IoT, en mettant en évidence les exigences à respecter, ainsi que ses enjeux et défis. De plus, il illustre une attaque spécifique, l'attaque "Hello Flood", pour souligner les vulnérabilités potentielles dans l'IoT.

Le troisième chapitre intitulé " **Simulation du scénario**" offre une perspective approfondie sur le scénario de la maison intelligente, du port intelligent et l'attaque "Hello Flood", en mettant en évidence l'utilisation de la simulation NetLogo comme outil d'analyse. Il propose également une mesure de prévention pour éviter tout danger d'épuisement des ressources.

I *Chapitre : Généralités sur l'Internet of Things*

1. Introduction

L'Internet des Objets (IoT) représente un réseau dynamique où les objets communiquent entre eux, partagent des informations et collaborent pour simplifier notre vie quotidienne. L'idée fondamentale derrière l'IoT est de doter les objets d'une intelligence et d'une connectivité, leur permettant de communiquer entre eux et avec des systèmes informatiques à travers Internet. Ces objets connectés sont équipés de capteurs, de processeurs et de logiciels intégrés qui leur permettent de collecter des informations sur leur environnement, de les traiter en temps réel et de prendre des actions en conséquence. L'objectif ultime de l'IoT est de permettre une convergence entre le monde réel et le monde virtuel, ouvrant ainsi la voie à une multitude de possibilités.

Le présent rapport se penche tout d'abord sur une présentation et une vue d'ensemble de l'IoT : son histoire, son architecture, ses domaines d'applications et sur les différents défis qui en découlent actuellement. Nous terminerons par une conclusion.

2. Qu'est-ce que l'internet of things

2.1 Définitions de l'Internet of Things

Le terme "Internet des objets" fait généralement référence à des scénarios dans lesquels la connectivité du réseau et la capacité de calcul s'étendent à des objets, des capteurs et des articles de tous les jours qui ne sont pas normalement considérés comme des ordinateurs, ce qui permet à ces dispositifs de générer, d'échanger et de consommer des données avec une intervention humaine minimale [2].

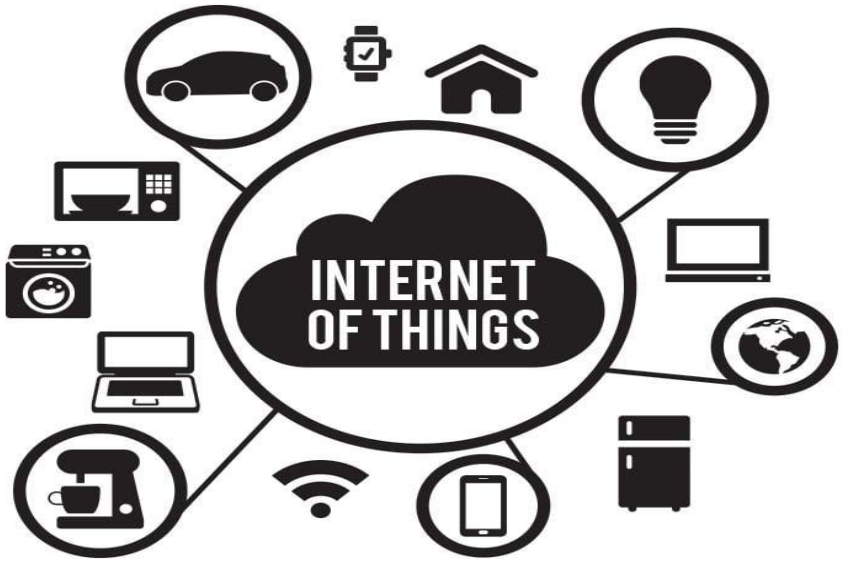


Figure I.1 *- Internet of things* [3]

2.2 Technologies habilitantes

Le concept consistant à combiner des ordinateurs, des capteurs et des réseaux pour surveiller et contrôler des dispositifs existe depuis des décennies. Cependant, la convergence récente de plusieurs tendances du marché technologique rapproche l'Internet des objets d'une réalité généralisée. Il s'agit notamment de la connectivité omniprésente, de l'adoption généralisée des réseaux IP, de l'économie de l'informatique, de la miniaturisation, des progrès de l'analyse des données et de l'essor de l'informatique en nuage [2].

2.3 Modèles de connectivité

Les mises en œuvre de l'IoT utilisent différents modèles techniques de communication, chacun ayant ses propres caractéristiques. Quatre modèles de communication courants sont décrits par l'Internet Architecture Board : Dispositif-à-dispositif, Dispositif-à-cloud, Dispositif-à-passerelle, et Partage de données en amont. Ces modèles mettent en évidence la flexibilité des moyens par lesquels les dispositifs IoT peuvent se connecter et apporter de la valeur à l'utilisateur [2].

3. Histoire de l'IoT

L'Internet des objets (IoT) est un concept qui consiste à connecter des objets physiques au moyen d'Internet pour leur permettre de communiquer entre eux et d'envoyer et de recevoir des données. L'histoire de l'IoT remonte aux années 1990, lorsque des chercheurs et des innovateurs ont commencé à s'intéresser et à imaginer comment les objets du monde réel pourraient être connectés à Internet.

L'expression "Internet des objets" a été inventée pour la première fois en 1999 par Kevin Ashton, un expert en marketing numérique britannique co-fondateur de l'Auto-ID Center au MIT. Ashton a inventé ce terme pour illustrer la connexion des étiquettes RFID utilisées dans les chaines d'approvisionnement des entreprises à Internet pour la gestion des biens sans intervention humaine [1]. Toutefois, l'idée d'appareils connectés existe depuis les années 1970. Ainsi, le premier objet connecté était une machine à Coca, à l'Université de Carnegie Mellon, au début des années 1980.

Au fil du temps, de nombreuses innovations ont été développées pour faire progresser l'IoT, notamment les technologies sans fil, les capteurs et les protocoles de communication.

En 2010, l'IoT a commencé à se développer en dehors des cercles universitaires et technologiques, grâce à l'avènement de produits grand public tels que les thermostats intelligents, les systèmes de sécurité pour la maison et les objets de suivi fitness.

Depuis, l'IoT a évolué rapidement pour inclure de plus en plus de dispositifs connectés, améliorer les capacités de collecte de données et renforcer la sécurité pour les utilisateurs.

L'IoT est le résultat d'une vision de l'avenir qui a commencé il y a plus de 20 ans et qui a évolué au fil des ans grâce à l'innovation et à l'adoption de technologies avancées. Aujourd'hui, l'IoT est considéré comme l'un des éléments clés de la transformation numérique et continue de se développer rapidement.

4. Pourquoi l'Internet of Things (IoT) est-il si important

Ces quelques dernières années, l'IoT est devenu l'une des technologies les plus importantes du 21ème siècle. Maintenant que nous pouvons connecter des objets du quotidien (appareils électroménagers, voitures, thermostats, interphones bébés) à Internet par l'intermédiaire de terminaux intégrés, des communications sont possibles en toute fluidité entre les personnes, les processus et les objets.

Grâce à des traitements informatiques peu coûteux, au cloud, au Big Data, à l'analytique et aux technologies mobiles, les objets physiques peuvent partager et collecter des données avec un minimum d'intervention humaine. Dans ce monde hyper-connecté, les systèmes digitaux peuvent enregistrer, surveiller et ajuster chaque interaction entre les objets connectés. Le monde physique rencontre le monde digital, et ils coopèrent [4].

5. Quelles sont les technologies qui ont rendu l'IoT possible

Alors que l'idée de l'Internet des objets existe depuis longtemps, c'est grâce aux récents progrès technologiques que cette idée a pu se concrétiser :

1. **Capteurs et actionneurs** : Les capteurs mesurent les caractéristiques physiques, tandis que les actionneurs réalisent des actions concrètes dans le domaine de l'IoT. L'accès à des capteurs abordables et à faible consommation d'énergie a rendu la technologie IoT accessible à un plus grand nombre d'industries. Ces capteurs fiables et abordables ont ouvert la voie à de nouvelles possibilités.

2. **Connectivité :** la prolifération des protocoles de réseau pour Internet a simplifié la connectivité des capteurs avec le cloud et d'autres objets, ce qui a permis des transferts de données plus efficaces.

3. **Plates-formes cloud :** la disponibilité croissante des plateformes cloud offre aux entreprises et aux consommateurs l'infrastructure nécessaire pour évoluer, sans avoir à se soucier de sa gestion.

4. **Machine learning et analyses :** les avancées dans le domaine de l'apprentissage automatique et de l'analyse des données ont permis aux entreprises d'obtenir plus rapidement et plus facilement des informations à partir des vastes quantités de données stockées dans le cloud. Ces technologies continuent de repousser les limites de l'IoT, tandis que les données produites par l'IoT alimentent à leur tour ces technologies.

5. **Intelligence artificielle (IA) conversationnelle :** les progrès réalisés dans les réseaux neuronaux ont permis aux appareils IoT de gérer le traitement du langage naturel, ce qui a rendu les assistants personnels numériques tels qu'Alexa, Cortana et Siri attrayants, abordables et adaptés à une utilisation domestique [4].

6. Architectures de l'IoT

6.1 Architecture à trois couches

En général, l'architecture de l'IoT est divisée en trois couches de base : la couche application, la couche réseau et la couche perception, qu'on verra plus en détail ci-dessous :

6.1.1 Couche perception

Également connue sous le nom de couche de capteur, interagit avec les dispositifs et composants physiques à l'aide de dispositifs intelligents (RFID, capteurs, actionneurs, codes à barres 2D, GPS etc.). Son objectif est de connecter les objets à un réseau IoT et de collecter et traiter les informations associées à ces derniers via les dispositifs intelligents déployés, en transmettant les informations traitées à la couche supérieure à travers des interfaces de couche et de les transformer en signaux numériques [5].

Pour percevoir les propriétés d'objets qui ne peuvent être perçus directement, il faut implanter un microprocesseur dans leur corps. Les puces peuvent détecter des données telles que la température, la vitesse, etc. et les traiter. Cette approche requiert une nanotechnologie pour rendre les puces assez petites pour être implantées dans tout type d'objet, y compris le sable. Ainsi, la nanotechnologie et la technologie d'intelligence embarquée sont considérées comme des technologies clés pour la couche de perception [6].

6.1.2 Couche réseau

Appelée également couche de transmission, est implémentée comme la couche intermédiaire de l'architecture de l'IoT. Son rôle est de recevoir les informations traitées provenant de la couche de perception et de déterminer les routes pour transmettre les données et les informations au centre de traitement. Cette couche est considérée comme la plus importante de l'architecture de l'IoT, car elle intègre de nombreux dispositifs (nœud central, commutateurs, passerelles, cloud computing, etc.) et différentes technologies de communication (Bluetooth, WiFi, LTE, Zigbee, FTTx etc.) [5]. À cette couche, nous pouvons trouver de nombreux protocoles, tels qu'IPv6, qui est nécessaire pour l'adressage de milliards d'objets. Le but de la couche réseau est de transmettre les données entre différents objets ou applications en utilisant des interfaces ou des passerelles entre des réseaux hétérogènes et en prenant en compte divers protocoles de communication.

6.1.3 Couche application

Elle est implémentée comme la couche supérieure de l'architecture de l'IoT. Ce modèle de couches décrit la structure de l'IoT au niveau technique. Elle reçoit les données transmises par la couche réseau et les utilise pour fournir les services ou les opérations requis. Par exemple, la couche d'application peut fournir un service de stockage pour sauvegarder les données reçues dans une base de données, ou fournir un service d'analyse pour évaluer les données reçues afin de prédire l'état futur des dispositifs physiques [5]**.** La fonction de cette couche est donc de fournir toutes sortes d'applications pour chaque industrie. Comme les différentes applications

favorisent le développement de l'Internet des objets, cette couche joue un rôle important dans le développement à grande échelle de l'Internet des objets.

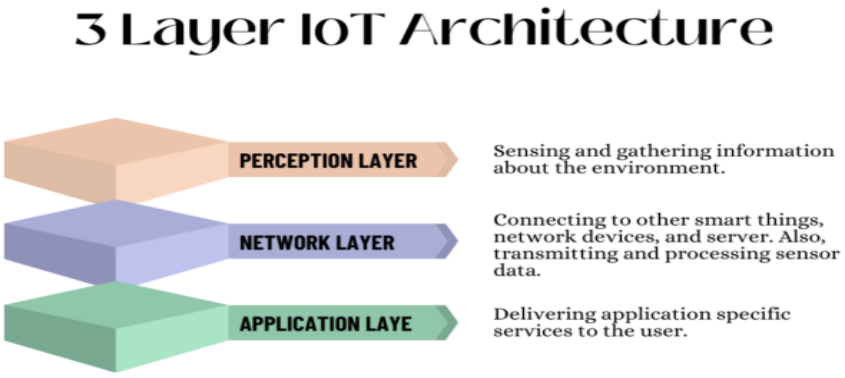


Figure I.2 *- Les 3 principales couches de l'IoT* [7]

6.2 Architecture orientée service SOA

L'architecture orientée service (SoA) est un modèle basé sur des composants utilisé pour connecter les différentes unités fonctionnelles, ou services, d'une application via des interfaces et des protocoles. Le SoA est adapté à l'architecture IoT car il permet la réutilisation des composants logiciels et matériels et améliore la faisabilité de l'architecture. Dans une architecture IoT basée sur le SoA, quatre couches existent et interagissent entre elles : la couche de perception, la couche de réseau, la couche de service (également connu sous le nom de couche intermédiaire) et la couche d'application. La couche de perception est utilisée pour mesurer, collecter et extraire les données des dispositifs physiques. La couche de réseau détermine les routes et fournit un support de transmission de données. La couche de service fournit des services pour soutenir la couche d'application et se compose de la découverte, de la composition, de la gestion et des interfaces de service. La couche d'application prend en charge les demandes de service des utilisateurs et peut prendre en charge diverses applications telles que le réseau intelligent, le transport intelligent et les villes intelligentes [5].

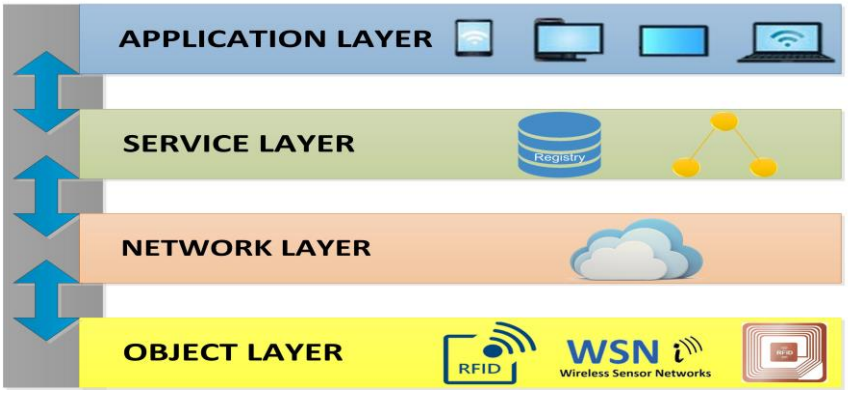


Figure I.3 *- Architecture basée sur SOA pour les systèmes IoT* [8]

6.3 Architecture Middleware

L'architecture Middleware est une architecture commune dans l'IoT. Elle aide à créer des applications de manière plus efficace en agissant comme une liaison entre les applications, les données et les utilisateurs. Cette architecture contient cinq couches : couche de perception, couche de réseau, couche de middleware, couche d'application et couche business. La couche de middleware a des fonctionnalités critiques telles que l'agrégation et le filtrage des données reçues des périphériques matériels, la découverte d'informations et le contrôle d'accès aux dispositifs pour les applications [9].

Dans le middleware, les détails des différentes technologies sont masqués et les interfaces standard sont fournies pour permettre aux développeurs de se concentrer sur le développement d'applications sans considérer la compatibilité entre les applications et les infrastructures [5]. Ses avantages sont :

- Support pour diverses applications ;
- La compatibilité avec divers systèmes d'exploitation et plateformes ;
- Calcul distribué et interaction de services parmi les réseaux hétérogènes, dispositifs et applications ;
- Support des protocoles standard ;
- Fournit des interfaces et des protocoles standards, offrant la portabilité et l'interopérabilité.
- Fournit une interface stable de haut niveau pour les applications.

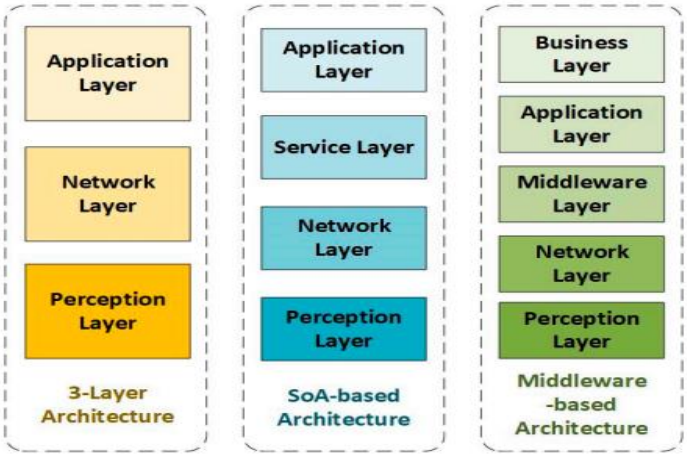


Figure I.4 *- Architectures IOT les plus courantes* [9]

7. Platforme de l'Internet of Things

Une plateforme IoT est un élément essentiel d'un écosystème global qui soutient et connecte tous les composants d'un système IoT. Elle simplifie l'approvisionnement, la gestion et l'automatisation des appareils connectés dans le domaine de l'Internet des objets. La plateforme IoT relie différents matériels au cloud en utilisant des options de connectivité solides, des mécanismes de sécurité de niveau entreprise et des capacités de traitement des données étendues. Elle offre des fonctionnalités prêtes à l'emploi qui accélèrent le développement

d'applications pour les appareils connectés, tout en garantissant l'évolutivité et la compatibilité entre les appareils [10].

La plateforme IoT est souvent qualifiée d'intergiciel (middleware) car elle fait le lien entre les appareils distants et les applications des utilisateurs, gérant toutes les interactions entre les couches matérielles et applicatives. Les plateformes IoT sont conçues pour être des médiateurs, collectant les données des appareils via différents protocoles et topologies de réseau, gérant la configuration et le contrôle à distance des appareils. Dans les écosystèmes IoT du monde réel, les intergiciels IoT sont censés être compatibles avec presque tous les dispositifs connectés et s'intégrer avec des applications tierces utilisées par ces dispositifs [11]. Cette flexibilité par rapport au matériel sous-jacent et aux logiciels permet à une plateforme IoT unique de gérer facilement tous les types de dispositifs connectés de manière cohérente.

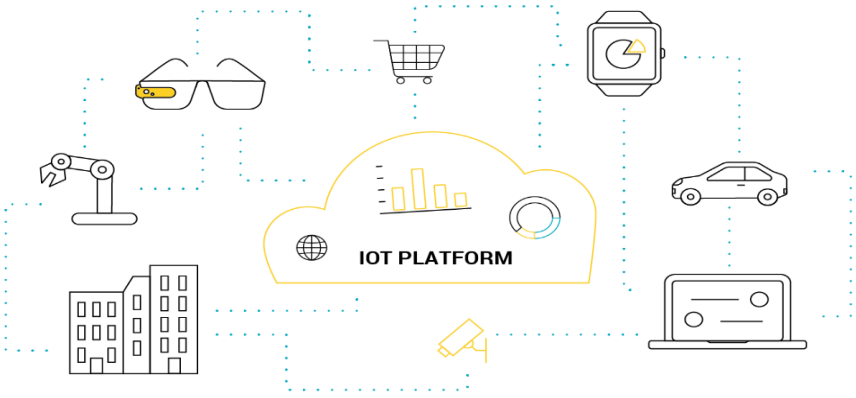


Figure I.5 *- Plateforme de l'IoT* [12]

Donc nous pouvons dire que les plateformes IoT contribuent à :

- Connecter le matériel, comme les capteurs et les dispositifs.
- Gérer différents protocoles de communication hardware et software.
- Assurer la sécurité et l'authentification des dispositifs et des utilisateurs.
- Collecter, visualiser et analyser les données recueillies par les capteurs et les appareils [13].

8. Protocoles de communication dans l'Internet of Things

Différents protocoles de communication sont utilisés dans l'Internet des objets (IoT), chacun ayant ses avantages et ses inconvénients. Voici quelques exemples de protocoles couramment utilisés dans l'IoT :

Protocole	Définition
1. MQTT (Message Queuing Telemetry Transport)	MQTT est un protocole léger conçu pour les réseaux à faible bande passante et à latence élevée. Il est utilisé pour les applications IoT nécessitant une communication en temps réel entre machines (M2M). MQTT fonctionne sur un modèle de publication/abonnement, où

	les clients s'abonnent à des canaux de communication (topics) et reçoivent les messages publiés par d'autres clients.
2. CoAP (Constrained Application Protocol)	CoAP est un protocole adapté aux objets connectés opérant sur des réseaux à faible consommation d'énergie et à bande passante limitée. Basé sur le protocole HTTP, CoAP utilise des méthodes de requête similaires (GET, POST, PUT, DELETE). Il est utilisé pour les applications IoT impliquant la communication entre capteurs et actionneurs.
3. HTTP (Hypertext Transfer Protocol)	HTTP est le protocole standard utilisé pour le transfert de données sur le Web. Il est utilisé dans l'IoT pour des applications nécessitant une communication bidirectionnelle, comme la domotique et la sécurité. Les appareils IoT utilisant le protocole HTTP peuvent être accessibles via un navigateur web ou une application mobile.
4. Zigbee	Zigbee est un protocole sans fil basé sur la norme IEEE 802.15.4. Il est utilisé dans les réseaux de capteurs sans fil et les systèmes de contrôle d'éclairage. Zigbee utilise une topologie en étoile, avec un coordinateur gérant le réseau et les connexions entre les appareils. Zigbee offre des fonctions de sécurité avancées telles que le chiffrement AES 128 bits et la gestion des clés.
5. LoRaWAN (Long Range Wide Area Network)	LoRaWAN est un protocole sans fil basé sur la technologie LoRa (Long Range). Il est utilisé dans les réseaux de capteurs sans fil à longue portée, notamment dans les applications agricoles et industrielles. LoRaWAN utilise une architecture en étoile, avec des capteurs connectés à des passerelles qui relaient les données vers un serveur central. LoRaWAN utilise également des techniques de modulation de fréquence pour améliorer la pénétration des signaux radio à travers les bâtiments et les obstacles.

Tableau 1 *– Protocoles de communication dans l'IoT*

En résumé, le choix des protocoles dans l'IoT dépend des exigences spécifiques de chaque application, telle que la bande passante, la puissance de calcul et la consommation d'énergie. Il est important de choisir le protocole le mieux adapté à chaque situation afin d'assurer une communication efficace entre les appareils IoT [14].

9. Domaines d'application de l'internet of Things

Les domaines d'application les mieux adaptées à l'IoT sont celles dont les processus métier peuvent bénéficier de l'utilisation de capteurs. Nous retrouvons les principaux domaines d'application suivants :

9.1 Domaine des villes intelligentes (Smart city)

Les villes intelligentes visent à améliorer l'infrastructure urbaine existante en mettant en place des stratégies de développement urbain. Elles utilisent diverses technologies qui différent par leurs porté et fonctionnalité telles que l'Internet, les communications sans fil, l'infrarouge le Bluetooth et le Wi-Fi [15] pour optimiser l'utilisation des ressources publiques, tout en réduisant les coûts. L'IoT joue un rôle essentiel en permettant un accès centralisé aux ressources publiques pour surveiller les transports et entretenir les espaces publics [16].

Cependant, de nouvelles solutions technologiques sont nécessaires pour gérer efficacement les ressources limitées de l'infrastructure urbaine face à une croissance démographique rapide et des contraintes financières. L'IoT offre des opportunités prometteuses pour améliorer la gestion des ressources urbaines, telles que la circulation des marchandises, la mobilité des véhicules et la protection de l'environnement. Il est particulièrement utile dans les environnements M2M et les emplacements fixes, tels que les stations météorologiques et les compteurs électriques, en prenant en charge de nombreux dispositifs de détection à faible bande passante [17].

Figure I.6 *– Ville Intelligente* [18]

9.1.1 Exemples d'utilisations

Les villes intelligentes regroupent divers secteurs tels que la gestion des eaux usées, l'éclairage urbain, le transport urbain, les services d'urgence et la gestion du trafic [19]. De nouveaux projets IoT pour les villes intelligentes émergent continuellement, adaptant les technologies disponibles aux besoins spécifiques. Pour améliorer l'efficacité des organismes publics et la qualité de vie des habitants, une plateforme IoT dédiée est essentielle. Cette plateforme collectera, traitera et interprétera les données générées par les dispositifs intelligents, établissant une infrastructure solide pour la connectivité des villes [20].

Voici un aperçu des cas d'utilisation les plus courants dans les villes intelligentes à travers le monde :

9.1.1.1 Éclairage urbain

L'éclairage urbain intelligent est devenu l'une des applications les plus populaires de l'Internet des Objets (IoT) dans les villes intelligentes. De plus en plus de villes adoptent les communications sans fil afin de réduire les coûts et de remédier aux problèmes liés à la consommation d'énergie [21]. Lumca Lighting, une société basée à Québec, offre une solution complète d'éclairage extérieur appelée "Lumca Smart Pole". Ce système intègre des fonctionnalités intelligentes telles que l'alimentation, la connectivité et les capteurs, qui sont configurés et gérés via une plateforme logicielle centralisée appelée "Digi Remote Manager". Cette solution permet aux municipalités de réaliser des économies d'énergie et de remédier aux problèmes de déficience énergétique.

9.1.1.2 Sécurité des citoyens

Les technologies de ville intelligente basées sur l'Internet des Objets (IoT) ont introduit des outils de surveillance, d'analyse et de prise de décision en temps réel pour renforcer la sécurité publique. En combinant les données provenant de capteurs sonores et de caméras de vidéosurveillance disséminées dans toute la ville avec les informations issues des médias sociaux, les solutions de sécurité publique sont capables de prédire les situations de crime potentielles. Cette approche permet aux forces de l'ordre d'anticiper les activités criminelles et d'intervenir de manière préventive [20].

9.1.1.3 L'IoT dans le trafic routier

Les villes adoptent l'Internet des Objets (IoT) pour mettre en place des solutions de gestion intelligente du trafic. Ces solutions utilisent divers capteurs et exploitent les données GPS des smartphones des conducteurs pour surveiller et contrôler le nombre, l'emplacement et la vitesse des véhicules. Parallèlement, les feux de circulation intelligents, connectés à une plateforme de gestion basée sur le cloud, permettent de surveiller les horaires des feux verts et d'ajuster automatiquement les feux en fonction des conditions de circulation actuelles afin de réduire les embouteillages [22]. De plus, en utilisant des données historiques, les solutions intelligentes de gestion du trafic peuvent prévoir les tendances de circulation et prendre des mesures pour éviter les congestions potentielles.

9.1.1.4 La norme de l'air

L'utilisation de l'Internet des Objets (IoT) dans les environnements urbains permet de surveiller la qualité de l'air dans les zones fréquentées, les parcs et les itinéraires de santé [23]. De plus, des moyens de communication sont mis en place pour permettre aux applications de santé sur les appareils des coureurs d'être connectées à l'infrastructure. Ainsi, les individus peuvent trouver le chemin le plus sain pour leurs activités en plein air et rester connectés à leur application d'entraînement préférée en permanence. Cela nécessite la mise en place de capteurs de pollution atmosphérique dans toute la ville et la mise à disposition des données des capteurs aux résidents.

9.1.1.5 Parking intelligent

Les solutions de stationnement intelligentes utilisent les données GPS des smartphones des conducteurs pour détecter l'occupation des places de stationnement et générer une carte en temps réel. Lorsqu'une place de stationnement se libère à proximité, les conducteurs reçoivent une notification et peuvent utiliser la carte sur leur téléphone pour trouver rapidement et facilement une place de stationnement, évitant ainsi de chercher au hasard.

9.1.1.6 Transports publics fiables

L'internet des objets (IoT) peut fournir aux autorités de transport en commun des informations en temps réel pour faire face aux perturbations telles que les fermetures de routes, les intempéries ou les pannes d'équipement [24]. Grâce à l'utilisation de caméras et d'appareils connectés, les plans d'urgence peuvent être mis en place pour assurer un accès continu et sécurisé aux transports publics pour les résidents.

***Figure I.7**- Les composants de la ville intelligente* [25]

9.2 Domaine de santé

L'internet des objets (IoT), un nouveau paradigme technologique, trouve des applications dans de nombreux domaines, y compris les soins de santé. Son utilisation complète dans le secteur médical présente des avantages mutuels, permettant aux établissements de santé de fonctionner de manière plus efficace et aux patients de recevoir des soins de qualité supérieure, comme le montre la figure 8. Cette technologie aide à surmonter les contraintes de ressources, tant financières qu'humaines, en permettant l'accès aux soins pour les patients éloignés des spécialistes et en aidant les communautés à faire face au vieillissement de la population [26]. En adoptant cette approche basée sur la technologie dans les soins de santé, nous pouvons nous attendre à des améliorations significatives de la qualité et de l'efficacité des traitements, contribuant ainsi à la santé globale des patients.

L'Internet des objets de santé (IoHealthcare) révolutionne le secteur des soins de santé en permettant la collecte, le stockage, l'analyse et la diffusion d'informations médicales. Cette technologie réduit le besoin de ressources humaines pour gérer ces données et améliore leur exactitude. Grâce à une analyse rapide, les ressources limitées peuvent être allouées là où elles sont le plus nécessaires dans le domaine des soins de santé.

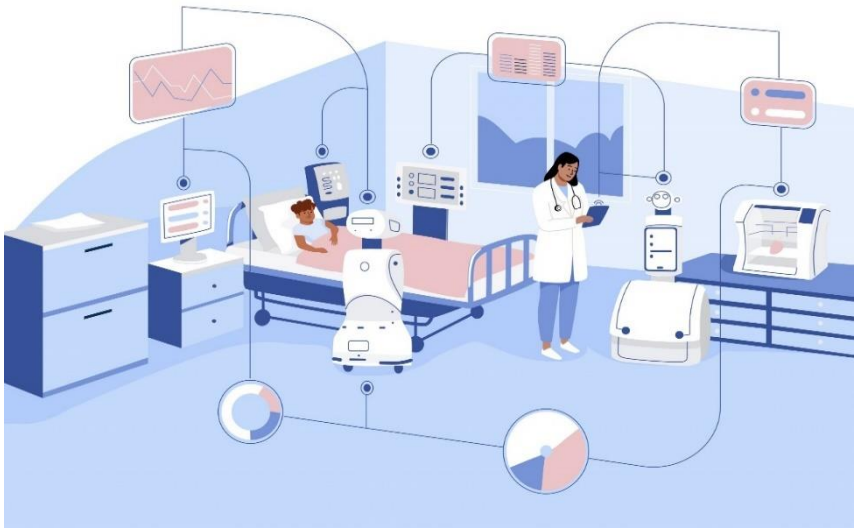


Figure I.8 *– Hôpital Intelligent* [27]

L'internet des objets (IoT) étend les possibilités d'utilisation de la technologie dans le domaine des soins de santé en connectant non seulement les individus, les applications et les données, mais aussi les capteurs et les dispositifs qui collectent des données biométriques et contextuelles. Les systèmes basés sur l'IoT peuvent être utilisés pour traiter divers problèmes de santé, qu'il s'agisse du bien-être général, de problèmes physiques ou mentaux, de soins préventifs, de traitements ou de réadaptation, ou encore de handicaps temporaires ou de maladies chroniques. Dans ce contexte, les smartphones, les montres et autres dispositifs intelligents, ainsi que des capteurs et des équipements supplémentaires, peuvent être connectés aux réseaux IoT pour fournir des informations sur l'état de santé d'une personne, ses activités et son environnement.

9.2.1 Cas d'utilisations

Dans un contexte où les coûts des soins de santé sont élevés pour la plupart des gens, où la population mondiale vieillit et où les maladies chroniques sont de plus en plus courantes, l'IoT offre la promesse d'améliorer l'efficacité des établissements de santé. Cette technologie a le potentiel de révolutionner le secteur des soins de santé dans la prochaine décennie, en offrant de multiples applications, allant de la surveillance à distance à l'intégration des dispositifs médicaux [28].

9.2.1.1 Suivi et rapports simultanés

Le suivi en temps réel à l'aide de dispositifs connectés peut sauver des vies lors d'urgences médicales telles que l'asthme, l'insuffisance cardiaque ou le diabète. Grâce à des appareils médicaux intelligents connectés à des applications mobiles, ces dispositifs collectent des données médicales et de santé essentielles, puis les transfèrent aux médecins via la connexion de données du smartphone. Les informations recueillies, telles que la pression artérielle, l'oxygène, la glycémie, le poids et les ECG, sont stockées dans le cloud et peuvent être partagées avec des personnes autorisées, comme des médecins, des compagnies d'assurance ou des consultants externes. Ainsi, ces données peuvent être consultées indépendamment de l'emplacement, de l'heure ou de l'appareil utilisé.

9.2.1.2 Repérage et alerte

Grâce à l'Internet des objets (IoT), les dispositifs peuvent collecter des données essentielles et les transmettre aux médecins pour un suivi en temps réel. Ils peuvent également envoyer des notifications aux personnes concernées via des applications mobiles et d'autres dispositifs connectés en cas de situations critiques [29]. L'IoT permet l'alerte, le suivi et la surveillance en temps réel, ce qui facilite des traitements pratiques, une meilleure précision diagnostique, une intervention appropriée des médecins et une amélioration globale des résultats dans la prestation de soins aux patients.

9.2.1.3 Réduction des coûts

Grâce à l'adoption de solutions IoT et de dispositifs médicaux connectés, les professionnels de la santé peuvent surveiller les patients en temps réel. Cela réduit le besoin de consultations médicales non nécessaires, ainsi que les séjours hospitaliers et les réadmissions, grâce à une collecte et une gestion efficaces des données.

9.2.1.4 Une meilleure expérience pour les malades

Grâce à la connexion du système de soins de santé à travers l'internet des objets, les patients s'impliquent davantage dans leur traitement, tandis que les médecins peuvent établir des diagnostics plus précis en ayant accès à toutes les informations essentielles sur leurs patients.

9.2.1.5 Réduire les erreurs et le gaspillage

L'exploitation des données IoT et l'automatisation des processus sont des méthodes efficaces pour réduire les gaspillages, comme les tests inutiles et les dépenses excessives liées à l'imagerie, tout en minimisant les coûts du système et les erreurs.

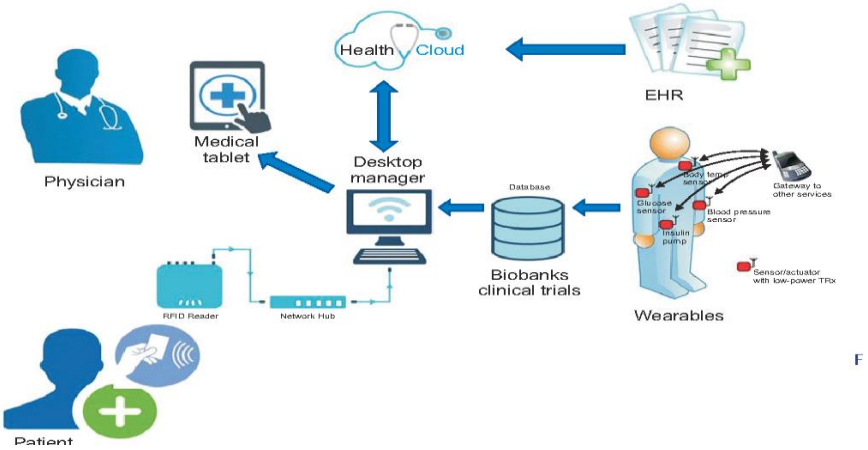


Figure I.9 *- Internet of Healthcare Things* [30]

9.3 Domaine de maisons intelligentes (Smart Home)

Une maison intelligente et connectée est une résidence équipée de capteurs, de systèmes et de dispositifs qui peuvent être contrôlés, surveillés et accessibles à distance via Internet [31]. Elle regroupe différents appareils tels que des téléphones portables, des ampoules intelligentes, des trackers de fitness, des haut-parleurs intelligents, des lave-vaisselles et des capteurs de qualité de l'eau, permettant ainsi une interconnexion variée. La domotique intelligente offre de nombreux avantages en réduisant la nécessité d'interventions humaines dans le contrôle des appareils électroniques. Les systèmes domotiques utilisent souvent des protocoles de communication tels que Z-Wave, RedTacton [32], BidCoS et ZigBee, Li-Fi [33]qui offrent des transferts de données rapides et une consommation d'énergie moindre que le Wi-Fi [34]. Un hub est utilisé pour connecter ces appareils à distance ou aux services cloud via Wi-Fi ou Ethernet filaire. Les technologies de la maison intelligente offrent des avantages tels que des économies d'énergie, un confort amélioré, un mode de vie plus respectueux de l'environnement, une plus grande sécurité et bien d'autres avantages encore [35].

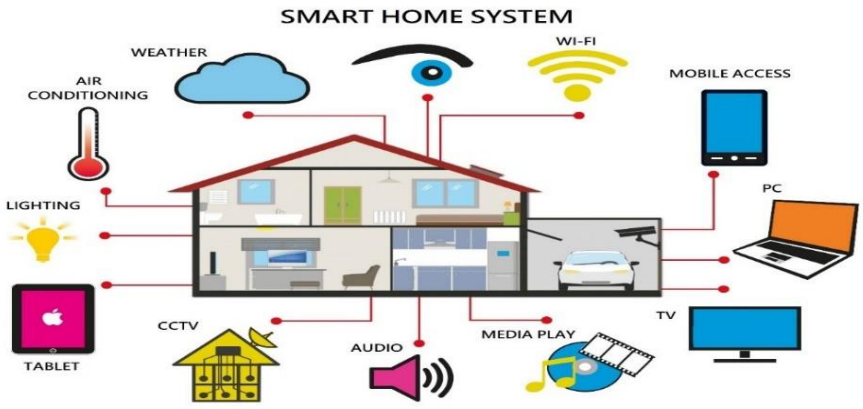


Figure I.10 *– Maison Intelligente* [36]

9.3.1 Parties prenantes (Acteurs) du Smart Home

Les maisons intelligentes nécessitent une gestion coordonnée de leurs différents gadgets, qui sont principalement des dispositifs électroniques. Cette évolution a transformé le domaine de la domotique en rendant rapidement les appareils ménagers plus accessibles et intuitifs grâce à leur intégration avec les smartphones et les tablettes [37]. Dans le contexte de l'Internet des objets (IoT), tel que les maisons intelligentes, il existe différents acteurs impliqués, allant des investisseurs technologiques aux développeurs et intégrateurs de technologies [38]. Les parties prenantes spécifiques peuvent varier en fonction du système de maison intelligente réel.

9.3.1.1 Fabricants de dispositifs

Les entreprises qui produisent des appareils, y compris celles qui proposent des produits intelligents comme les compteurs intelligents et les appareils de divertissement. Les consommateurs peuvent acheter ces appareils directement auprès des fabricants, mais le plus souvent ils passent par des revendeurs ou des prestataires de services [38]. Quelques exemples de fabricants sont Honeywell, Samsung et LG.

9.3.1.2 Les fournisseurs de réseaux

Les fournisseurs de télécommunications offrent et gèrent l'infrastructure de réseau, telle que le réseau principal, le réseau sans fil et les connexions entre les réseaux, pour les fournisseurs de services qui veulent offrir des services de maison intelligente. En d'autres termes, ce sont eux qui assurent la connexion des individus à Internet. Un exemple de fournisseur de télécommunications est Verizon.

9.3.1.3 Utilisateurs finaux

L'utilisateur final est la personne qui utilise les services. C'est généralement le résident de la maison qui achète et utilise les divers appareils et services de la maison intelligente et connectée, etc.

9.3.1.4 Régulateurs

Les régulateurs sont des organismes externes chargés de superviser les services et les secteurs industriels spécifiques. Ils sont responsables de la mise en place de normes, de certifications et d'accréditations dans des domaines tels que la qualité, la sécurité et la protection. Par exemple, un organisme de réglementation de la vie privée peut élaborer des lois visant à protéger les informations personnelles identifiables contre une utilisation abusive. Cette entité peut avoir un impact sur l'ensemble des acteurs du secteur concerné.

9.3.1.5 Fournisseurs de services

AT&T, verisure et Leak Defense sont des exemples de fournisseurs de services qui proposent aux utilisateurs finaux des équipements matériels pour prendre en charge ou activer différents services de maison connectée intelligente. Ces entreprises offrent des solutions et des dispositifs pour aider les utilisateurs à bénéficier des avantages de la maison connectée intelligente.

9.3.1.6 Fournisseurs de plateformes

Des entreprises comme Apple, Google et Amazon jouent un rôle important en fournissant des outils et des cadres qui aident à résoudre les problèmes d'intégration et permettent d'évaluer, personnaliser et automatiser les appareils connectés. Les fabricants d'appareils collaborent généralement avec ces fournisseurs de plateformes pour faciliter l'intégration de fonctionnalités tierces.

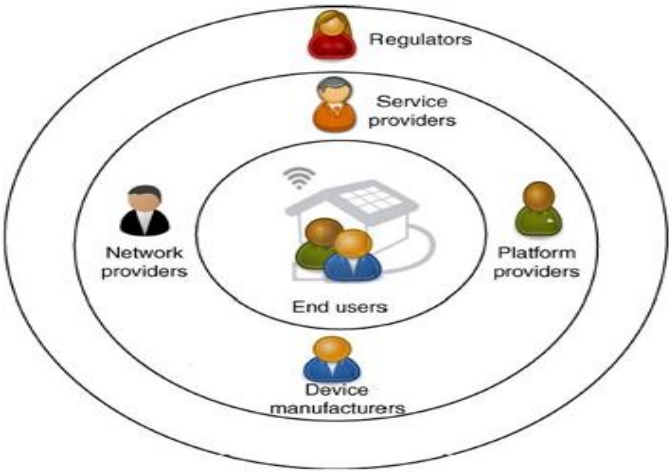


***Figure I.11**- Les acteurs de la maison intelligente* [39]

9.3.2 Architectures de la maison intelligente

L'architecture d'un système informatique définit les types de composants du système ainsi que leurs modèles d'interaction. L'architecture des maisons intelligentes est fortement influencée par les capacités de calcul de leurs composants. Il existe deux styles architecturaux principaux de maisons intelligentes et connectées : le premier centralisé et le second distribué.

9.3.2.1 Architecture centralisée

Dans une maison intelligente centralisée, le système de contrôle est géré par un ordinateur qui collecte les données des capteurs, gère l'interface utilisateur, exécute les algorithmes de contrôle et envoie des instructions aux actionneurs. Toutes les données sont centralisées et gérées par une passerelle locale spécifique. Cette passerelle est responsable de la logique du système, du stockage des données et de la communication avec les appareils connectés à la maison intelligente [40]. En plus de la fonction de contrôle, la passerelle assure également l'interface avec Internet et fournit des services aux résidents de la maison. Une option possible est de limiter les fonctions de la passerelle à la collecte de données, à l'interface logicielle avec les dispositifs de la maison intelligente et aux processus essentiels [41].

9.3.2.2 Architecture distribuée

Dans une maison intelligente distribuée, le système de contrôle est conçu et mis en place comme un réseau d'ordinateurs interconnectés. Cette architecture distribuée utilise les ressources informatiques des objets connectés pour intégrer des composants logiciels dans les différents appareils de la maison intelligente. Bien que l'architecture puisse être conceptuellement distribuée, elle peut rester physiquement centralisée dans la passerelle domestique. Contrairement à une approche centralisée où les informations circulent par le biais d'un nœud central, dans le modèle distribué, l'architecture ressemble à un réseau pair à pair et les informations ne sont échangées que lorsque cela est nécessaire. Les dispositifs connectés dans ce modèle sont considérés comme autonomes et intelligents. Les architectures distribuées peuvent utiliser une approche basée sur les services ou une approche basée sur les agents mobiles [42]. Le principal inconvénient du modèle distribué est que la mise en place de la sécurité du réseau est plus complexe par rapport à une approche centralisée.

9.3.3 Catégories de services

La maison connectée intelligente regroupe différents services domestiques intelligents pour offrir un environnement pratique, bénéfique et sécurisé aux membres du foyer, les aidant ainsi à accomplir efficacement leurs tâches ménagères [42]. En général, les systèmes de maison connectée intelligente peuvent être regroupés en quatre catégories : les services de soins de santé, de sécurité, d'énergie et de divertissement.

9.3.3.1 Soins de santé

Le secteur des services de santé se concentre sur la fourniture de soins de santé mobiles et de soutien à la forme physique, dans le but de permettre une vie saine et autonome. Contrairement à d'autres domaines, les services de santé incluent également l'utilisation de capteurs portables qui permettent une surveillance continue des signes vitaux, même en dehors du domicile. Il s'agit de dispositifs connectés tels que des appareils de mesure physiologique, des moniteurs de fitness et des balances sans fil.

9.3.3.2 Services de sécurité

Les systèmes de sécurité sont conçus pour surveiller, détecter et contrôler les menaces à la sécurité et à la sûreté. Dans le contexte des maisons intelligentes, ces systèmes vont des services de surveillance à distance des entrées à des systèmes capables de reconnaître automatiquement les dangers physiques tels que les incendies ou les cambriolages, et de prendre les mesures appropriées de manière autonome [43]. Ce domaine comprend des fonctionnalités telles que les systèmes d'alarme, les caméras de sécurité et les serrures de porte intelligentes.

9.3.3.3 Divertissement

Les systèmes domestiques intelligents et connectés visent à rendre le divertissement plus agréable en offrant du contenu personnalisé et des services de communication sociale [43]. Dans ce domaine, nous retrouvons généralement des haut-parleurs intelligents, des téléviseurs connectés et des consoles de jeux.

9.3.3.4 Énergie

Les systèmes énergétiques cherchent à gérer l'énergie de manière efficace dans les maisons. Cela implique l'utilisation de compteurs intelligents, de thermostats intelligents et de systèmes d'éclairage adaptatifs. Dans ce domaine, les systèmes peuvent utiliser des technologies intelligentes et des méthodes de contrôle pour prédire et maximiser automatiquement l'efficacité énergétique et le confort de l'utilisateur.

9.4 Domaine de l'Industrie (IIoT)

L'internet industriel des objets (IIoT) désigne l'extension et l'utilisation de l'internet des objets (IoT) dans les secteurs industriels et les applications. Mettant fortement l'accent sur le big data, la communication de machine à machine et l'apprentissage automatique, l'IIoT permet aux industries et aux entreprises d'améliorer l'efficacité et la crédibilité de leurs opérations. L'internet industriel des objets se compose d'une multitude d'appareils connectés par des logiciels de communication, Les systèmes de résultats, et même les appareils individuels qui les composent, peuvent échanger, analyser, surveiller, collecter et agir instantanément sur les informations pour transformer intelligemment leur comportement ou leur environnement, le tout sans intervention humaine. L'IIoT peut être considéré comme un très grand nombre de systèmes industriels connectés qui communiquent et coordonnent leurs analyses de données et leurs actions afin d'améliorer les performances industrielles et d'avantager la société dans son ensemble. Les systèmes industriels qui relient le monde numérique au monde réel par l'intermédiaire de capteurs et d'actionneurs qui résolvent des problèmes de contrôle sophistiqués sont communément appelés systèmes cyber-physiques.

Il existe deux points de vue sur la différence entre l'internet des objets industriel (IIoT) et l'internet des objets (IoT). Le premier point de vue est qu'il s'agit de deux domaines d'intérêt clairement distincts. L'IIoT connecte des machines et des capteurs critiques dans des secteurs à fort enjeu tels que les transports, les équipements de manutention des ports maritimes, les soins de santé, l'énergie et le contrôle industriel. Il s'agit de systèmes dans lesquels un échec se traduit souvent par une menace pour la vie ou d'autres situations d'urgence. Les systèmes IoT ont tendance à être des dispositifs grand public tels que les thermomètres domestiques intelligents, les outils de fitness portables et les distributeurs automatiques de nourriture pour animaux de compagnie. Le deuxième point de vue considère l'IIoT comme l'infrastructure qui doit être mise en place avant que les applications IoT puissent être développées. L'IoT, dans une certaine mesure, dépend de l'IIoT industriel.

L'IIoT se concentre sans hésitation sur les systèmes cyber-physiques intelligents. Ces systèmes sont constitués de machines connectées à des ordinateurs qui interprètent, analysent et prennent des décisions presque instantanément, sur la base de données de capteurs provenant de nombreuses sources largement distribuées. L'IIoT permet au système intelligent de votre voiture de freiner automatiquement lorsqu'il détecte un obstacle sur la route. Il permet au système de surveillance des personnes malades dans les hôpitaux de tout suivre, du rythme cardiaque du patient à la pénétration de ses médicaments. Il permet à une machine minière ou

à un robot spatial de se protéger et d'opérer efficacement là où les humains ne peuvent pas le faire [44] [45][46].

Figure I.12 *- Représentation de l'Internet Industrial of Things* [47]

10. Challenge et enjeux de l'Internet of Things

Dans cette section, nous allons aborder l'essentiel des défis populaires ou des défis généraux de l'environnement IoT

10.1 Sécurité

La sécurité est une préoccupation importante dans les technologies de l'information, et l'internet des objets présente des défis de sécurité spécifiques. Il est essentiel de relever ces défis et de garantir la sécurité des produits et services IoT. Les utilisateurs doivent avoir confiance dans la protection de leurs appareils et de leurs données, car l'IoT devient de plus en plus présent dans notre quotidien. Des appareils et services IoT mal sécurisés peuvent être vulnérables aux cyberattaques et mettre en danger les données des utilisateurs. L'interconnexion des appareils IoT signifie que la sécurité de chaque appareil affecte la sécurité globale d'Internet. Ce défi est aggravé par le déploiement massif d'appareils IoT similaires, leur capacité à se connecter automatiquement et leur utilisation dans des environnements non sécurisés. Les développeurs et utilisateurs d'appareils IoT ont la responsabilité de protéger les utilisateurs et Internet contre les dommages potentiels. Il est nécessaire de collaborer pour trouver des solutions adaptées à l'échelle et à la complexité des problèmes de sécurité de l'IoT.

10.2 Confidentialité

Le plein potentiel de l'internet des objets dépend de stratégies qui respectent les choix individuels en matière de protection de la vie privée. Les dispositifs de l'IoT peuvent offrir une grande valeur aux utilisateurs, mais les préoccupations concernant la vie privée peuvent entraver son adoption complète. Le respect du droit à la vie privée et des attentes des utilisateurs est essentiel pour établir la confiance dans l'internet, les appareils connectés et les services associés. L'internet des objets redéfinit le débat sur la vie privée, car il modifie la collecte, l'analyse, l'utilisation et la protection des données personnelles. Par exemple, l'IoT soulève des inquiétudes concernant la surveillance accrue, la difficulté à refuser la collecte de données et l'agrégation des données pour créer des profils détaillés des utilisateurs. Ces défis peuvent être surmontés en élaborant des stratégies qui respectent les choix individuels en matière de vie privée tout en favorisant l'innovation technologique et les nouveaux services [2].

10.3 Réseautage

La mise en réseau est très importante dans l'Internet car elle implique des éléments clés pour gérer les réseaux. Une étude [48] a abordé les défis liés aux réseaux via des réseaux mobiles ad hoc (MANET). Les chercheurs ont interconnecté des réseaux mobiles ad hoc avec des réseaux fixes grâce à des passerelles. Dans l'IoT, il est difficile de prédire où un objet se déplace et il peut être nécessaire de le faire passer d'un réseau à un autre. Le problème principal réside dans le changement fréquent des passerelles et la difficulté à localiser les objets. Les réseaux mobiles ad hoc (MANET) sont composés de nœuds mobiles auto-organisés ou d'objets, et ils offrent un moyen de maintenir une connexion. De plus, les réseaux multi-homed ad hoc sont considérés comme une extension de l'infrastructure existante dans l'IoT.

10.4 Hétérogénéité

L'environnement de l'IoT est un exemple d'hétérogénéité, car il comprend de nombreux dispositifs différents. L'objectif principal de l'IoT est de trouver un moyen de gérer cette hétérogénéité et d'exploiter au mieux la fonctionnalité de ces dispositifs. Dans une étude [49], des chercheurs ont proposé des solutions pour résoudre certains problèmes de l'IoT, tels que l'interconnexion et l'hétérogénéité. Ils ont créé un langage spécialisé, un éditeur graphique et une plateforme IoT appelée Midgar. Cette plateforme permet de gérer les objets intelligents hétérogènes dans l'environnement IoT et facilite leur interaction, quel que soit leur type. Midgar évite les complexités des méthodes traditionnelles de gestion de ce problème. De plus, l'IoT utilise une approche appelée architecture orientée services (SOA) pour améliorer le fonctionnement des ressources hétérogènes, comme les capteurs et les actionneurs. Cette approche offre une grande flexibilité et évolutivité au système, tant pour l'intégration externe que pour les échanges au sein du middleware.

10.5 Interopérabilité

L'utilisation de différentes technologies propriétaires pour l'IoT peut nuire à sa valeur pour les utilisateurs et l'industrie. L'absence d'interopérabilité entre les produits et services peut

rendre l'intégration difficile, augmenter la complexité et susciter des inquiétudes quant à la dépendance envers les fournisseurs. De plus, les dispositifs IoT mal conçus et mal configurés peuvent perturber les ressources réseau et l'internet dans son ensemble. L'adoption de normes, de modèles de référence et de bonnes pratiques permettra de réduire le nombre de dispositifs perturbateurs. L'utilisation de normes ouvertes et largement disponibles, comme le protocole Internet, favorisera les avantages pour les utilisateurs, l'innovation et les opportunités économiques [2].

L'interopérabilité consiste à créer des systèmes ou des dispositifs qui peuvent coopérer efficacement. Dans une étude [50], les chercheurs ont proposé une architecture basée sur l'interopérabilité sémantique pour l'informatique omniprésente et l'IoT. Cette architecture utilise une solution appelée "smart-M3" pour partager des informations sémantiques entre les agents. Elle divise l'environnement IoT en petits espaces gérables et utilise un courtier d'information sémantique pour faciliter les échanges d'informations et la surveillance en temps réel du monde physique. L'architecture montre de bonnes performances en termes d'interaction des agents et permet une interaction en temps réel avec le monde physique. Des outils sont nécessaires pour soutenir le développement et le déploiement de dispositifs et d'applications dans les futurs systèmes IoT.

10.6 Quality of Service (QoS)

La qualité de service (QoS) est définie comme le temps nécessaire pour que le message parvienne de l'expéditeur au destinataire. Si ce temps est égal ou inférieur à une exigence prédéfinie, la QoS est considérée comme atteinte. Selon l'UIT, la QoS représente le degré de conformité de la prestation de service entre le fournisseur et l'utilisateur, conformément à un accord entre eux [22]. Pour garantir la QoS, des modèles de service sont utilisés pour évaluer le niveau de QoS de chaque service Internet.

Les services Internet sont classés en différents modèles, qui offrent des fonctionnalités telles que la priorisation des applications Internet et la détermination des exigences de QoS pour répondre aux besoins des utilisateurs. Ces modèles prennent en compte des facteurs tels que le délai (temps réel dur, temps réel mou et temps non réel), la criticité de l'application et l'interactivité de l'utilisateur. Les principaux modèles de services Internet sont l'ouverture, la souplesse et la complétude, qui permettent de fournir une QoS adaptée aux services Internet. Dans une étude [20], des chercheurs ont comparé trois algorithmes (ILP, GA et BA) pour l'IoT et ont choisi l'algorithme BA en raison de ses bons résultats en temps réel, notamment pour les zones à grande échelle [23].

10.7 Cloud computing

L'informatique est omniprésente avec des exemples tels que l'informatique en nuage et l'IoT qui utilisent l'informatique distribuée. Le cloud computing offre un accès fiable et décentralisé à de nombreuses ressources informatiques, avec trois couches principales : IaaS, PaaS et SaaS. Il est considéré comme un cadre standard pour l'IoT, qui connecte le monde réel et les petits objets. Cependant, l'IoT rencontre des défis tels que le stockage limité, l'évolutivité et la confidentialité, tandis que le cloud computing offre une capacité de traitement pratiquement

illimitée. L'intégration de l'informatique en nuage à l'IoT est un sujet de recherche majeur pour surmonter les défis liés à la confidentialité, à l'évolutivité, aux ressources de stockage et à la virtualisation, en exploitant la puissance de traitement du cloud computing pour les capteurs et autres composants de l'IoT [37].

11. Conclusion

L'internet des objets a révolutionné notre façon de vivre et de travailler en connectant des appareils physiques à l'internet et en leur permettant de communiquer entre eux. Il a permis des avancées sans précédent dans divers secteurs, notamment les soins de santé, l'agriculture, les transports et la fabrication, pour n'en citer que quelques-uns. Il a permis de créer de nouveaux modèles commerciaux, d'accroître l'efficacité et la productivité, et d'améliorer notre qualité de vie.

Cependant, l'adoption généralisée de la technologie IoT suscite également des inquiétudes en matière de confidentialité, de sécurité et de gestion des données. Avec le nombre croissant d'appareils connectés et les grandes quantités de données qu'ils génèrent, il existe un besoin croissant de normes, de réglementations et de meilleures pratiques pour garantir une utilisation sécurisée et responsable de la technologie IoT.

L'internet des objets est une technologie qui évolue rapidement et qui a le potentiel d'apporter des avantages considérables, mais il faut aussi l'examiner et la gérer avec soin pour s'assurer que son impact est positif et durable. Alors que l'IoT continue de se développer, il sera important que les individus et les organisations coopèrent afin de trouver un équilibre entre innovation et sécurité.

Dans le chapitre suivant nous allons étudier les principes du monitoring et de la sécurité

II ***Chapitre : Monitoring et Sécurité dans l'IoT***

1. Introduction

Les objets connectés dans l'IoT sont capables d'interagir avec leur environnement et d'effectuer des taches de manière autonome, sans nécessiter de contrôle extérieur. Cette capacité peut causer divers problèmes de sécurité et de confidentialité. Comme dans tout réseau de communication la plupart des appareils connectés sont vulnérables aux attaques, aux piratages et aux logiciels malveillants en raison de leur capacité limitée de calcul, de stockages et de réseau, les rendant plus susceptibles aux cyberattaques que d'autres types d'appareils tels que les ordinateurs, les smartphones etc. [51] [52] En effet, les nombreuses interconnexions entre les objets et les utilisateurs, ainsi qu'entre les objets eux-mêmes, créent de vastes quantités de données difficiles à gérer. Sachant que les appareils IoT collectent et transmettent souvent des données sensibles telles que des informations personnelles et des données de localisation, ce qui peut compromettre la vie privée des utilisateurs.

Le monitoring et la supervision sont des pratiques à considérer dans l'IoT, et pour cause, les appareils connectés peuvent être déployés à grand échelle et éloignés géographiquement, ce qui rend difficile la surveillance manuelle. Le monitoring consistant à surveiller les dispositifs en temps réel, à détecter rapidement les problèmes et à prendre des mesures préventives avant que ça ne devienne critique. La supervision, quant à elle, impliquant la prise en charge proactive des systèmes IoT pour maintenir leur fonctionnement. Il est donc impératif de tenir compte de ces mesures de contrôle pour garantir le bon déroulement des opérations des appareils connectés.

La sécurité dans l'IoT est donc un défi complexe et une préoccupation croissante qui nécessite une attention particulière. Pour se protéger de ce type de problèmes ; la surveillance, le monitoring et la supervision sont des pratiques nécessaires pour assurer la fiabilité, la sécurité et le bon fonctionnement des dispositifs IoT.

Dans ce chapitre, nous nous pencherons sur les principes fondamentaux du monitoring et de la sécurité dans l'IoT. Nous explorerons les défis uniques auxquels nous sommes confrontés dans cet environnement complexe et dynamique. En particulier, nous aborderons une attaque spécifique qui a gagné en notoriété ces dernières années : l'attaque hello flood.

2. Généralités sur le monitoring

2.1 Contexte et importance du monitoring en général

L'IoT (Internet des objets) fait référence à un réseau d'appareils connectés à Internet qui collectent et échangent des données. Ces dispositifs peuvent inclure des capteurs, des caméras, des appareils portables et d'autres technologies connectées.

La surveillance est importante dans l'IoT car elle permet de surveiller et de protéger les données collectées par ces dispositifs connectés. En effet, l'IoT peut générer une quantité massive de données qui peuvent être sensibles et nécessitent d'être protégées. La surveillance permet également de surveiller le fonctionnement des dispositifs connectés pour détecter les pannes ou les erreurs, et pour améliorer la fiabilité du système.

En outre, la surveillance dans l'IoT peut aider à prévenir les attaques de sécurité, telles que les piratages ou les violations de données, en surveillant les activités suspectes sur le réseau et en signalant les anomalies. Cela est particulièrement important étant donné que les dispositifs connectés peuvent souvent être vulnérables aux attaques de sécurité en raison de leur manque de protection et de leur configuration parfois par défaut.

En somme, la surveillance dans l'IoT est essentielle pour protéger les données et les dispositifs connectés, et pour garantir la sécurité et la fiabilité du système dans son ensemble [53].

2.2 Définition

Le monitoring est une méthode de collecte et d'analyse de données en temps réel sur un système ; la disponibilité, la sécurité, le débit, l'utilisation des ressources etc. C'est un processus qui permet d'identifier les problèmes potentiels, et de détecter les comportements inhabituels ou les signes de dysfonctionnement avant qu'ils n'affectent l'expérience des utilisateurs, de surveiller et d'évaluer les performances pour s'assurer que le système fonctionne correctement et de manière optimale, et de mettre en place des mesures préventives et correctives si nécessaire [54].

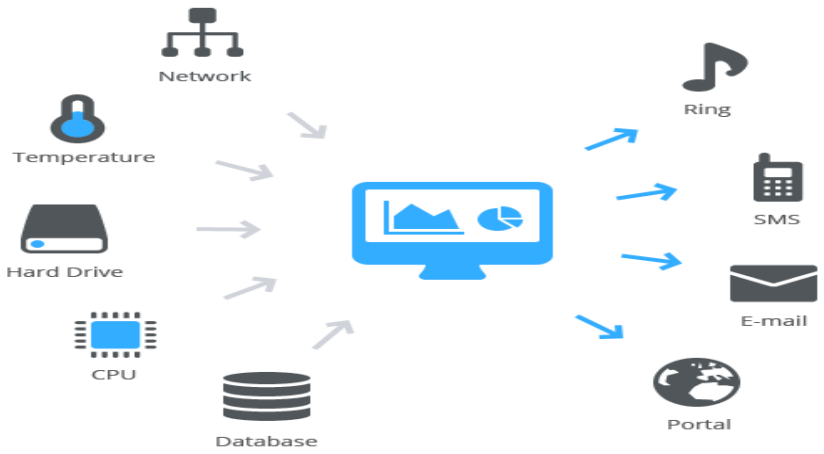


Figure II.1 *- Monitoring et supervision des réseaux* [55]

2.3 Objectif du monitoring

En général, le monitoring vise à surveiller et à collecter des données sur des processus, des systèmes ou des équipements, afin de prendre des décisions informées pour améliorer leur performance. Il permet de :

- Surveiller en temps réel : Le monitoring collecte et analyse les données en temps réel pour détecter les problèmes dès qu'ils se produisent.
- Prévenir les problèmes : En surveillant régulièrement les processus et les équipements, le monitoring peut aider à détecter les signes avant-coureurs de problèmes et à les résoudre avant qu'ils ne deviennent critiques.

- Optimiser les performances : Le monitoring permet d'analyser les données collectées pour identifier les domaines où des améliorations peuvent être apportées, afin d'optimiser la performance d'un système ou d'un processus.

Dans le contexte de l'IoT, le monitoring est crucial pour garantir le bon fonctionnement des dispositifs connectés et assurer la sécurité des données. Les objectifs spécifiques du monitoring dans l'IoT comprennent :

- Surveiller les dispositifs connectés : Le monitoring permet de surveiller les dispositifs connectés pour détecter les pannes et les problèmes de performance, et prendre des mesures pour les résoudre.
- Sécuriser les données : Les dispositifs IoT sont souvent vulnérables aux attaques de sécurité. Le monitoring permet de surveiller les données pour détecter les tentatives de piratage et prendre des mesures pour protéger les données.
- Collecter des données : Le monitoring est également utilisé pour collecter des données sur l'environnement physique, les comportements des utilisateurs et les performances des dispositifs, afin d'améliorer les opérations et de fournir des services personnalisés [1].

2.4 Méthodes du monitoring

Les méthodes de monitoring sont essentielles pour collecter, analyser et visualiser les données en temps réel. Voici quelques-unes des méthodes de monitoring utilisées en général et dans l'IoT :

En général, les méthodes de monitoring comprennent :

- Supervision en temps réel : Cette méthode permet de surveiller les processus, les équipements et les applications en temps réel. Elle fournit une vue en direct de la performance du système et permet de détecter les problèmes avant qu'ils ne deviennent critiques.
- Analyse des données : L'analyse des données est utilisée pour extraire des informations pertinentes à partir de données collectées par les dispositifs de monitoring. Elle permet de détecter les tendances et les anomalies, et de prendre des décisions pour améliorer la performance du système.
- Visualisation : La visualisation est utilisée pour afficher les données collectées sous forme de graphiques, de tableaux ou de diagrammes, pour faciliter la compréhension et l'analyse des données.

Dans le contexte de l'IoT, les méthodes de monitoring comprennent :

- Capteurs : Les capteurs sont utilisés pour collecter des données sur l'environnement physique et les comportements des utilisateurs. Ils permettent de surveiller la performance des dispositifs IoT et d'analyser les données collectées.
- Edge computing : L'edge computing permet d'analyser les données collectées par les dispositifs IoT sur place, plutôt que de les envoyer à un centre de données distant pour

analyse. Cela permet une analyse en temps réel des données et une réactivité plus rapide aux problèmes.

- Machine learning : Le machine learning est utilisé pour analyser les données collectées par les dispositifs IoT et pour détecter les tendances et les anomalies. Cela permet de prendre des décisions pour améliorer la performance des dispositifs IoT [24].

2.5 Domaines d'application de la surveillance dans l'IoT

La surveillance dans l'IoT peut avoir des domaines d'application très divers. En voici quelques exemples :

- La surveillance de la qualité de l'air ou de l'eau dans les villes intelligentes, avec des capteurs IoT placés dans différents endroits pour mesurer la pollution et la qualité de l'environnement [56].
- La surveillance de la santé à domicile, avec des dispositifs portables tels que des montres connectées ou des capteurs intégrés dans les vêtements, pour surveiller les signes vitaux et les activités quotidiennes des patients atteints de maladies chroniques ou en convalescence[1].
- La surveillance de la sécurité dans les usines, les entrepôts ou les bâtiments intelligents, avec des capteurs et des caméras IoT pour détecter les incidents, les intrusions ou les défaillances des équipements [57].
- La surveillance des équipements industriels, avec des capteurs et des dispositifs IoT pour surveiller les performances, la maintenance et les pannes des machines [24].
- La surveillance des cultures agricoles, avec des capteurs IoT pour mesurer les niveaux d'humidité, de température, de lumière et de nutriments dans les sols et les plantes [57].
- La surveillance du trafic routier et de la sécurité routière, avec des capteurs IoT pour mesurer la densité de la circulation, les vitesses des véhicules et les conditions météorologiques [56].

Ces exemples ne sont pas exhaustifs et il existe de nombreuses autres applications de la surveillance dans l'IoT. Les technologies et les protocoles de l'IoT sont en constante évolution, ouvrant ainsi de nouvelles possibilités pour l'application de la surveillance dans différents domaines.

2.6 Comment superviser et quels sont les problèmes à contrôler dans l'IOT

La supervision de l'IoT implique la surveillance continue des capteurs, des appareils connectés et des réseaux pour s'assurer qu'ils fonctionnent correctement et pour détecter les anomalies ou les pannes. Il est important de surveiller les indicateurs de performance clés pour optimiser la disponibilité, la qualité de service, la sécurité et la gestion des ressources.
Voici quelques problèmes courants à surveiller dans l'IoT, et les méthodes pour les contrôler :

1. **Disponibilité** : Il est important de surveiller la disponibilité des appareils et des réseaux pour s'assurer qu'ils fonctionnent correctement. Les outils de surveillance peuvent être utilisés pour détecter les pannes, les déconnexions et les problèmes de connectivité. Les capteurs peuvent être surveillés pour s'assurer qu'ils sont alimentés et qu'ils envoient les données de manière régulière. La surveillance de la disponibilité peut également aider à identifier les problèmes liés à la configuration ou à la gestion du réseau.

2. **Sécurité** : Les failles de sécurité peuvent entraîner des violations de données, des attaques de malwares et compromettre la confidentialité et l'intégrité des données. Il est important de surveiller les appareils pour détecter les tentatives de piratage, les vulnérabilités et les menaces de sécurité. Les données peuvent être cryptées pour empêcher leur interception, et les mesures de sécurité, comme l'authentification et l'autorisation, peuvent être mises en place pour contrôler l'accès aux données.

3. **Performances** : La surveillance des performances permet de s'assurer que les appareils répondent aux exigences de performance et de qualité de service. Les indicateurs clés de performance incluent le temps de réponse, le débit, la latence et la qualité de service. Les outils de surveillance peuvent être utilisés pour surveiller ces indicateurs et pour identifier les goulets d'étranglement, les problèmes de capacité et les goulots d'étranglement du réseau.

4. **Trafic et utilisation des ressources** : Il est important de surveiller le trafic et l'utilisation des ressources pour optimiser la disponibilité et la qualité de service, et pour éviter les surcharges. Les outils de surveillance peuvent être utilisés pour surveiller le trafic réseau, les ressources système et les applications. Les alertes peuvent être configurées pour alerter les utilisateurs en cas de dépassement des seuils critiques [58].

Les outils de supervision de l'IoT incluent des plates-formes de gestion de l'IoT, des logiciels de surveillance des réseaux, des outils d'analyse des données et des outils de surveillance de la sécurité. Ces outils peuvent fournir des données en temps réel, des alertes et des rapports pour aider les utilisateurs à identifier et à résoudre les problèmes rapidement. La supervision de l'IoT peut aider à améliorer la disponibilité, la sécurité et les performances, tout en réduisant les coûts d'exploitation et de maintenance.

2.7 Outils du monitoring

Les outils de monitoring (surveillance) sont utilisés dans de nombreux domaines, tels que les systèmes informatiques, les réseaux, les serveurs, les applications web, etc. Voici quelques-uns des outils couramment utilisés dans le domaine du monitoring :

Nagios : C'est l'un des outils de monitoring les plus populaires. Il permet de surveiller les hôtes, les services, les protocoles réseau, les alertes et les notifications, ainsi que de générer des rapports et des graphiques.

Zabbix : C'est une plateforme de monitoring open source qui offre une surveillance en temps réel des performances, de la disponibilité et de l'intégrité des serveurs, réseaux et applications. Elle propose également des fonctionnalités avancées telles que la collecte de données, l'analyse des tendances et la corrélation des événements.

Hyperic : Hyperic, également connu sous le nom de VMware vRealize Hyperic, est un outil de monitoring et de gestion des performances largement utilisé dans les environnements informatiques. Il est conçu pour surveiller les applications, les serveurs, les bases de données, les systèmes d'exploitation, les infrastructures virtuelles et d'autres composants.

SolarWinds : C'est une suite d'outils de surveillance réseau et de gestion des performances. Elle permet de surveiller les équipements réseau, les serveurs, les applications, les bases de données et plus encore. Elle offre des fonctionnalités avancées telles que la visualisation des topologies, l'analyse des performances, les alertes et les rapports détaillés.

IBM Tivoli Monitoring : C'est une solution de monitoring et de gestion des performances qui permet de surveiller les applications, les serveurs, les bases de données, les services web et les environnements virtualisés. Il offre des fonctionnalités de suivi en temps réel, d'alerting de génération de rapports et d'analyse des tendances.

ManageEngine OpManager : C'est un outil de monitoring réseau et de gestion des performances qui permet de surveiller les équipements réseau, les serveurs, les applications, les bases de données, les services cloud, etc. Il offre des fonctionnalités de cartographie réseau, d'alerting, de reporting et de gestion des configurations [59]**.**

3. Sécurité dans l'Internet des Objets

3.1 Définition de la sécurité dans l'Iot

La sécurité dans l'IoT fait référence à la sécurité des appareils connectés à internet tels que les capteurs, les caméras, les thermostats et autres objets intelligents. La sécurité de l'IoT implique la fusion de la cybersécurité avec d'autres disciplines d'ingénierie. En d'autres termes, elle ne traite pas seulement des données, des serveurs, des réseaux et de la sécurité de l'information, mais elle comprend également la surveillance et le contrôle de l'état des systèmes physiques connectés à internet. Cela peut inclure des machines, des systèmes de transport, des équipements de productions et d'autres systèmes physiques qui peuvent être contrôlés ou surveilles via Internet.

La sécurité de l'IoT est un domaine complexe et diversifié qui nécessite une approche globale pour assurer la protection de tous les aspects du système. Elle prend en compte non seulement les aspects de cybersécurité tels que la confidentialité, l'intégrité et la disponibilité des données,

mais aussi les aspects physiques tels que la sécurité des dispositifs et celle des utilisateurs qui interagissent avec ces systèmes [60].

3.2 Exigences de la sécurité dans l'IoT

Pour garantir un déploiement sécurisé de l'IoT, il est essentiel de prendre en compte les principes fondamentaux que nous verrons plus-bas. En respectant ces principes, l'IoT peut offrir des avantages significatifs tout en minimisant les risques de sécurité.

- **Confidentialité** : Les appareils IoT peuvent stocker des informations sensibles par exemple les données médicales, personnelles, militaires etc. [61] Le principe de confidentialité implique que les services non autorisés ne doivent pas être en mesure d'accéder aux données sensibles et confidentielles. Il implique aussi la protection de la vie privée et des informations propriétaires [52] [62].

- **Intégrité** : Il s'agit de garantir que les informations et les dispositifs IoT ne puissent pas être modifier ou utilisés par des utilisateurs et des objets non autorisés. Des attaquants peuvent tenter de manipuler les données en insérant des parties de données falsifiées dans les messages transmis afin de modifier leur sens original, ce qui peut causer de graves dommages. C'est pourquoi il est indispensable d'avoir des mécanismes de sécurité qui garantissent l'intégrité des données transmises telles que le chiffrement, la signature numérique, les codes de hachage afin de protéger les informations contre les attaques externes et s'assurer que les données collectées par les dispositifs IoT sont fiables et non altérées [52] [62].

- **Disponibilité** : Cette propriété garantit que les ressources informatiques et les informations sont disponibles pour les services qui en ont besoin et qui ont été autorisés à y accéder [52]. Cela est particulièrement important dans les applications IoT, où de nombreux nœuds peuvent avoir besoin d'accéder aux mêmes ressources pour fournir des informations en temps réel ou prendre des décisions critiques. Ainsi en garantissant la disponibilité des ressources systèmes nous pouvons assurer que les nœuds peuvent accéder aux informations dont ils ont besoin et que les décisions prises sont fiables et pertinentes [62].

- **Authentification** : Ce principe est essentiel pour garantir que les informations et les données sont authentiques et qu'elles n'ont pas été altérés ou falsifiés. Cela signifie que les parties qui participent à une transaction sont bien celles qu'elles prétendent être. Ce principe doit être respecté pour éviter toute tentative de fraude ou de falsification d'identité [52] [62].

- **Non-répudiation** : Ce dernier est l'aptitude d'un système à confirmer la réalisation ou la non-réalisation d'une action par les nœuds sources. Il est important de s'assurer que les nœuds sources ne nient pas leur authenticité lors de l'envoi des messages qui ont été générés par eux. Cela signifie que le système doit être capable de fournir une preuve que le message

a bien été envoyé par le nœud source spécifié, et que ce dernier ne peut pas nier avoir envoyé le message en question. Elle empêche donc les utilisateurs malveillants de nier leur participation à des actions pouvant causer des dommages au système [62].

- **Contrôle d'accès** : Cette propriété permet d'assurer que seules les personnes autorisées ont accès aux systèmes ou aux informations [51]. Afin de prévenir les attaques potentielles et malveillantes, il est nécessaire de reconnaitre chaque utilisateur et chaque appareil pour pouvoir appliquer les politiques de sécurité. Ainsi les capteurs non conformes dans le réseau doivent être bloqués ou se voir accorder un accès limité [62].

3.3 Enjeux et défis de la sécurité dans l'IoT

Avec l'avènement des objets connectés, il est important de connaitre les multiples enjeux et défis qui entourent la sécurité de l'IoT :

3.3.1 Enjeux de la sécurité

Matériels et logiciels : L'Internet des Objets utilise des dispositifs matériels et logiciels qui peuvent être divisés en deux catégories : les unités centrales et les unités terminales. Ces appareils permettent la récoltent les données et le contrôle les actionneurs [61].

Vulnérabilité aux cyberattaques : La plupart des dispositifs IoT sont vendus avec des identifiants faibles et par défaut (nom d'utilisateur et mot de passe) pour simplifier leur utilisation. Cependant, ce type d'identifiant peut être facilement deviné par les cyber-attaquants leurs donnant un accès facile aux appareils IoT et à leur utilisation à des fins malveillantes. D'autant plus que la plupart des utilisateurs ne modifient pas ces identifiants, laissant les dispositifs vulnérables aux attaques [61].

Dispositifs de surveillance : Quelques dispositifs IoT peuvent subir des altérations ou dysfonctionner à cause de logiciels malveillants. Il faut donc mettre en place un système de surveillance avancé capable de détecter les éventuels problèmes qui peuvent affecter les dispositifs IoT connectés au réseau [61].

Protection des données : Internet est un média public de communication, ce qui rend les données vulnérables au vol et à la modification. Si les données sont compromises, cela peut porter atteinte à la confidentialité et la sécurité de la personne concernée. Pour éviter ces risques il est essentiel d'utiliser des algorithmes de sécurité fiables pour garantir la protection des données [61].

3.3.2 Défis de la sécurité

Interopérabilité : les capacités fonctionnelles des dispositifs IoT ne devraient pas être considérablement limitées par la création et l'application de méthodes de sécurité [52].

Contraintes de ressources : Les appareils IoT ayant une mémoire et une puissance de traitement limités peuvent ne pas être en mesure de supporter les opérations couteuses des mesures de sécurité traditionnelles, telles que le cryptage asymétrique [52].

Contrôle autonome : Les systèmes informatiques classiques doivent être configuré par les utilisateurs, Par contre, les appareils IoT doivent ajuster leurs paramètres eux-mêmes (de manière autonome) [52].

Volume d'information : Un nombre croissant de menaces de sécurité pourrait viser les données sensibles et traités par de nombreuses applications IoT, Notamment le réseau électrique intelligent, la ville intelligente etc. [52]

Evolutivité : L'IoT implique un grand nombre d'appareils connecté, ce qui rend difficile la gestion de la sécurité à grande échelle. Par conséquent, les mesures de sécurité et de protection de la vie privée doivent être évolutives pour protéger l'ensemble du réseau contre les attaques potentielles [52].

Protection de la vie privée : La collecte de données constitue un risque sérieux pour la vie privée dans le cadre de l'IoT, car les dispositifs sont conçus pour générer et recueillir de nombreuses données. Les emplacements et les méthodes utilisés pour sécuriser les données posent des problèmes de confidentialité, ce qui nécessite des mesures de sécurité pour protéger ces données et les rendre inidentifiables [63].

3.4 Types d'attaques dans l'IoT

Il existe plusieurs attaques de sécurité reliée à l'IoT, dans cette section nous allons énumérer et expliquer les menaces qui pèsent sur chaque couche comme décrit ci-dessous :

3.4.1 Couche de perception

- Accès non-autorisé : Sans une authentification appropriée, ce type de violation de la sécurité peut être effectué par des personnes non autorisées, ce qui ouvre la porte à l'accès, à la modification et au préjudice des données des utilisateurs [64].

- Capture de nœuds : Les nœuds du système IoT peuvent être capturés par un attaquant. En créant de nouveaux identifiants pour les dispositifs IoT, il peut ensuite passer à la réplication d'identifiants. Cette agression peut avoir des conséquences néfastes [61].

Le nœud malveillant profite de la défaillance d'un nœud légal. Lorsque ce dernier échoue, la connexion factuelle détourne toutes les communications ultérieures par le nœud malveillant, ce qui entraîne une perte de données [65].

- Clonage d'étiquettes : Le clonage d'étiquettes (ou "tag cloning" en anglais) est une technique d'attaque qui consiste à copier les données stockées dans une étiquette RFID (Radio-Frequency

IDentification) existante et à les copier sur une autre étiquette vierge. Cette technique permet à un attaquant de créer une réplique exacte de l'étiquette d'origine, y compris son identifiant unique, son contenu et sa structure de données.
Une fois que l'étiquette clonée est créée, l'attaquant peut utiliser celle-ci pour accéder aux dispositifs IoT de la même manière que l'étiquette original. Ce dernier peut produire différentes informations ce qui peut engendrer des conséquences négatives [61].

- Attaque par injection de données erronées : Dans le but de corrompre un système IoT, de fausses données peuvent être introduites dans le système par un pirate informatique qui a pris le contrôle du dispositif ou du nœud IoT. Un comportement malveillant résulte de l'envoi de données incorrectes au centre et aux autres dispositifs IoT. De plus, les données de contrôle produites à partir de ces valeurs erronées entrainent également à des résultats de commande incorrects [61].

3.4.2 Couche réseau

- Attaque de type « Homme du milieu » (MiTM) : C'est une attaque de sécurité dans laquelle un attaquant s'immisce entre deux appareils qui communiquent entre eux (forme d'écoute illégale) pour intercepter et/ou manipuler les données qui ont été échangées. L'attaquant peut ainsi lire ou modifier les données avant qu'elles n'arrivent à leur destinataire légitime. Ces attaques comprennent le détournement de session, les serveurs mandataires malveillants, des attaques de rejeu etc. [52]

Dans le cas de l'IoT, si la connexion n'est pas sécurisée c'est-à-dire si elle n'utilise pas des protocoles de sécurité tel que le chiffrement et l'authentification, l'attaquant peut facilement accéder aux données échangées. De plus, il peut également se faire passer pour l'un des appareils auprès de l'autre, ce qui peut entrainer l'envoi de données incorrectes ou la réception de données manipulées [64].

- Attaque Hello flood : Un grand nombre de messages « hello » sont envoyés simultanément à une cible, saturant ses ressources et entrainant une interruption de service [64]. Nous analyserons cette attaque de manière plus approfondie ultérieurement.

- Sybil attaque : Cette forme d'attaque est particulièrement répondue dans les réseaux IoT et est difficile à repérer. L'attaquant manipule les nœuds et crée de fausses identités afin d'obtenir des informations et de prendre le contrôle d'un réseau de dispositifs IoT [61]. Ces identités artificielles appelés nœuds Sybil, peuvent être utilisés pour tromper les autres nœuds [52] en simulant des identités légitimes et en créant de fausses données, afin de perturber les communications ou de mener des attaques malveillantes [65].

- Warmhole Attaque : Une attaque par trou de ver dans l'IoT est une attaque difficile à identifier et destructrice. Elle implique la création d'un tunnel de communication malveillant entre deux points du réseau, et peut être réalisé en exploitant une vulnérabilité de sécurité dans les protocoles de communications.

L'attaque consiste à capturer le trafic de données d'un point réseau et à la transmettre à un autre point du réseau sans altérer l'information créant ainsi un raccourci qui contourne les nœuds intermédiaires [65]. Elle permet à l'attaquant d'accéder à des informations confidentielles ou de contrôler à distance des dispositifs IoT vulnérables.
Les conséquences de cette attaque peuvent endommager la topologie et le flux du réseau [64].

- Attaque par déni de service (DoS) : les attaques DoS visent à perturber la disponibilité des systèmes informatiques. Elles cherchent à empêcher les utilisateurs légitimes d'accéder aux ressources informatiques en les saturant de demandes ou de trafic réseau. Le Ping de la mort, le Tear Drop, l'inondation du protocole de datagramme utilisateur (UDP), l'inondation de synchronisation (SYN) et les types d'attaques de déni de service de la couche 4 sont des exemples d'attaques DoS [61].

- Spoofing attaque : Spoofing ou usurpation d'identité est un type d'attaque dans lequel l'usurpateur prend l'identité d'une autre personne pour accéder à des ressources restreintes ou voler des données. [64] L'attaquant s'introduit dans le système en obtenant l'adresse IP ou l'étiquette RFID (IP Spoofing et RFID spoofing) et envoi des données nuisibles au système [61].

- Sinkhole attaque : L'attaque Sinkhole affecte la performance des technologies de réseau IoT. Les capteurs laissés sans surveillance sont les plus sensibles aux attaques de type « sinkhole », le nœud piraté ou malveillant attire l'information de tous les nœuds environnants en créant de faux itinéraires [61] et procède a d'autre types d'attaque telles que la modification, la fabrication et la transmission sélective [65].

3.4.3 Couche application

- Virus malicieux : Un attaquant peut infecter les dispositifs et les programmes IoT avec des logiciels malveillants qui se propagent automatiquement à d'autres dispositifs ou programmes de manière autonome, comme des vers informatiques. Ce qui lui permet de compromettre rapidement un grand nombre de dispositifs. Ces logiciels malveillants ont été conçus pour altérer des données privées, surveiller l'activité des utilisateurs, prendre le contrôle des dispositifs, ou perturber le fonctionnement normal des systèmes [61].

- Attaque de phishing : Il existe plusieurs méthodes pour mener une attaque de phishing, telle que l'envoi des messages ou des courriels usurpateurs en se faisant passer pour une entité légitime. La victime en ouvrant le courriel clique sur un lien malveillant, ce qui peut entrainer l'installation d'un logiciel malveillant, le gel du système ou la divulgation d'informations confidentielles pouvant être utilisées pour le vol d'identité [66]. L'attaquant installe des programmes d'écoute de trafic pour intercepter les données sensibles échangées entre l'utilisateur et l'application. Ces programmes d'écoute peuvent être installés sur les appareils IoT des utilisateurs ou sur les serveurs hébergeant l'application [64].

- **Injection de code :** Les attaquants peuvent injecter du code malveillant dans une application IoT en exploitant une vulnérabilité de sécurité, dans le but de prendre le contrôle de l'application ou du serveur ou dans le pire des cas de l'ensemble du système [64].

- Déni de service Distribuée (DDoS) : L'attaquant peut perturber la disponibilité d'un dispositif IoT en inondant la couche application avec un grand nombre de requêtes, ce qui peut entrainer une surcharge du serveur et une indisponibilité de l'application. L'utilisateur perd le contrôle du système, ce qui permet à l'agresseur de mener toute sortes d'action malveillantes sans restriction [64].

Parmi les problèmes de sécurité rencontrés, l'attaque par Déni de Service Distribuée (DDOS) est l'une des attaques de sécurité les plus répondues. Lors d'une attaque DDoS, un grand nombre d'appareils compromis (généralement des ordinateurs et d'autres appareils en réseau) sont utilisés pour inonder de trafic un réseau ciblé, le rendant incapable de répondre aux demandes d'utilisateurs légitimes. Cette dernière contient plusieurs types d'attaques parmi-elles :

- **UDP flood :** Est une attaque dans laquelle l'attaquant envoie un grand nombre de paquets User Datagram Protocol (UDP) vers un serveur ou un réseau cible. Contrairement au protocole TCP, UDP est un protocole sans connexion, ce qui signifie qu'il n'y a pas de processus de poignée de main entre le client et le serveur pour établir une connexion avant l'envoi des données.

- **ICMP/PING flood** : L'attaquant submerge le réseau cible avec une énorme quantité de paquets Internet Control Message Protocol (ICMP) ou de requêtes ping consommant sa bande passante et ses ressources et le rendant incapable de répondre aux demandes légitimes. Les attaques ICMP/PING peuvent être lancées à partir de plusieurs sources, ce qui les rend difficile à bloquer ou à filtrer.

- **SYN flood** : L'attaque DDoS par SYN flood exploite une vulnérabilité connue dans le processus de connexion TCP à travers une séquence de trois étapes. Cette séquence nécessite une demande SYN pour établir une connexion avec un hôte, suivie de réponses SYN-ACK de l'hôte, et enfin une réponse ACK de la part du demandeur. Dans une attaque SYN flood, le demandeur envoie de multiples demandes SYN, mais ne répond pas aux réponses SYN-ACK de l'hôte, ou utilise des adresses IP falsifiées pour envoyer les demandes SYN. Le système hôte continue alors d'attendre une confirmation pour chaque demande, ce qui consomme des ressources jusqu'à ce qu'aucune nouvelle connexion ne soit possible, entraînant une interruption de service [67].

- **Hello flood** : Une attaque "Hello Flood" est une attaque DDoS qui consiste à inonder un serveur ou un dispositif réseau avec un grand nombre de messages "hello". Ces messages peuvent être envoyés à partir de nombreux ordinateurs ou dispositifs infectés, ce qui rend difficile la détection de la source de l'attaque. Cette attaque peut surcharger les ressources du système cible et causer un déni de service. Les attaques Hello Flood sont particulièrement dangereuses pour les réseaux de capteurs sans fil, où les nœuds

sont souvent équipés de ressources limitées en termes d'énergie, de capacité de traitement et de mémoire.

- **Scripts malicieux** : L'attaquant peut injecter des scripts malveillants dans une page web de l'application IoT, dans le but de voler des données sensibles et de nuire aux capacités de l'appareil IoT [61].

4. Attaque hello flood

4.1 Description de l'attaque hello flood

L'attaque Hello flooding est un type d'attaque qui cible les protocoles de routage dans les réseaux de capteurs sans fil [68]. Elle se produit lorsqu'un adversaire, qui n'est pas un nœud légal du réseau (nœud malveillant) inonde de messages « hello » n'importe quel nœud légitime du réseau, forçant ces derniers à le choisir comme parent, et gaspillant leurs énergies ce qui entraine ainsi une panne du réseau [69].

4.2 Mécanisme de l'attaque hello flood

Au cours de cette attaque, l'assaillant s'empare d'un nœud et diffuse des messages « hello » afin de tromper les nœuds légitimes en leur faisant croire que les messages proviennent de leurs voisins. Lorsque les nœuds du réseau reçoivent ces messages, ils supposent que l'émetteur est à portée de communication, ils réagissent en établissant une liste de voisinage et en ajoutant le nœud malveillant comme voisin dans leurs tables de routage. Ces derniers envoient leurs données, pensant qu'il s'agit de la station de base. De cette manière, l'attaquant peut sans difficulté prendre le contrôle du réseau, et collecter des données confidentielles, la station de base quant à elle se retrouve complètement déconnectée du réseau [69].

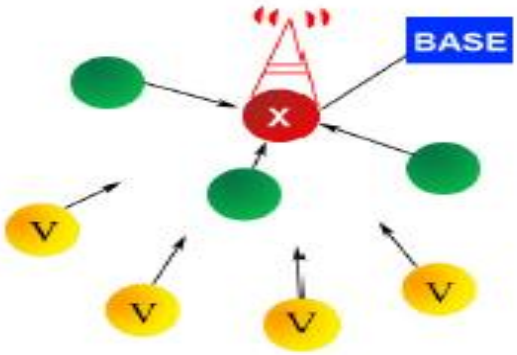


Figure II.2 *- Attaque hello flood*

4.3 Solutions préventives contre l'attaque hello flood dans l'IoT

Ci-dessous quelques mesures à prendre pour prévenir cette attaque et protéger les dispositifs IoT :

- Mettre à jour les dispositifs IoT : en installant les dernières mises à jour du firmware ou des logiciels. Afin de s'assurer que les dispositifs IoT sont à jour.
- Utilisation des adresses IP statiques : en configurant les dispositifs IoT avec des adresses IP statiques plutôt qu'avec des adresses IP dynamiques pour aider à réduire la visibilité des dispositifs sur le réseau et rendre plus difficile leur ciblage lors d'une attaque.
- Utilisation des protocoles sécurisés : en optant pour des protocoles de communication sécurisés tels que HTTPS ou MQTT sécurisé (MQTT over TLS) pour chiffrer les échanges de données entre les dispositifs IoT et les serveurs ou les applications avec lesquels ils communiquent.
- Segmentation physique du réseau : en plaçant les dispositifs IoT sur un réseau physique séparé qui n'est pas directement accessible depuis le reste de l'infrastructure. Cela contribuera à limiter l'impact de l'attaque et à réduire la surface d'attaque potentielle.

5. Conclusion

En conclusion, le monitoring et la sécurité sont deux aspects essentiels de l'IoT pour garantir la fiabilité et la confidentialité des données transmises. Le monitoring permet de surveiller l'état des dispositifs connectés et de détecter les éventuelles anomalies ou pannes. Il permet également de collecter et d'analyser les données pour améliorer la performance et l'efficacité des systèmes IoT.

Quant à la sécurité, elle est primordiale pour protéger les dispositifs, les réseaux et les données contre les cyberattaques. Les risques de sécurité dans l'IoT sont nombreux, notamment en raison de la complexité des systèmes et des vulnérabilités des dispositifs connectés. Il est donc crucial de mettre en place des mesures de sécurité adéquates, telles que l'authentification, le chiffrement des données, la gestion des clés et la détection des attaques.

En somme, le monitoring et la sécurité sont des éléments clés pour garantir le bon fonctionnement et la protection des systèmes IoT. Les utilisateurs doivent être conscients de ces enjeux et prendre les mesures nécessaires pour assurer la fiabilité, la confidentialité et la sécurité des données transmises et des dispositifs connectés.

Dans le prochain chapitre nous allons mettre en pratique les notions mentionnés précédemment et détaillé notre scénario et notre simulation.

III *Chapitre : Simulation du scénario*

1. Introduction

Dans ce chapitre, nous examinerons le scénario de maison intelligente qui simule des situations réelles, permettant ainsi d'évaluer les performances et les interactions des différents composants du système. Nous explorerons également le scénario d'attaque Hello Flood, qui vise à perturber les communications réseau en inondant les appareils cibles avec un grand nombre de messages Hello.

La simulation NetLogo sera utilisée comme outil pour modéliser ce scénario de maison intelligente et d'attaque Hello Flood. NetLogo est un langage de modélisation et de simulation multi-agents, qui permet de représenter des systèmes complexes et d'étudier leur comportement à travers des simulations interactives.

En utilisant NetLogo, nous serons en mesure de créer un modèle de maison intelligente virtuelle, d'explorer différentes configurations et d'analyser l'impact des interactions entre les différents dispositifs et systèmes. Nous pourrons également simuler l'attaque Hello Flood et évaluer son impact sur la communication au sein de la maison intelligente.

Ce chapitre offre une perspective approfondie sur le scénario de la maison intelligente ainsi que celui de l'attaque hello flood, et l'utilisation de la simulation NetLogo comme outil d'analyse. Pour finir nous allons proposer une mesure de prévention afin d'éviter tout danger d'épuisement de ressources.

2. Scénario Maison Intelligente

2.1 Description du scénario

En supposant que nous avons un agent Mohamed informaticien employé du port maritime qui vit dans une maison moderne doté d'un système intelligent.

Le système détecte le mouvement de Mohamed lors de son réveil et allume automatiquement la lumière de sa chambre. Lorsqu'il veut prendre son bain il se dirige vers la baignoire se trouvant dans la salle de bain cette dernière se remplit automatiquement d'eau, le radiateur s'allume et la température augmente. Pendant ce temps, le radiateur de la chambre est allumé pour chauffer la pièce pour qu'il puisse se changer sans attraper froid. Le robinet intelligent de la salle de bain fait couler l'eau dès qu'il détecte les mains d'une personne sous ce dernier. Il se dirige vers la cuisine pour prendre son café qui a déjà été préparé préalablement par la cafetière.

Mohamed quitte la maison pour aller travailler. Le système de maison intelligente verrouille automatiquement toutes les portes et les fenêtres, ferme tous les volets pour protéger la maison contre toute intrusion, active le système de sécurité (l'alarme) et éteint les lumières. En hiver les radiateurs sont ajustés pour économiser de l'énergie.

En arrivant au port le capteur de mouvement détecte sa présence et active la caméra de surveillance qui effectue une reconnaissance faciale de l'employé. Mohamed accède au port, il débute sa journée de travail celle de gérer le réseau, surveiller l'activité des employés et des navires qui consiste à charger et décharger la marchandise avec les équipements de manutentions.

En retournant à la maison Mohamed arrive devant chez lui en voiture. La caméra intelligente qui se trouve devant le garage et qui est muni d'un capteur de mouvement détecte la présence du véhicule, le garage s'ouvre automatiquement et la pièce s'allume pour laisser entrer la voiture, et il se ferme une fois qu'elle est à l'intérieur. En se dirigeant vers la porte d'entrée, cette dernière se déverrouille automatiquement si la caméra de surveillance qui se trouve à l'entrée reconnait son visage. Le système de maison intelligente détecte sa présence et allume automatiquement la lumière du salon et de chaque pièce qui détecte la présence de Mohamed. Le climatiseur et le radiateur s'activent en fonction de la température extérieure afin de maintenir une température confortable à l'intérieur de la maison.

Le réfrigérateur est équipé d'un système de contrôle de la température pour maintenir les aliments frais. Mohamed peut vérifier la température du réfrigérateur à distance via une application mobile. Le réfrigérateur est également équipé de capteurs pour détecter s'il est ouvert ou fermé. Si la porte reste ouverte pendant plus de 30 secondes, le système lui envoie une notification.

Dès que Mohamed s'assoit sur le fauteuil du salon la télévision s'allume, il peut également utiliser la télécommande pour l'éteindre et l'allumer s'il le souhaite. La maison intelligente détecte cette activité, les lumières de la pièce s'ajustent automatiquement pour crée une ambiance de détente.

Mohamed se prépare pour aller dormir. Le système de maison intelligente éteint automatiquement toutes les lumières.

2.2 Condition du scénario

- L'éclairage des pièces de la maison se fait automatiquement, en détectant la présence d'une personne dans une pièce la lumière s'allume systématiquement et s'éteint lorsqu'elle sort de celle-ci.

- Lorsque Mohamed veut prendre son bain la baignoire se remplit d'eau et le radiateur s'allume automatiquement afin de chauffer la pièce. Au même moment, le radiateur de la chambre est allumé pour chauffer la pièce pour qu'il puisse se changer sans attraper froid.

- Si Mohamed rentre dans la cuisine et demande son café à haute voix la cafetière lui prépare son café automatiquement.

- Lorsque Mohamed se trouve devant certains objets de la maison tel que le robinet, la baignoire, les portes etc… ces derniers détectent sa présence. L'eau de la baignoire et du robinet se mettent à couler, les portes s'ouvrent automatiquement et se referment dès que Mohamed rentre ou sort d'une pièce.

- Lorsque Mohamed quitte la maison. Le système de maison intelligente verrouille automatiquement toutes les portes et les fenêtres, active le système de sécurité (l'alarme) et éteint les lumières.

- Si Mohamed veut rentrer chez lui ou au niveau du port, la caméra de surveillance se trouvant à l'entrée effectue une reconnaissance faciale si la personne est bien Mohamed, la porte d'entrée se déverrouille pour le laisser entrer.

- Les radiateurs et les climatiseurs se mettent en marche selon la température :
- Si la température est inférieure ou égale à 15 °c les radiateurs peuvent s'allumer selon la pièce choisie par Mohamed tandis que les climatiseurs restent éteints.
- Si la température est supérieure ou égale à 25 °c les climatiseurs peuvent s'allumer tandis que les radiateurs restent éteints.
- Si la température est comprise entre 16 et 27 °c les fenêtres peuvent s'ouvrirent.

- Lorsque Mohamed s'assoit sur le fauteuil du salon la télé se met en marche et la lumière du salon s'ajuste.

- Si le réfrigérateur est laissé ouvert par Mohamed ce dernier envoie une notification sur son smartphone pour le prévenir.

- Si l'alarme détecte la présence d'un intrus, elle se déclenche et informe le propriétaire.

- Si un des objets de la maison tombe ne panne (en cas d'attaque) le réfrigérateur informe le propriétaire en lui envoyant une notification.

3. Scenario d'attaque hello flood sur la maison intelligente

3.1 Description des cas d'attaque

1. Le cybercriminel découvre une vulnérabilité dans le protocole de communication Hello utilisé par les périphériques connectés d'une maison intelligente, tels que les caméras de surveillances, les thermostats intelligents, les systèmes d'alarme, etc.
2. Le cybercriminel met en place un botnet, qui est un réseau de smartphones infectés, pour lancer une attaque hello flood en envoyant un grand nombre de paquets Hello aux périphériques connectés de la maison intelligente.
3. Les périphériques connectés commencent à recevoir un flux important de paquets Hello, ce qui entraîne une saturation de la bande passante et une surcharge des périphériques.
4. En raison de la surcharge des périphériques connectés, certains peuvent cesser de fonctionner ou afficher des erreurs, ce qui peut compromettre la sécurité et le confort du propriétaire.
5. Par exemple, les caméras de surveillance peuvent cesser de fonctionner, les systèmes d'alarme peuvent ne plus être opérationnels, les serrures intelligentes peuvent ne plus répondre, les thermostats intelligents peuvent ne plus fonctionner correctement, etc.

6. Attaque sur une porte intelligente : Une attaque "Hello flood" ciblant une porte intelligente pourrait la saturer de requêtes et la rendre inutilisable. Cela pourrait empêcher les occupants de la maison d'entrer ou de sortir, compromettant leur sécurité et leur confort.
7. Attaque sur des fenêtres intelligentes : Des fenêtres intelligentes peuvent être équipées de capteurs de température, d'humidité et de luminosité qui peuvent être contrôlés à distance. Une attaque "Hello flood" ciblant ces capteurs pourrait surcharger le système, ce qui empêcherait les occupants de surveiller les conditions environnementales à l'intérieur de la maison.
8. Attaque sur une caméra de surveillance intelligente : Une caméra de surveillance intelligente peut être ciblée par une attaque "Hello flood", ce qui la saturerait de requêtes et la rendrait inutilisable. Cela pourrait laisser la maison vulnérable aux intrus, car il n'y aurait pas de moyen de surveiller les activités autour de la maison.
9. Attaque sur une alarme de sécurité intelligente : Une alarme de sécurité intelligente peut être ciblée par une attaque "Hello flood", ce qui empêcherait les occupants de la maison d'être alertés en cas d'intrusion ou d'incendie. Cela pourrait compromettre la sécurité de la maison et la sécurité des occupants.

Le propriétaire de la maison intelligente peut ne plus être en mesure de surveiller sa propriété ou de contrôler les périphériques connectés, ce qui peut créer un sentiment d'insécurité et de vulnérabilité.

3.2 Description du scénario de l'attaque hello flood

L'attaquant repère la caméra de surveillance et commence l'attaque en envoyant des paquets hello flood afin de surcharger cette dernière et la mettre en panne. Cette pane entraine la non reconnaissance des voitures et personnes devant la maison ce qui laisse les portes et le garage qui lui sont reliés verrouillés. Pour être en mesure d'accéder à la maison, il attaque la porte d'entrée et la déverrouille.

A l'intérieur de la maison l'attaquant tentera de nuire au maximum d'objets.

Dès qu'il franchit la porte d'entrée il la verrouille pour que Mohamed ne puisse pas accéder à son domicile, l'alarme s'active et envoie une alerte pour prévenir le propriétaire qu'un intrus s'est introduit chez lui. En entrant dans le salon il découvre les objets se trouvant dans sa portée (tel que le radiateur du salon et de la cuisine, climatiseur du salon, fenêtre du salon et de la cuisine ainsi que l'alarme) et commence à saturer ces derniers avec des paquets hello flood, et les rend inutilisables afin de nuire au propriétaire.

Une fois arrivé dans la chambre il s'attaque aux objets se trouvant à l'intérieur (Radiateur, climatiseur, ordinateur, fenêtre) ainsi que ceux se trouvant dans la salle de bain (Radiateur et fenêtre) en envoyant des requêtes hello, ce qui entraine leur incapacité à fonctionner. L'attaquant s'empare du coffre qui est la raison principale de son attaque. Entre temps Mohamed et les forces de l'ordres arrivent devant la propriété pour l'arrêter.

3.2.1 Solution proposée

Nous avons constaté que le réfrigérateur est l'un des objets les moins susceptibles d'être attaqués dans une maison intelligente. C'est la raison pour laquelle nous l'avons choisi comme outil potentiel pour informer le propriétaire en cas d'attaque hello flood.

Le réfrigérateur intelligent est équipé de capteur de température qui peut être utilisé pour détecter les changements de température à l'intérieur et l'extérieur du réfrigérateur. Ce capteur peut être utilisé pour détecter le changement de température suspecte dans la maison.

L'attaque hello flood sur les radiateurs et climatiseurs entraine la chute ou l'augmentation soudaine des températures à l'intérieur, cela peut affecter la température à l'intérieur du réfrigérateur. Le réfrigérateur peut détecter ce changement et envoyer une alerte à Mohamed pour l'informer de cette situation suspecte.

3.3 Solution proposée pour d'autres attaques

En ce qui concerne les autres attaques, il existe plusieurs solutions de prévention tel que le monitoring qui implique l'utilisation d'outils pour collecter, surveiller et analyser les données afin de détecter les activités suspectes. Cette solution vise à minimiser le risque d'attaques et protéger efficacement les périphériques connectés. Dans notre cas nous avons opté pour l'utilisation d'un pare-feu pour les raisons suivantes :

- Le pare-feu permet de filtrer et bloquer les paquets malveillants entrants et les connexions non autorisées en utilisant des règles de filtrage.

- Le monitoring du pare-feu permet de surveiller les activités des paquets malveillants entrants sur le réseau afin de détecter rapidement les flux anormaux de trafic.

- Le pare-feu est souvent équipé de bases de données de signatures d'attaques connues ce qui permet de se protéger contre des attaques dont les schémas et les techniques sont déjà connus et répertoriés.

4. Simulation

La simulation est une méthode numérique pour résoudre un problème en imitant la réalité. C'est une approche essentiellement pratique qui permet de modéliser aussi bien des systèmes conceptuels que des systèmes déjà existants. Nous pouvons la percevoir comme étant la conduite d'une expérimentation indirecte dans le but de comparer plusieurs façons de procéder [70].

Nous pouvons retenir la définition donnée par **Drogoul** [71] formulé comme suit : " On nomme simulation la démarche scientifique qui consiste à réaliser une reproduction artificielle, appelée modèle, d'un phénomène réel que l'on désire étudier, à observer le comportement de cette reproduction lorsqu'on en fait varier certains paramètres, et à induire ce qui se passerait dans la réalité sous l'influence de variations analogues".

La simulation peut être identifiée par les mots clés suivants :

- Observer un système réel pour extraire les propriétés qui vont permettre d'élaborer un modèle.
- Le modèle qui est un ensemble de règles, d'équations, de variables et de paramètres qui décrivent le fonctionnement du système, ainsi que les interactions entre ses différentes composantes.
- Exécution du modèle sur ordinateur.
- Le modèle est manipulé pour tester des hypothèses, évaluer des stratégies et aider à la prise de décision en fournissant une compréhension plus approfondie du système étudié.
- Les solutions obtenues sont celles du modèle et non du système modélisé.
- Son but est d'analyser les résultats afin de choisir parmi plusieurs solutions celle qui semble être la plus pertinente.

4.1 Simulation base multi-agents

La simulation multi-agents, en anglais Multi-Agent Based Simulation (MABS) se base sur le concept de systèmes conçu autour des agents pour concevoir, spécifier et exécuter la simulation.

Elle permet de représenter la complexité d'un phénomène en simulant le comportement de divers agents autonomes interagissant entre eux dans un environnement donné. Chaque un d'entre eux est programmé pour agir selon des règles déterminées. Ils évoluent simultanément au fil du temps pour réaliser une ou plusieurs tâches et ont une vision locale de l'environnement via leurs capteurs.

Pour implémenter une simulation multi-agents, il est essentiel de dérouler des modèles suivants :

- Le modèle de l'espace (l'environnement) pour la description de l'environnement.
- Le modèle de temps pour décrire l'évolution de la simulation au cours du temps.
- Le modèle de l'interaction agent/environnement qui décrit la dynamique du système (comportements des agents) contrôlé [72].

4.2 Système de systèmes (SoS)

Un système de systèmes (SoS) est un groupe de systèmes distincts et indépendants qui sont reliés ou intégrés pour créer un système plus grand et plus complet. En d'autres termes, il s'agit d'un réseau de systèmes interconnectés qui coopèrent pour atteindre un objectif commun.

Un système de systèmes se distingue par son comportement émergent, dans lequel le comportement et les capacités combinés des systèmes interconnectés dépassent ceux des systèmes composants. Les systèmes individuels qui composent un système de systèmes conservent leur indépendance et accomplissent des tâches uniques, mais ils dépendent également des interactions et des interdépendances avec d'autres systèmes pour atteindre des objectifs plus généraux [73].

4.3 Relation entre IoT, SMA et SoS :

L'Internet of Things, les SoS et les SMA, peuvent être interconnectés pour créer des systèmes plus vastes et plus adaptatifs. Dans un SoS basé sur l'IoT, les objets connectés peuvent agir en tant qu'agents dans un système multi-agent. Les objets connectés peuvent interagir et coopérer

pour coordonner les activités des systèmes individuels et atteindre les objectifs communs du SoS.

4.4 Choix Netlogo

Le choix de l'utilisation du simulateur NetLogo a été motivé par plusieurs raisons.

Tout d'abord, NetLogo est un logiciel open-source et gratuit, ce qui le rend accessible à un large public et permet une communauté active de développeurs et d'utilisateurs.

De plus, NetLogo est spécifiquement conçu pour les simulations basées sur des agents, ce qui facilite la modélisation de phénomènes complexes impliquant des interactions entre des entités simples.

NetLogo dispose également d'une bibliothèque d'agents préprogrammés qui peuvent être utilisés pour créer des modèles de manière rapide et efficace. Ces agents comprennent des tortues, qui peuvent être utilisées pour représenter des individus ou des entités dans un modèle, et des patchs, qui peuvent être utilisés pour représenter des emplacements spatiaux dans un modèle.

En outre, NetLogo offre une grande flexibilité en termes de programmation, de modélisation et de simulation. Permettant de créer des modèles sur mesure et de personnaliser notre expérience de simulation. Le logiciel prend en charge une grande variété de techniques de modélisation, telles que les graphes, les réseaux et les systèmes multi-agent.

Enfin, NetLogo possède une interface graphique conviviale qui facilite l'exploration des modèles et l'analyse des résultats.

Figure III.1 *- Logo de NetLogo.*

4.5 Présentation Netlogo

NetLogo est un langage de programmation et un environnement de modélisation pour la simulation de systèmes complexes. Il a été créé par Uri Wilensky en 1999 à l'Université Northwestern et son développement est poursuivi de manière continue par le Center for Connected Learning and Computer-Based Modeling, il a pour ancêtre StarLogoT [74].

NetLogo permet de modéliser des systèmes complexes en utilisant des agents individuels et leur interaction avec l'environnement. Les agents peuvent être des animaux, des personnes, des voitures, des plantes, des molécules ou tout autre objet que l'on souhaite modéliser. Les interactions entre les agents et l'environnement peuvent être définies en utilisant des règles de

comportement simples, ce qui permet de simuler des comportements émergents et des phénomènes complexes.

NetLogo offre une interface graphique conviviale qui permet aux utilisateurs de créer des modèles de simulation en utilisant des "primitives". Les utilisateurs peuvent également écrire leur propre code en utilisant le langage de programmation NetLogo.

NetLogo dispose également d'une bibliothèque de modèles prédéfinis qui peuvent être utilisés comme point de départ pour votre propre projet. Ces modèles incluent des simulations de la dynamique des populations, de l'évolution, de l'économie, de la physique et bien d'autres domaines.

Figure III.2 *- Lancement du simulateur NetLogo*

4.5.1 Concept d'agent dans NetLogo

Netlogo est constitué d'un ensemble d'agents qui peuvent suivre des instructions. Les activités des différents agents s'exécutent simultanément. Il existe 4 types d'agents dans Netlogo :

- **Tortue (Turtle)** : les tortues sont des agents qui peuvent se déplacer dans l'environnement. L'environnement est en deux ou trois dimensions (2D ou 3D) et est divisé en une grille de patchs.

➢ Variables de turtles : Comme pour les patches, l'état des turtles est décrit par l'intermédiaire d'un certain nombre de variables prédéfinies auxquelles nous pouvons ajouter un nombre arbitraire de nouvelles variables. Les turtles partagent avec les patches certaines variables comme la couleur de la turtle (color) ainsi que ses coordonnées sur la grille de patches (xcor et ycor). Comme pour les patches, nous pouvons définir un label ainsi qu'une couleur de label (label et label-color). La variable size permet de modifier la taille de la turtle et who renvoie l'identifiant id de la turtle.

➢ Primitives de turtles : Les turtles peuvent être manipulées à l'aide de primitives définies dans Netlogo. Là encore nous pouvons citer quelques-unes de ces primitives parmi les plus utilisées :
– distance : renvoie la distance entre la turtle appelante et la turtle passée en paramètre.
– die : fait mourir la turtle.
– hatch : crée un nombre spécifié de turtles filles de la turtle courante. Les enfants sont créés identiques et au même endroit que la mère.
– forward : la turtle avance d'un certain nombre de pas.
– move-to : la turtle se déplace à l'endroit de l'agent passé en paramètre.
– left, right : permet à la turtle d'opérer une rotation à droite ou à gauche selon un angle donné.
– -here : retourne un ensemble d'agents contenant les turtles se trouvant sur le patch de l'agent appelant.

- **Cellule (Patch)** : une cellule est un agent qui ne peut pas se déplacer, représentant un carré du sol sur lequel les tortues peuvent se situer et se déplacer. L'ensemble des cellules (la grille) forme l'environnement.

➢ Primitives de patches : Les patches peuvent être manipulés à l'aide de primitives définies dans Netlogo. Nous pouvons citer quelques-unes de ces primitives parmi les plus utilisées :
– neighbors : permet d'accéder à ses voisins.
– distance : retourne la distance séparant l'agent appelant et un autre agent passé en paramètre.
– sprout- : créer un certain nombre d'agents de l'espèce breeds sur le patch appelant.
– diffuse : cette commande est un peu particulière car c'est une primitive de l'observer. Elle permet aux patches de diffuser entre autres une de leurs variables à leurs voisins.

- **Lien (Link)** : c'est l'agent qui permet de connecter deux tortues. Les liens n'ont pas de coordonnées. Chaque lien a deux extrémités et chaque extrémité est une tortue. Si l'une des tortues meurt, le lien meurt aussi.

➢ Primitives de links : Les links peuvent être manipulés à l'aide de primitives définies dans Netlogo. Citons quelques-unes de ces primitives parmi les plus utilisées :
– create-links-to, create-links-from, create-links-with: crée un link.
– link-with : retourne le lien entre la tortue appelante et la turtle passée en paramètre.
– my-links : retourne tous les liens non orientés connectés à la turtle appelante.
– link-neighbors : renvoie un ensemble d'agents. Celui-ci contient toutes les turtles trouvées à l'autre extrémité des links connectés à la turtle appelante.
– my-in-links : retourne un ensemble d'agents. Celui-ci contient tous les links orientés venant vers la tortue appelante.
– my-out-links : retourne un ensemble d'agents. Celui-ci contient tous les links orientés partant de la tortue appelante.

- **Observateur (Observer)** : L'observateur peut être utilisé pour attribuer des ordres spécifiques à des patches ou à des tortues. Il collecte également des données pour créer des graphiques.

4.5.2 Procédures et fonctions

- **Les procédures** (commands) : Les procédures sont des fonctions spécialisées qui regroupent certaines instructions qu'on est amenées à exécuter plusieurs fois et qu'on utilise pour modifier les variables globales et/ou les variables qu'on passe en argument.

Déclaration :
to < nom_procédure > [<parametre1> <parametre2> . . .]
<Instructions>
End
Appel : <nom_procédure> <argument1> <argument2>

- **Les fonctions** (reporter) : Ce sont des méthodes qui retournent une valeur précise à la fin de leurs opérations. Valeur à stocker dans une variable ou à utiliser dans un calcul.

  Déclaration :
  To-report <nom_fonction> [<parametre1> <parametre2> . . .]
  <Instructions>
  Report <valeur>
  End
  Appel : <nom_fonction> <argument1> <argument2>

4.5.3 Définition des agents

- **Agent personne :** C'est l'agent protagoniste de notre simulation, notre maison intelligente fonctionne selon son activité.

```
Procédure_go
  Début
  Si personnage = Mohamed ou Attaquant
    Si bouton = gauche ou droite ou haut ou bas
        La personne se déplace selon la direction choisie.
    FinSi.
  FinSi.
  Si personnage = Mohamed
    Si il se trouve devant une porte
       La porte s'ouvre et se ferme automatiquement.
    FinSi.
    Si sa position est devant le frigo ou l'armoire ou le lavabo ou le coffre ou devant la
          voiture.
              Il interagit avec eux.
    FinSi.
    Si il demande son café et sa position est devant la table de la cuisine
        Son café sera préparé.
    FinSi.
  FinSi.
  Si personnage = attaquant
    Si l'attaque est effectuée et que sa position est devant une porte
       La porte s'ouvre et se ferme automatiquement.
    FinSi.
    Si il se positionne devant le coffre
      Il vole le coffre.
    FinSi.
  FinSi.
Fin.
```

La procédure go est un déroulement de toutes les procédures mentionnées plus bas. Mis-à-part la procédure attack. L'appel de ces procédures se fait par rapport au positionnement de chaque personnage.

```
Procédure_move
  Début
    Si déplacement = Maison
        La personne se retrouve dans l'environnement maison.
      Déplacement = S'assoir sur fauteuil
        La personne se retrouve dans le salon, s'assoit sur le fauteuil et la télévision s'allume.
      Déplacement = Rentrer dans la chambre
        La personne entre dans la chambre et la lumière s'allume automatiquement
      Déplacement = Vers le hall
         La personne entre dans le hall et la lumière s'allume automatiquement.
      Déplacement = Devant la porte de la chambre
        La personne se retrouve devant la porte de la chambre, la lumière s'allume et la porte
                                    s'ouvre automatiquement.
      Déplacement = Rentrer dans la salle de bain
        La personne entre dans la salle de bain et la lumière s'allume automatiquement.
      Déplacement = Devant la porte d'entrée
       La personne se retrouve devant la porte d'entrée, la caméra s'active et la porte s'ouvre
                                    automatiquement.
      Déplacement = Prendre un bain
         La personne prend son bain le radiateur de la salle de bain et du salon sont allumées
                                    pour chauffer les deux pièces.
    FinSi.
    Si déplacement = port
      Déplacement = devant le portail du port
          Mohamed se retrouve devant le portail du port.
    FinSi.
  Fin.
```

```
Procédure_lumiére
  Début
    Si Pièce = Salon ou Cuisine ou Hall ou Chambre ou Salle de bain ou Garage
        La lumière de la pièce s'allume automatiquement.
    FinSi.
  Fin.
```

```
Procédure_eteindre
Début
  Si Pièce = Salon ou Cuisine ou Hall ou Chambre ou Salle de bain ou Garage
    La lumière de la pièce s'éteint automatiquement.
  FinSi.
Fin.
```

- **Agent radiateurs :** Les radiateurs s'allument selon la température.

```
Procédure_chauffer
Début
  Si température <= 15 alors
    Si choix = Salon
        Le radiateur du salon s'allume automatiquement.
      Choix = Cuisine
        Le radiateur de la cuisine s'allume automatiquement.
      Choix = Chambre
        Le radiateur de la chambre s'allume automatiquement.
      Choix = Salle de bain
        Le radiateur du salon s'allume automatiquement.
    FinSi.
  Sinon les radiateurs ne s'allument pas.
  FinSi.
Fin.
```

- **Agent climatiseurs :** Les climatiseurs s'allument selon la température.

```
Procédure_clim
Début
  Si température > = 25 alors
     Les climatiseurs du salon et de la chambre s'allument.
  Sinon les climatiseurs ne s'allument pas.
  FinSi.
Fin.
```

- **Agent garage :** Le garage détecte la présence du véhicule du propriétaire grâce à la caméra de surveillance et s'ouvre automatiquement.
- **Agent voiture :** permet de se déplacer, de conduire Mohamed à son lieu de travail ou à la maison et de la garer.

```
Procédure_stationner/conduire
Début
  Si temps = 'nuit' et mohamed est dans l'environnement maison
       La voiture se déplace en se dirigeant vers le garage, lorsqu'elle se retrouve devant le
       garage la caméra détecte la présence de la voiture de Mohamed, la porte du garage s'ouvre
       pour qu'il puisse garer sa voiture et se referme dès qu'elle se retrouve à l'intérieur.
  FinSi.
  Si Mohamed est dans l'environnement maison et temps = 'jour'
    Mohamed se deplace vers le port.
  FinSi.
  Si Mohamed est dans l'environnement port
    Mohamed se déplace vers la maison.
  FinSi.
Fin.
```

- **Agent fenêtres :** Les fenêtres s'ouvrent selon la température.

```
Procédure_openwindow
Début
  Si température >= 16 et température <= 27
    Si choix = Salon
         La fenêtre du salon s'ouvre.
    Choix = Cuisine
         La fenêtre de la cuisine s'ouvre.
    Choix = Chambre
         La fenêtre de la chambre s'ouvre.
    Choix = Salle de bain
         La fenêtre de la salle de bain s'ouvre.
    FinSi.
  Sinon les fenêtres ne s'ouvrent pas.
  FinSi.
Fin.
```

```
Procédure_closewindow
Début
  Si la fenêtre d'une des pièces est ouverte alors
    Si choix = Salon
         La fenêtre du salon se ferme.
    Choix = Cuisine
         La fenêtre de la cuisine se ferme.
    Choix = Chambre
         La fenêtre de la chambre se ferme.
```

```
        Choix = Salle de bain
            La fenêtre de la salle de bain se ferme.
        FinSi.
    Sinon les fenêtres restent fermées.
    FinSi.
Fin.
```

- **Agent camera :** La caméra détecte la présence des personnes et voitures au niveau de l'entrée de la maison.

```
Procédure_sécurité
Début
La caméra effectue une reconnaissance faciale de la personne et vérifie la présence de la voiture
                                devant l'entrée.
    Si la caméra détecte Mohamed ou sa voiture alors
        La porte se déverrouille pour le laisser entrer ou le garage s'ouvre pour garer sa voiture.
    Sinon la porte ne se déverrouille pas et le garage ne s'ouvre pas.
    FinSi.
Fin.
```

- **Agent alarme :** Si un intru essaye de s'introduire dans la maison ou dans le bureau du port l'alarme se déclenche.

```
Procédure_alarmer
Début
    Si déplacement = Maison
    Détection de mouvements dans la maison
        Si la personne est l'Attaquant alors
            L'alarme se déclenche.
        Sinon l'alarme ne se déclenche pas
        FinSi.
    FinSi.
    Si déplacement = Port
    Détection de mouvements dans le bureau du port
        Si la personne est l'Attaquant alors
            L'alarme se déclenche.
        Sinon l'alarme ne se déclenche pas
        FinSi.
    FinSi.
Fin.
```

- **Agent équipement de manutention** (clark, navire, camion) : permet de charger et décharger la cargaison et d'accoster.

```
Procédure_Charger/décharger/accoster
Début
  Si équipement de manutention = clark haut ou clark milieu ou clark bas ou camion
    Ils chargent et déchargent la cargaison.
  FinSi.
  Si équipement de manutention = navire
       Il accoste.
  FinSi.
Fin.
```

```
Procédure_Attack
Début
  Si déplacement = 'maison' ou 'port'
    Si personnage = attaquant
     L'attaquant peut attaquer tous les objets se trouvant dans sa portée.
    FinSi.
  FinSi.
Fin.
```

```
Procédure_Notif
Début
  Si déplacement = 'maison '
    Les paquets (notification) s'envoient entre les deux routeurs de la maison et du port.
  Sinon aucun envoi de paquets ne se fait.
  FinSi.
Fin.
```

4.5.4 Propriétés des agents

Le tableau ci-dessous décrit les agents principaux utilisés dans notre scénario :

Logo de l'agent	Nom de l'agent	Personnalisation de l'agent dans NetLogo	Rôle
	Personne	breed [personnes personne] set shape "person" set size 2	Propriétaire de la maison et employé du port.

	Attaquant	breed [personnes personne] set shape "attaquant" set size 2	Intru dans la maison ou le port.
	Porte	breed [portes porte] set shape "porte"	Se verrouille et se déverrouille.
	Door	breed [dors dor] set shape "porteSo" set size 10	Se verrouille et se déverrouille. (Porte d')
	Voiture	breed [voitures voiture] set shape "car top" set size 5.5	Déplacer et conduire le propriétaire a son lieu de travail ou à la maison ou stationner.
	Caméra de surveillance	breed [cameras camera] set shape "camera" set size 5	Reconaissance faciale et verification de la présence des personnes et voitures.
	Radiateur	breed [radiateurs radiateur] set shape "radiateur" set size 3.5	Chauffer les pieces.
	Climatiseur	breed [climatiseurs climatiseur] set shape "clim" set size 6	Refroidire les pieces.
	Fenêtre	breed [fenetres fenetre] set shape "fenetre" set size 10	Aérer les pieces
	Alarme	breed [alarmes alarme] set shape "alarme2" set size 3	Alarmer en cas d'intrusion.

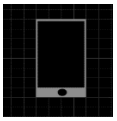
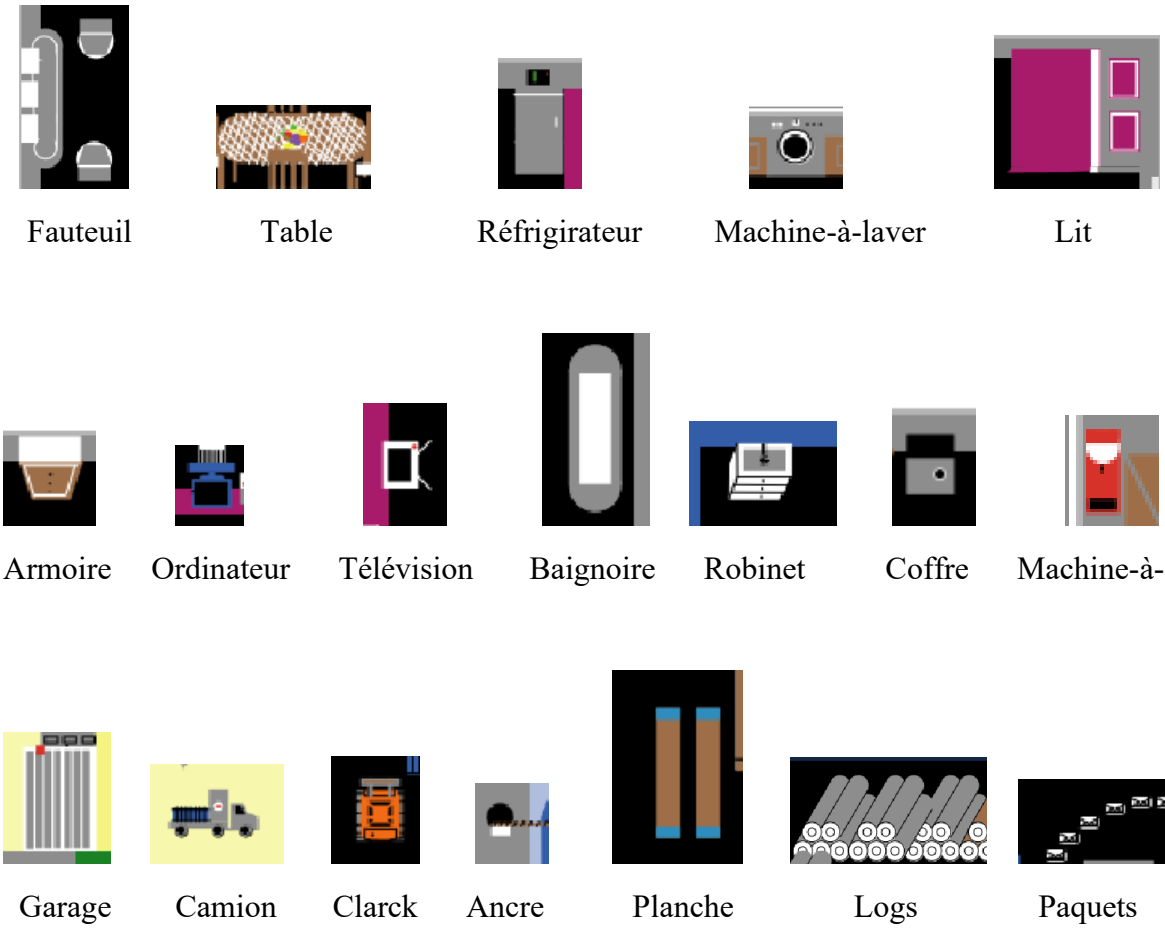
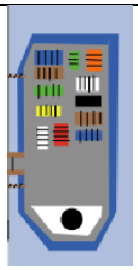
	Routeur	breed [routeurs routeur] set shape "routeur" set size 3	Fait passer les paquets
	Smartphone	breed [smartphones smartphone] set shape "phone" set size 2	Recevoire les notifications
	Capteur	breed [capteurs capteur] set shape "capteur" set size 2.5 set heading 360	Mesure les caractéristiques physiques et environnementaux

Tableau 2 *- Propriétés des agents*

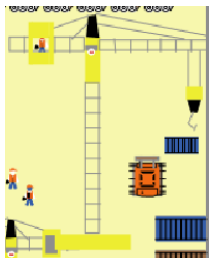
Les agents secondaires sont cités ci-dessous :





Navire

Contenaire



Grue

5. Présentation de notre simulation

5.1 Description des interfaces de notre scénario

L'interface de simulation (Figure 3) dans NetLogo est composée d'un ensemble de boutons, de curseurs, de sélecteurs, d'un moniteur et d'un panneau qui affiche le déroulement de la simulation, y compris les actions et les déplacements des agents dans leur environnement.

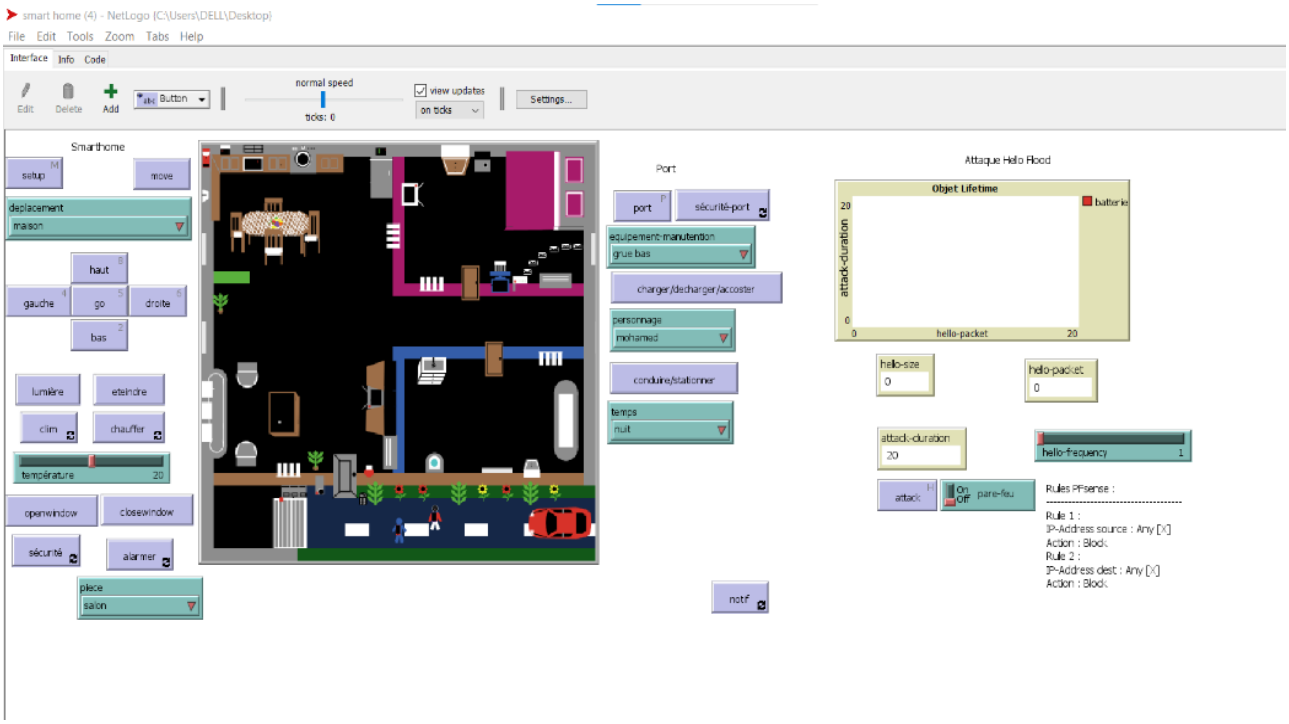


Figure III.3 *- Interface de simulation de la maison intelligente*

Notre interface est donc constituée de deux environnements :

1. Environnement maison intelligente (Figure 4)
2. Environnement port intelligent (Figure 5) : Notre stage à l'EPB (Entreprise Portuaire de Bejaïa) nous a conduit à constater l'absence d'équipements intelligents dans le port. Ce qui nous a encouragés à explorer la simulation d'un port intelligent à l'aide du simulateur NetLogo. Nous avons ainsi développé un modèle de simulation permettant d'analyser les opérations portuaires et d'évaluer différentes stratégies. Cette expérience a renforcé notre intérêt pour la gestion d'un port intelligent.

Chacun de ces environnements est constituée de boutons, choosers et sliders propres à lui.

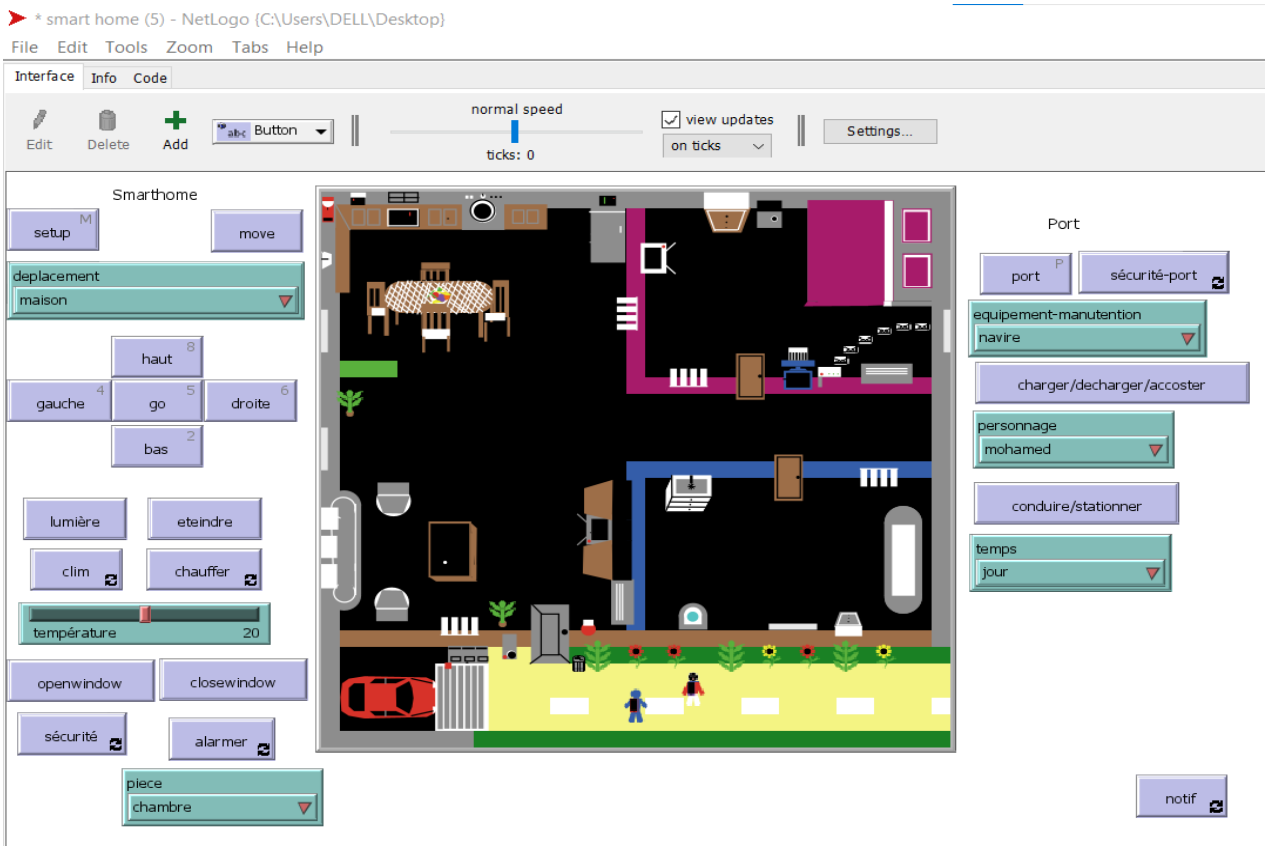


Figure III.4 *- Environnement Maison Intelligente*

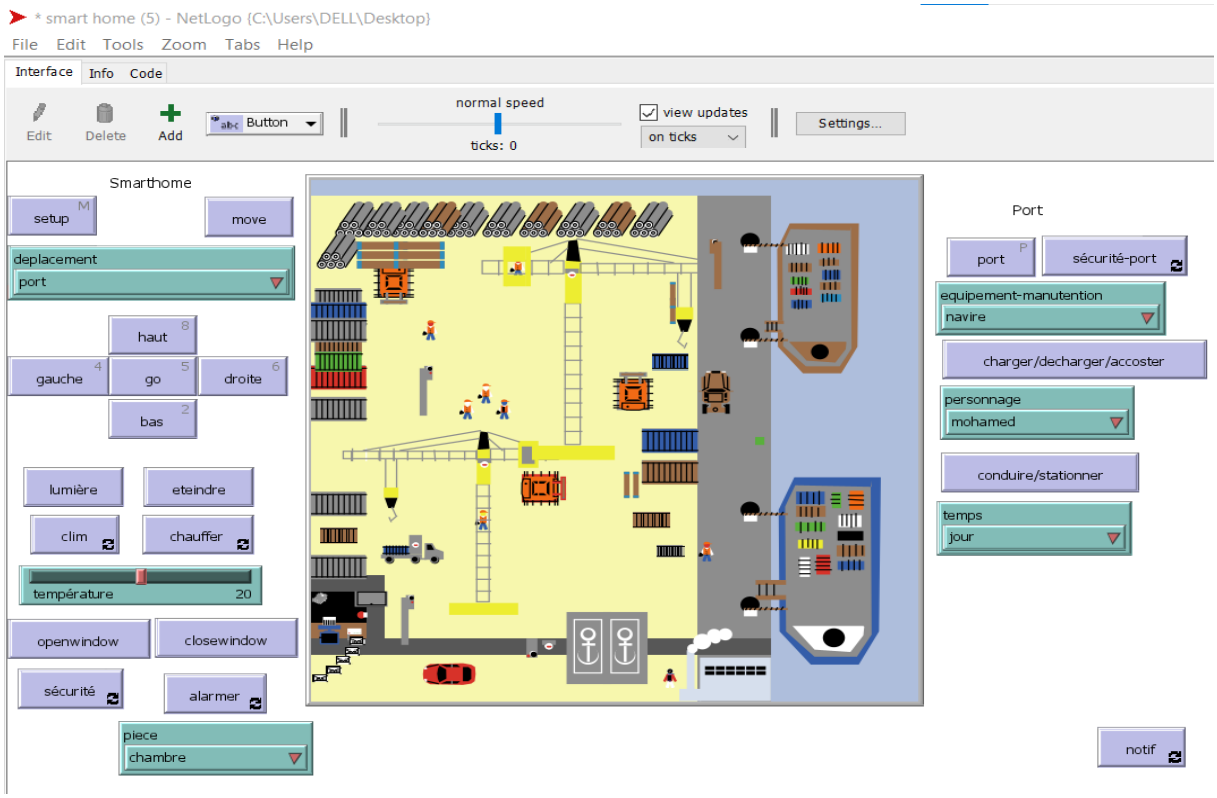


Figure III.5 *- Environnement Port Intelligent*

5.1.1 Déroulement des procédures

Dans NetLogo, un bouton est un élément d'interface graphique utilisé pour déclencher une action spécifique dans une simulation. Lorsqu'un utilisateur clique sur un bouton, il exécute une procédure ou une série d'instructions prédéfinies.

- **Setup :** c'est un bouton qui exécute la procédure **to setup**, et qui permet de créer les agents de la maison intelligente.

- **Port :** c'est un bouton qui exécute la procédure **to port**, et qui permet de créer les agents du port.

- **Move :** c'est un bouton qui exécute la procédure **to Move** qui permet de déplacer Mohamed instantanément d'une pièce à l'autre au niveau de la maison selon le déplacement choisi avec le sélecteur déplacement en déclenchant certaines procédures telles que lumière et chauffer.

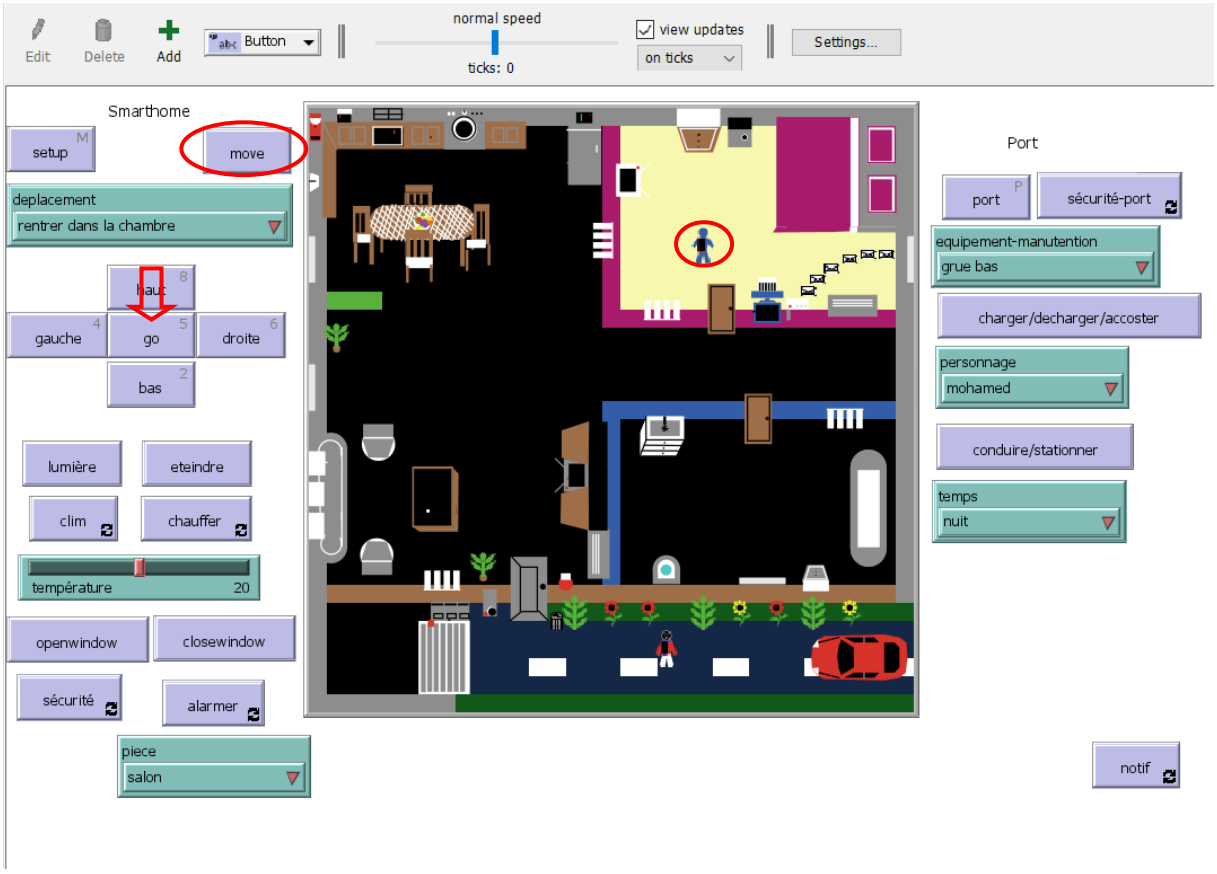


Figure III.6 *- Représentation du fonctionnement de la procédure Move*

- **Go** : c'est un bouton qui exécute la procédure **to Go** qui permet de se déplacer librement dans notre environnement. Elle déclenche également d'autres procédures telles que lumière, chauffage et clim.
- En cliquant sur haut puis go (ou sur le clavier 8 puis 5) la personne se déplace vers le haut.

- En cliquant sur bas puis go (ou sur le clavier 2 puis 5) la personne se déplace vers le bas.
- En cliquant sur gauche puis go (ou sur le clavier 4 puis 5) la personne se déplace vers la gauche.
- En cliquant sur droite puis go (ou sur le clavier 6 puis 5) la personne se déplace vers la droite.

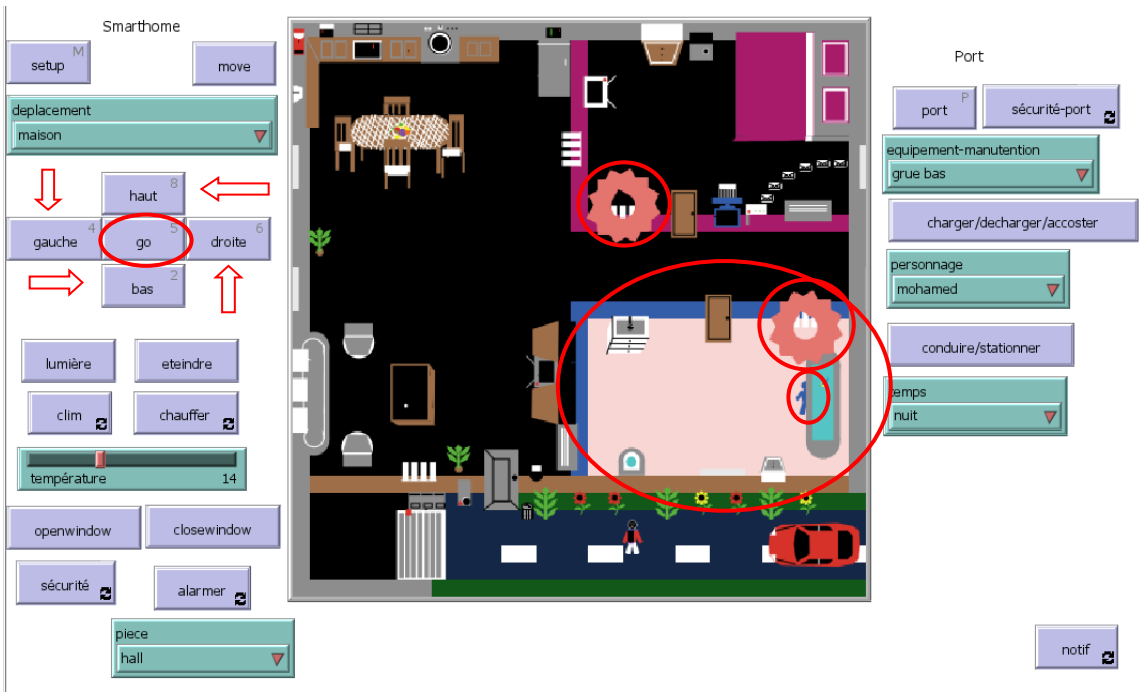


Figure III.7 *- Représentation du fonctionnement de la procédure Go*

➢ **Clim :** c'est un bouton qui exécute la procédure **to clim** qui permet d'allumer les climatiseurs, ce bouton fonctionne lorsque la température est supérieure ou égale à 25.

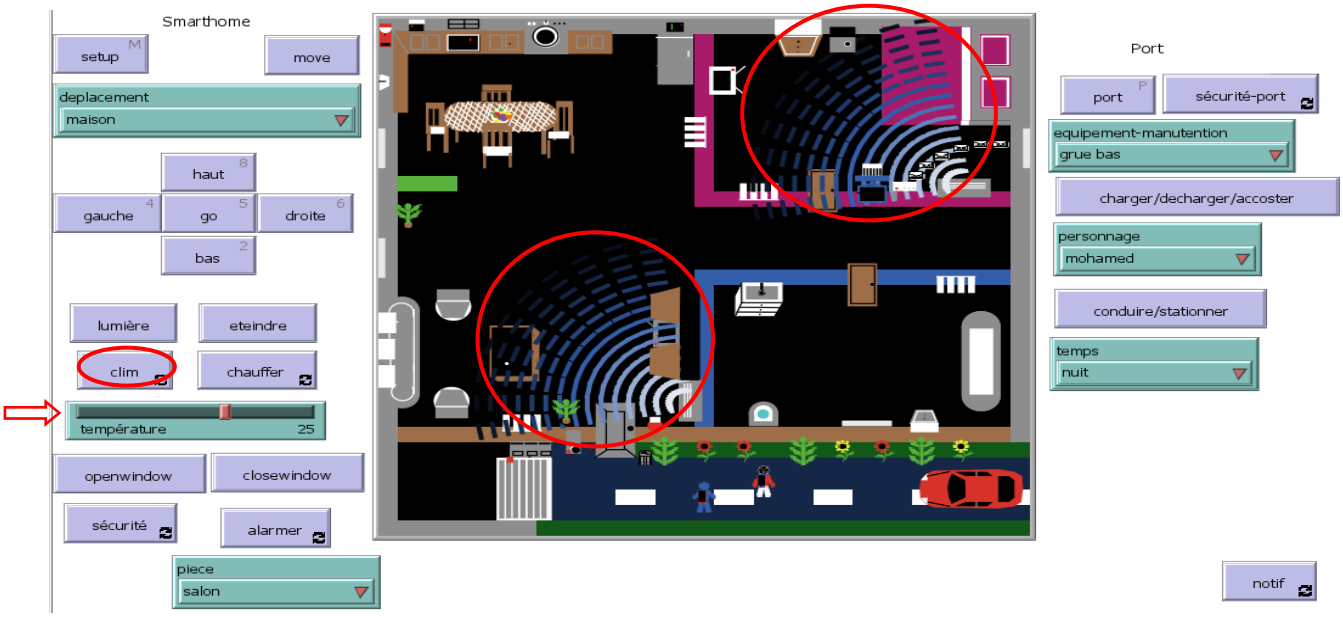


Figure III.8 *- Représentation du fonctionnement de la procédure Clim*

- **Chauffer** : c'est un bouton qui exécute la procédure **to chauffer** qui permet d'allumer les radiateurs dans une piéce choisie grâce au chooser pièce, ce bouton fonctionne si la température est inférieure ou égale à 15.

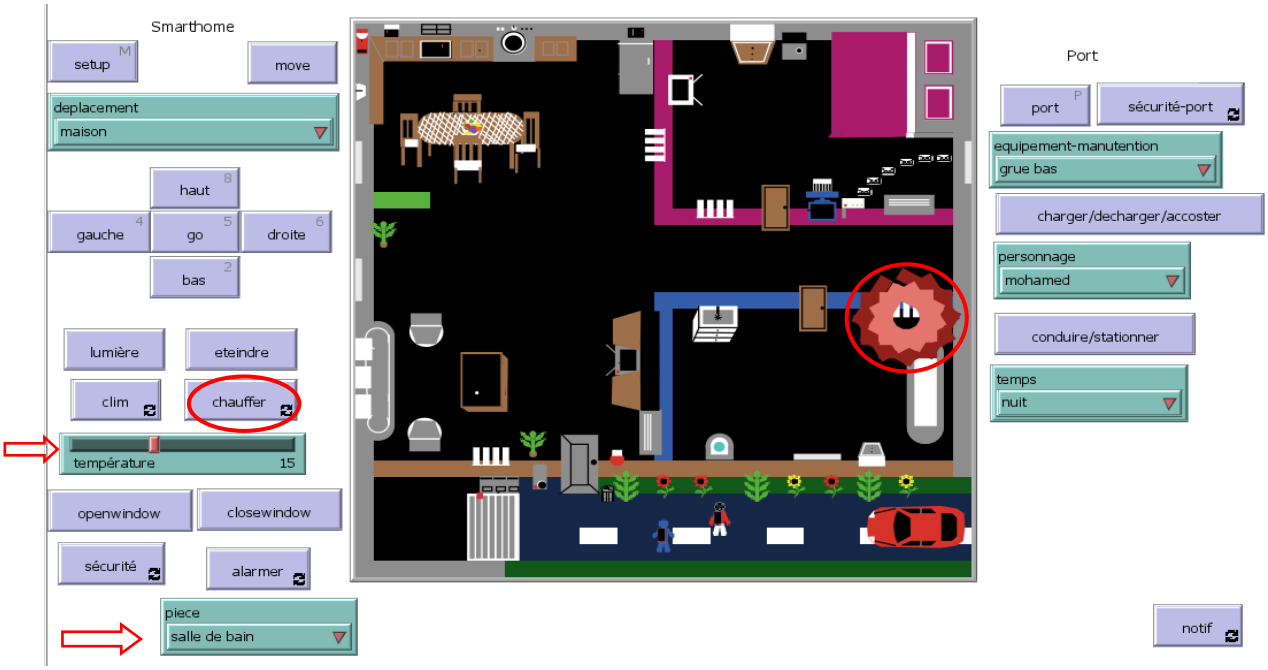


Figure III.9 *- Représentation du fonctionnement de la procédure chauffer*

- **OpenWindow :** c'est un bouton qui exécute la procédure **to OpenWindow** qui permet d'ouvrir les fenêtres dans une pièce choisie, lorsque la température est comprise entre 16 et 27.

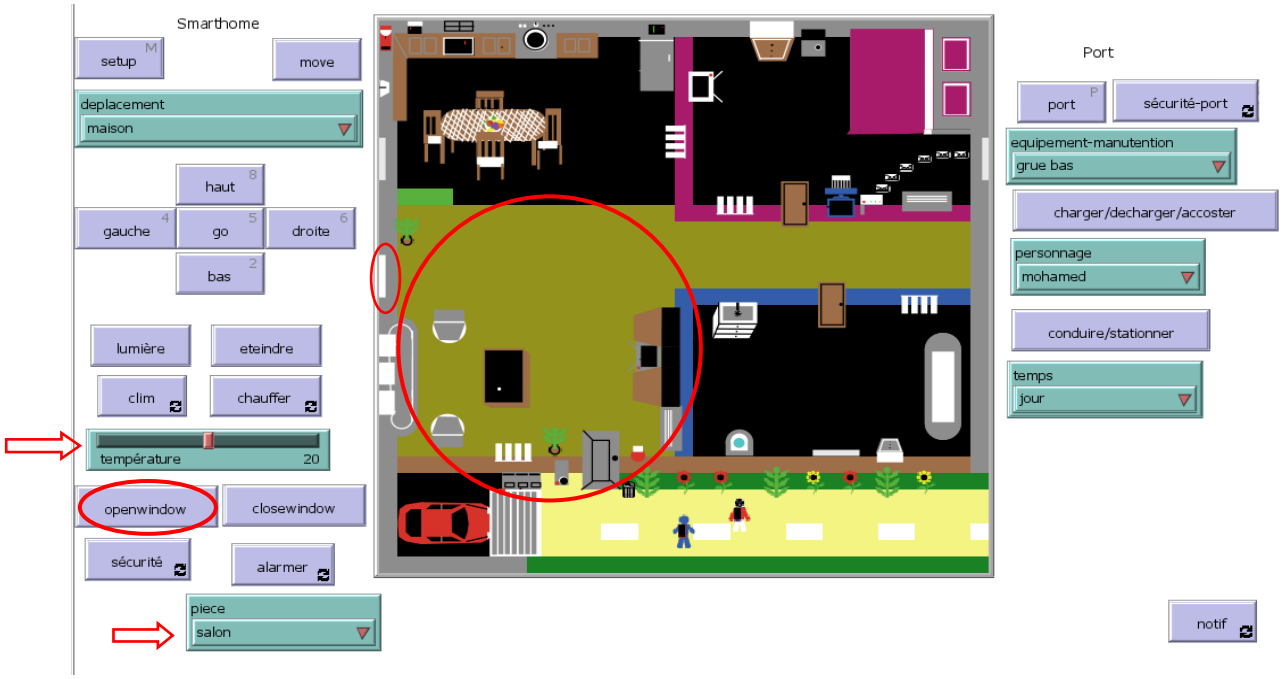


Figure III.10 *- Représentation du fonctionnement de la procédure Openwindow*

- **CloseWindow :** c'est un bouton qui exécute la procédure **to Closewindow** qui permet de fermer les fenêtres dans une pièce choisie.

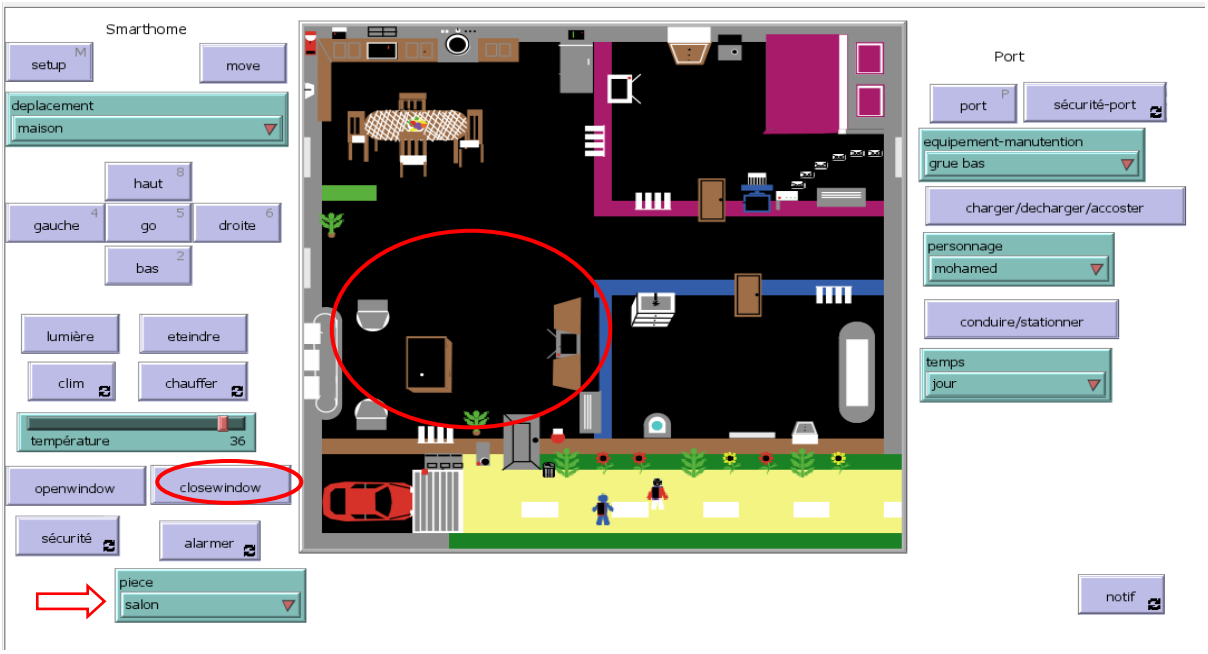


Figure III.11 *- Représentation du fonctionnement de la procédure Closewindow*

- **Sécurité :** c'est un bouton qui exécute la procédure **to Sécurité** qui permet d'activer la caméra de surveillance au niveau de l'entrée de la maison.

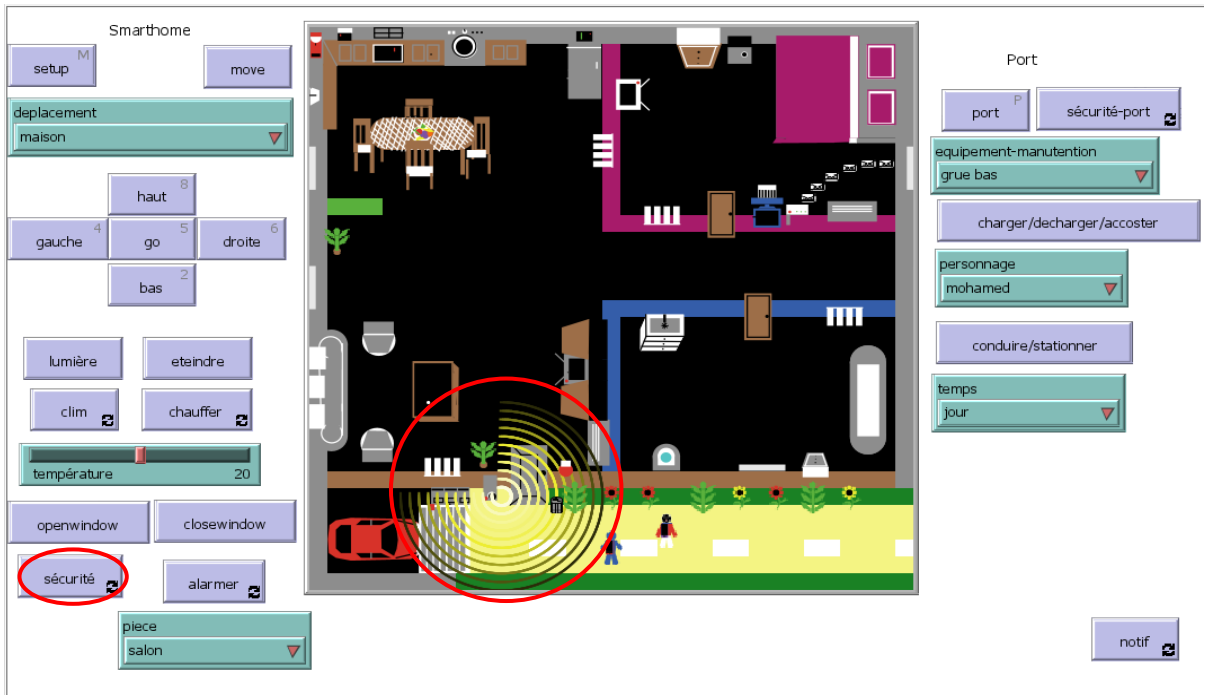


Figure III.12 *- Représentation du fonctionnement de la procédure Sécurité*

- **Alarme :** c'est un bouton qui exécute la procédure **to Alarmer** permettant d'activer l'alarme.

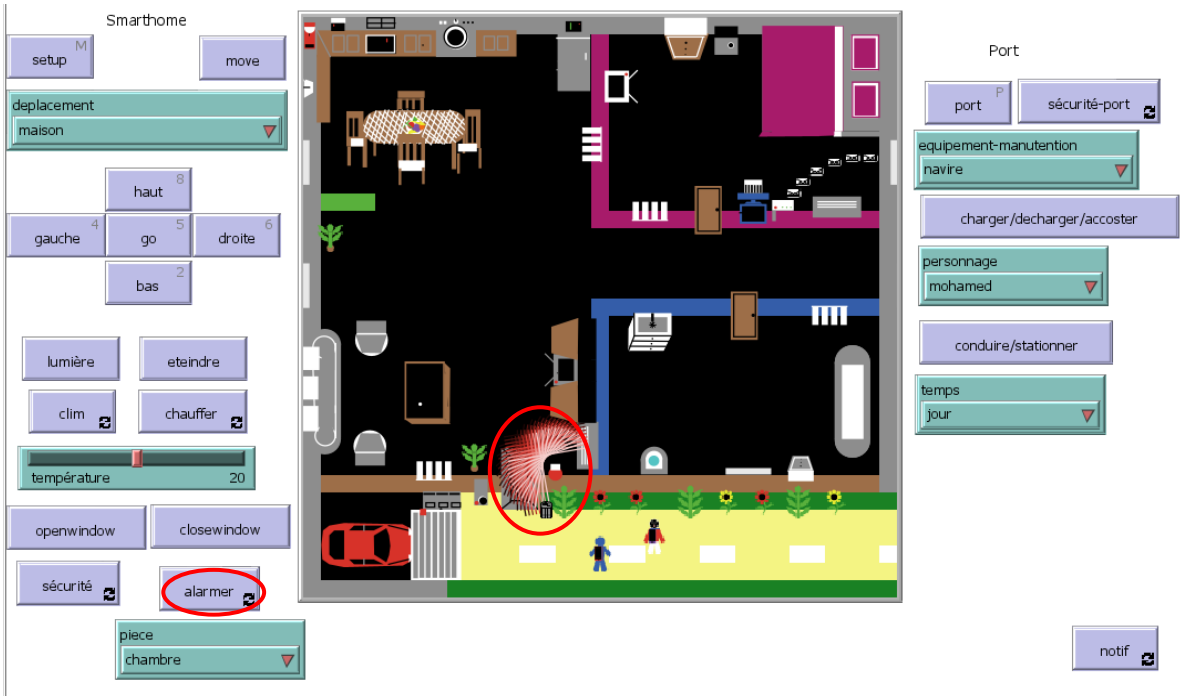


Figure III.13 *- Représentation du fonctionnement de la procédure Alarme*

- **Conduire/stationner :** c'est un bouton qui exécute la procédure **to Conduire/stationner** qui permet de déplacer la voiture et de la garer dans le garage.

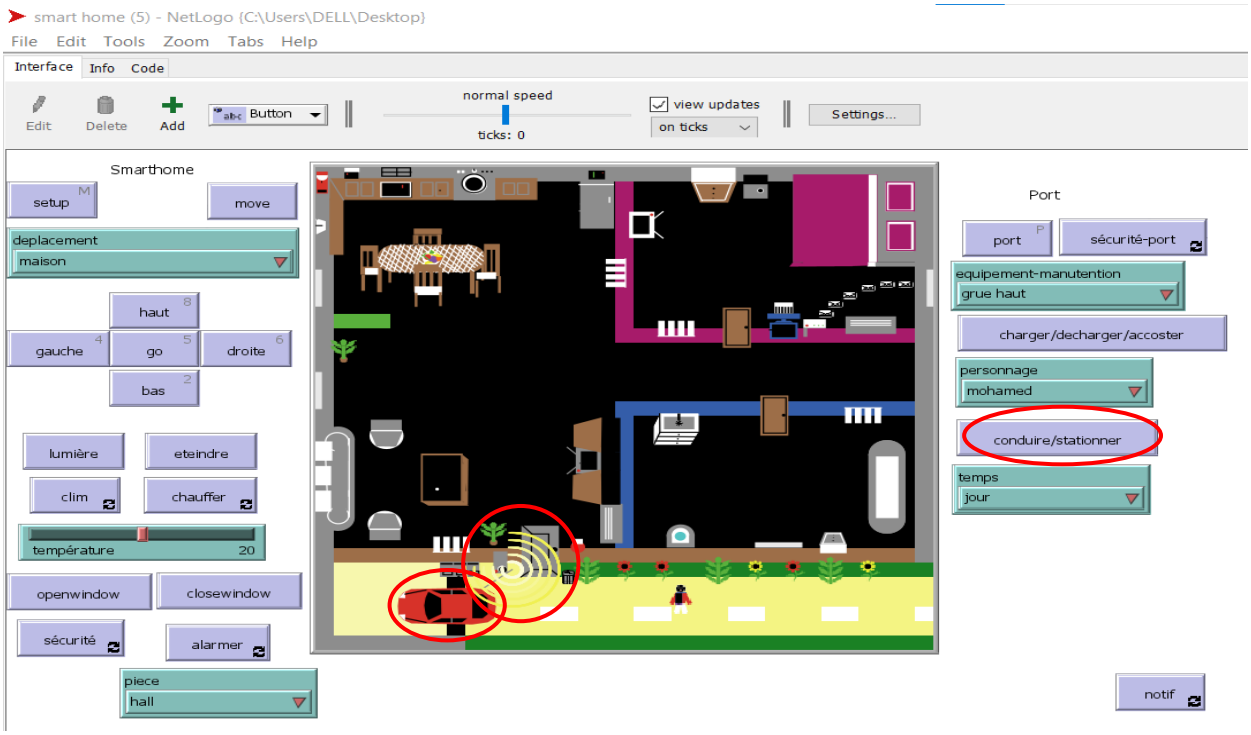


Figure III.14 *- Représentation du fonctionnement de la procédure Conduire/stationner*

- **Attack :** c'est un bouton qui exécute la procédure **to Attack** qui permet de réaliser une attaque hello flood sur les objets se trouvant dans la portée de l'attaquant ou un autre type d'attaque.

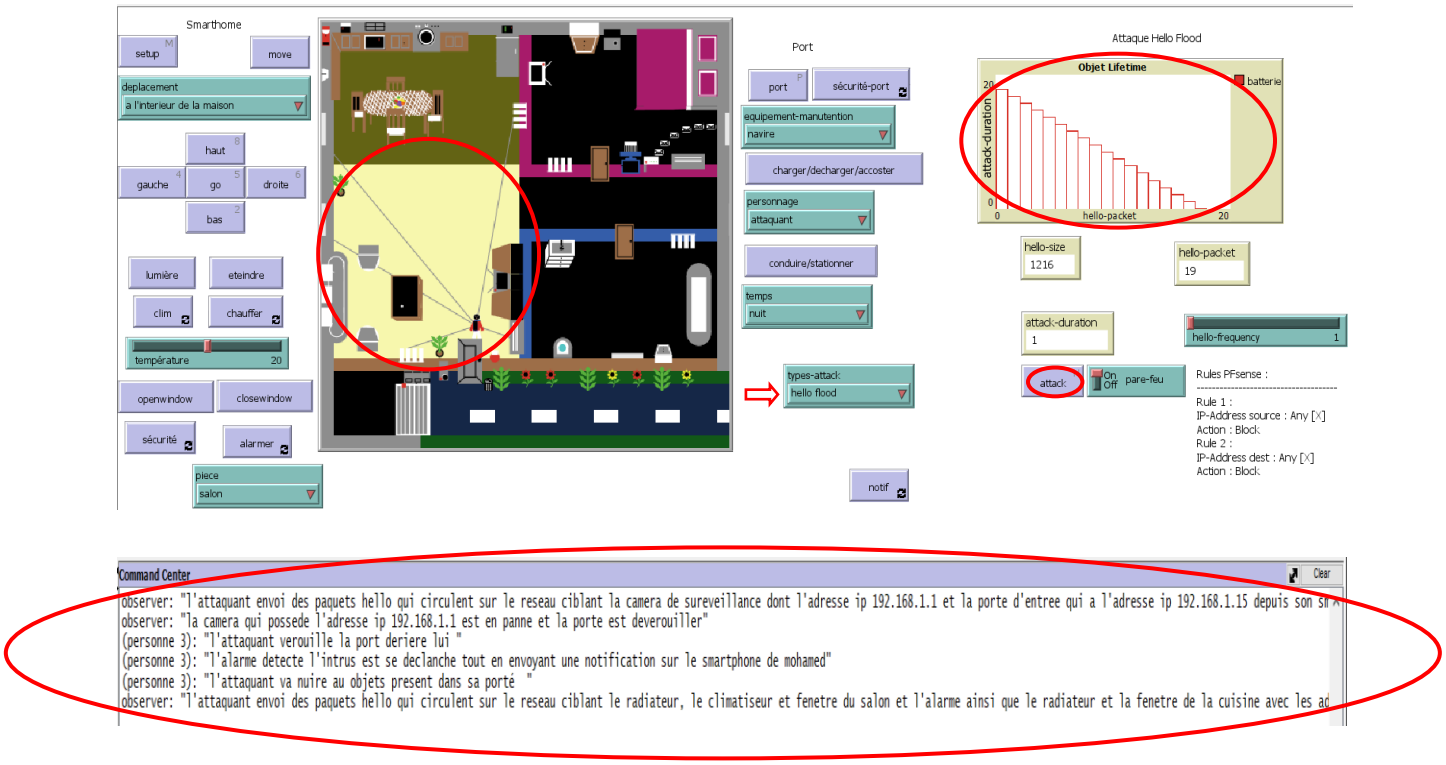


Figure III.15 *- Représentation du fonctionnement de la procédure Attack (Attaque hello flood)*

Graphe : Le graphe ci-dessous représente l'état de batterie des objets lors du déroulement de l'attaque hello flood en fonction du nombre de paquets envoyés et de la durée de l'attaque.

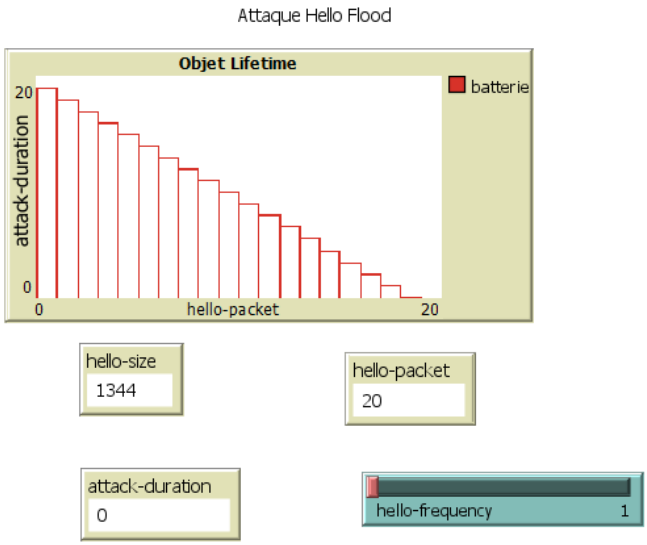


Figure III.16 *- Représentation du graphe de l'état de batterie des objets*

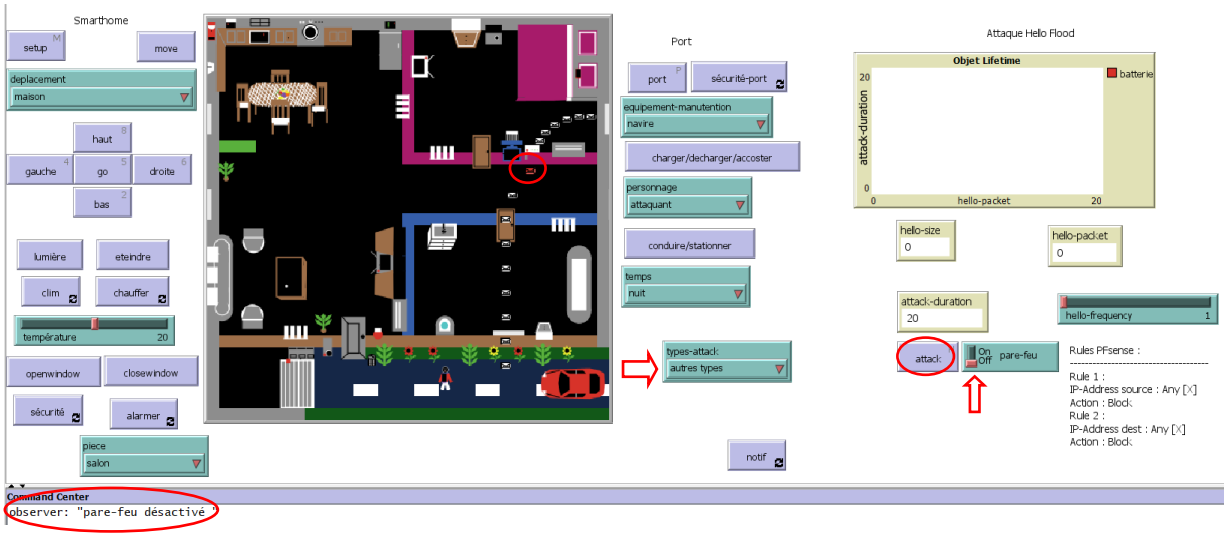


Figure III.17 *- Représentation du fonctionnement de la procédure Attack ("autres types d'attaques" lorsque le pare-feu est désactivé)*

Figure III.18 *- Paquet malveillant provenant d'un autre type d'attaque*

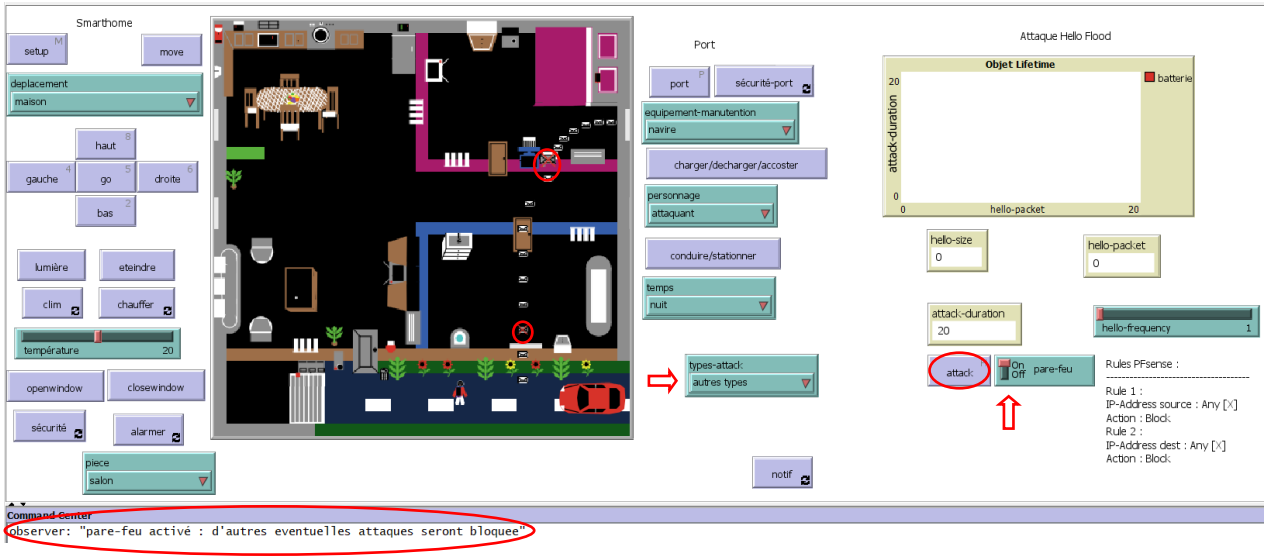


Figure III.19 *- Représentation du fonctionnement de la procédure Attack ("autres types d'attaques" lorsque le pare-feu est activé)*

Figure III.20 *– Représentation du paquet malveillant bloqué au niveau du routeur*

- **Notif :** c'est un bouton qui exécute la procédure **to Notif** qui permet de notifier et d'informer le propriétaire en envoyant un message en cas d'attaque.

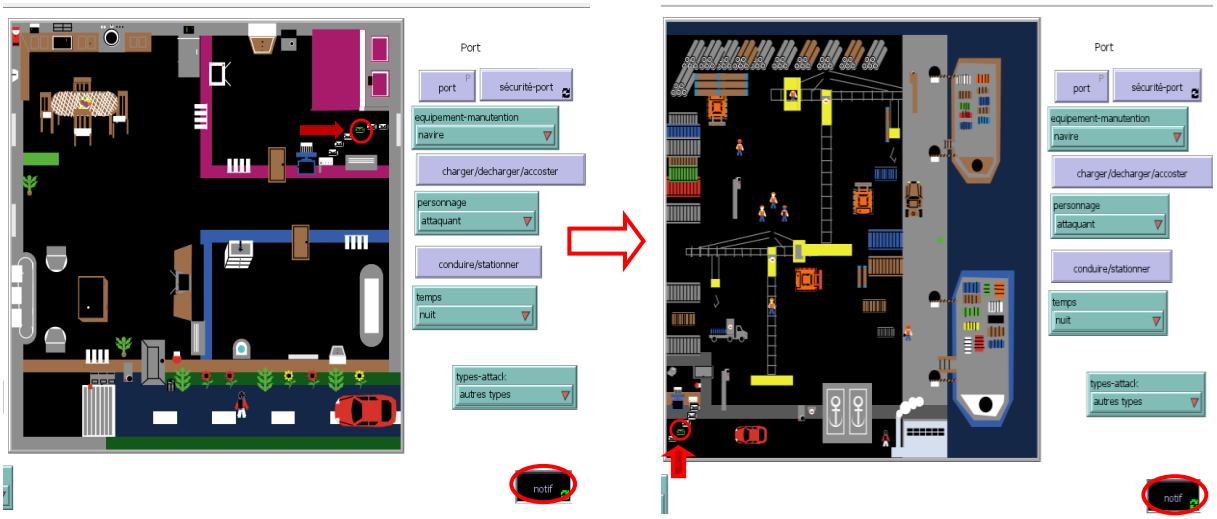


Figure III.21 *- Représentation du fonctionnement de la procédure Notif*

Figure III.22 *- Représentation de la notification*

Durant l'attaque "**hello flood**" sur la maison, une notification est envoyée à Mohamed pour l'informer (grâce au déclanchement de l'alarme). Ce dernier se rend directement chez lui et appel aussi tôt la police, qui arrive rapidement pour arrêter le coupable.

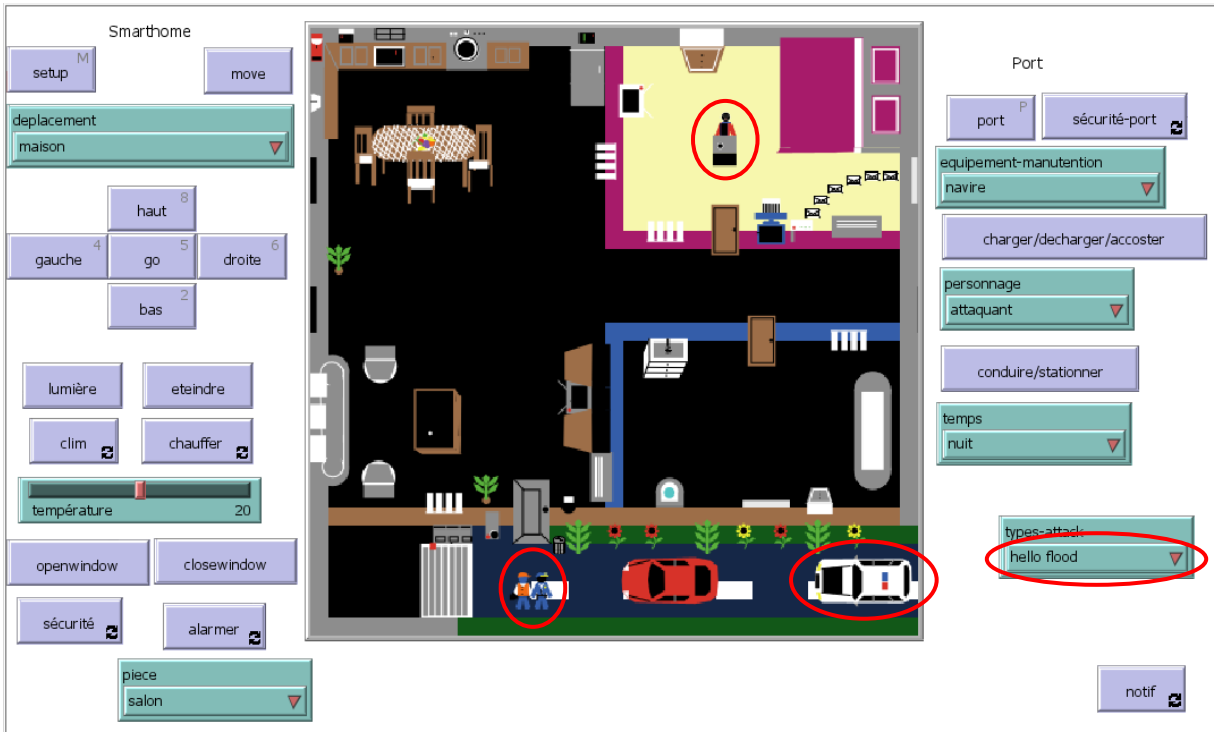


Figure III.23 *- Représentation de l'intervention de la police après une attaque hello flood sur la maison*

- **Sécurité-port :** c'est un bouton qui exécute la procédure **to Sécurité-port** qui permet d'activer toutes les caméras de surveillance présentes à l'entrée et au niveau du port.

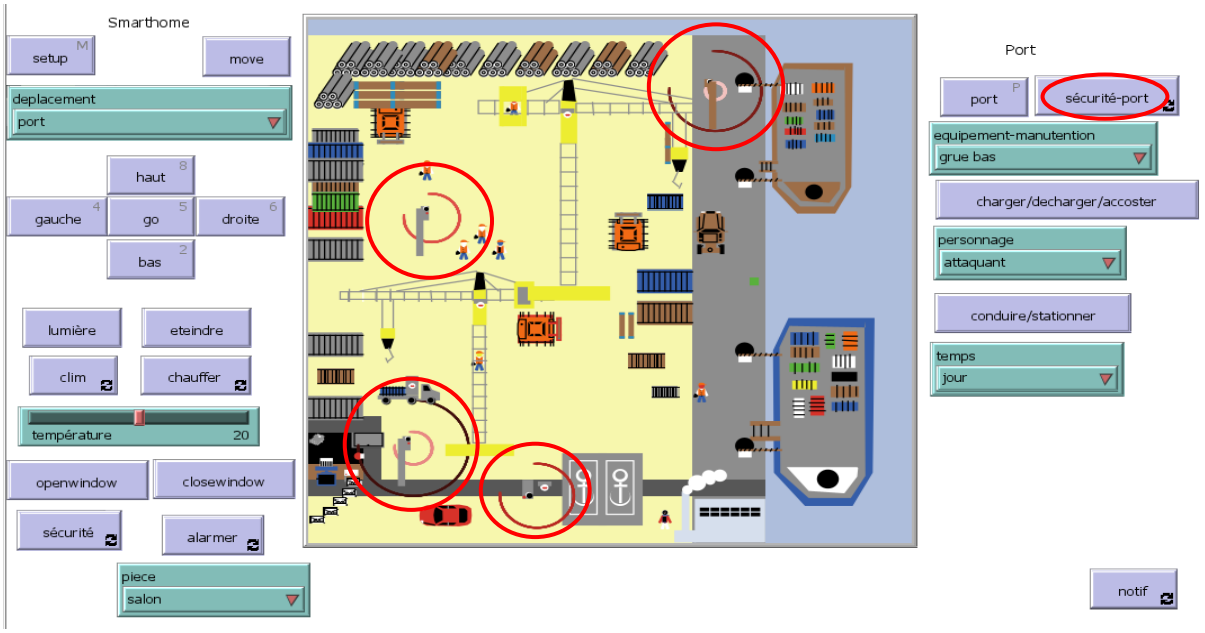


Figure III.24 *- Représentation du fonctionnement de la procédure Sécurité-port*

- **Charger/decharger/accoster :** c'est un bouton qui exécute la procédure **to charger/decharger/accoster** qui permet aux équipements de manutention et navire de se déplacer et de charger et décharger la cargaison.

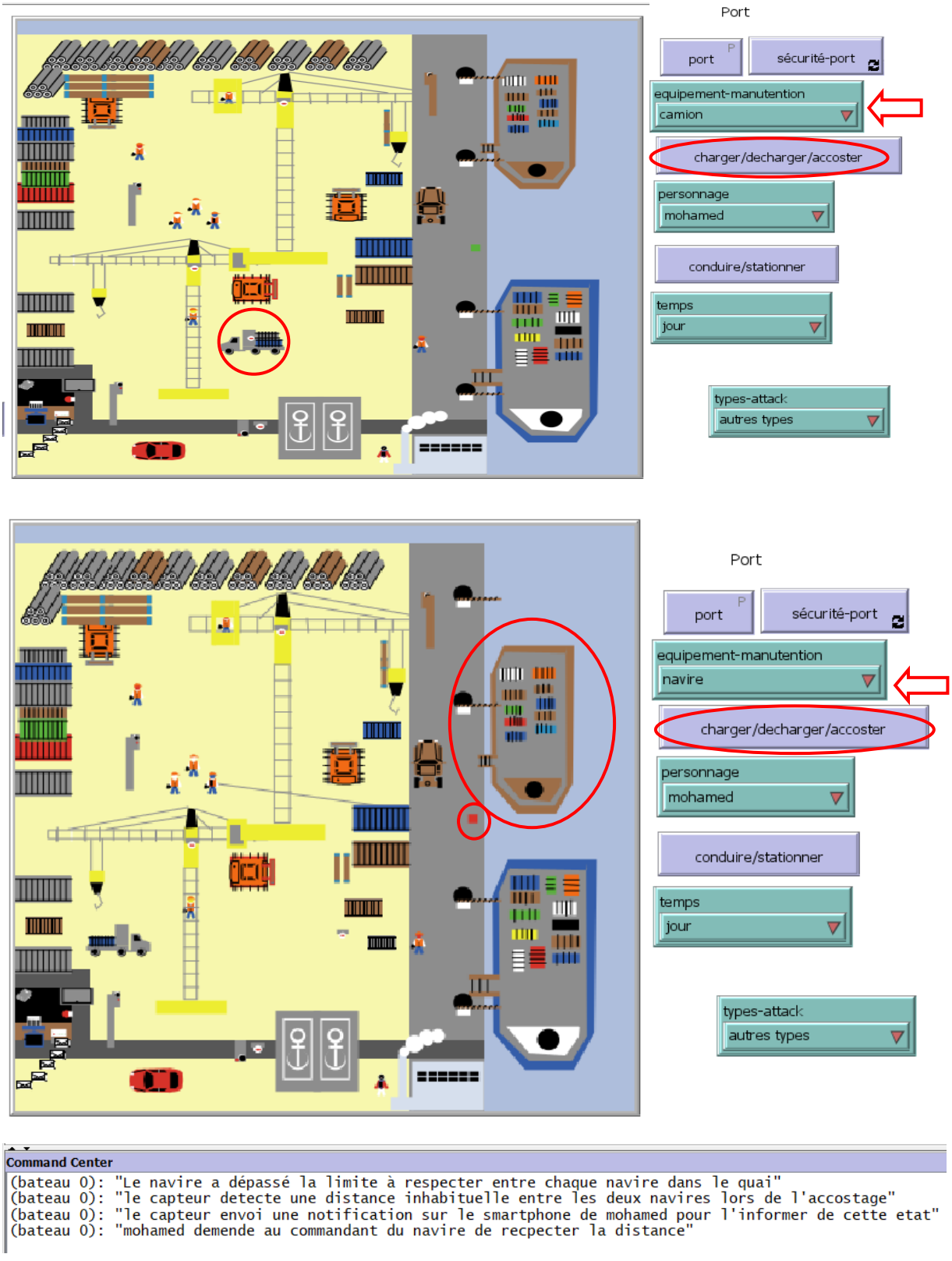


Figure III.25 *- Représentation du fonctionnement de la procédure charger/décharger/accoster*

6. Conclusion

Ce chapitre a présenté des scénarios liés à la maison intelligente et à l'attaque "hello flood" ainsi que la simulation d'une maison intelligente et d'un port intelligent à l'aide de NetLogo, ces simulations ont permis de mettre en évidence les avantages potentiels des technologies de l'Internet des objets (IoT) dans la gestion et l'optimisation des espaces domestiques et infrastructures portuaires.

La simulation d'une maison intelligente a démontré comment les dispositifs connectés peuvent interagir pour créer un environnement domestique plus confortable, sûr et économe en énergie. Les différents scénarios ont illustré la possibilité de surveiller les conditions de sécurité, de gérer efficacement la consommation énergétique et d'automatiser certaines tâches quotidiennes.

Quant à la simulation d'un port intelligent, elle a mis en lumière les avantages de l'utilisation de technologies avancées pour optimiser les opérations portuaires. Les scénarios ont illustré la surveillance en temps réel des activités portuaires et la gestion automatisée des flux de marchandises.

En conclusion, ces simulations ont permis de visualiser et d'explorer les fonctionnalités et les défis liés aux maisons intelligentes, aux ports intelligents et à la sécurité des dispositifs IoT. Elles ont souligné l'importance de l'innovation technologique et de la mise en œuvre de bonnes pratiques de sécurité pour exploiter pleinement le potentiel de l'IoT.

Conclusion Générale

En conclusion, notre étude nous a permis d'approfondir nos connaissances dans le domaine de l'Internet des objets (IoT) et de la sécurité. Nous avons acquis une compréhension approfondie des concepts clés, des enjeux et des défis liés à la sécurité d'une maison intelligente.

De plus, nous avons développé des compétences pratiques en utilisant NetLogo comme langage de simulation. Cette expérience nous a permis de modéliser et de simuler les interactions complexes au sein d'une maison intelligente et d'un port intelligent, en mettant l'accent sur l'attaque "Hello Flood" et ses conséquences potentielles. La simulation de la maison intelligente a souligné l'importance de l'interopérabilité et de la sécurité des dispositifs IoT pour garantir une expérience fiable et sécurisée, tandis que celle du port a montré comment les technologies de l'IoT peuvent améliorer l'efficacité, la sécurité et la gestion des ports.

En abordant le scénario d'attaque "hello flood" dans le contexte de la maison intelligente, nous avons mis en évidence les risques de sécurité associés à l'utilisation des dispositifs IoT. L'attaque "hello flood" a démontré comment un flux excessif de messages peut entraîner une surcharge du réseau et perturber le fonctionnement normal des appareils connectés. Cette simulation a souligné l'importance de mettre en place des mesures de sécurité robustes pour protéger les infrastructures et les données sensibles dans un environnement IoT.

Dans l'ensemble, cette expérience nous a permis de développer des compétences techniques solides dans le domaine de l'IoT et de la sécurité, ainsi que dans l'utilisation de NetLogo qui n'est pas initialement conçue spécifiquement pour les simulations de réseaux, mais nous avons pu créer une simulation adaptée à cet objectif.

Nous avons comme perspective de proposer des solutions appropriées dans le développement de maisons intelligentes sécurisées, tout en faisant face aux défis liés à la sécurité dans le contexte de l'Internet des objets. De plus, nous sommes fiers d'annoncer que nous avons soumis notre projet NetLogo comme modèle dans la bibliothèque de leur site officiel. Dans cette optique, nous envisageons également d'ajouter un module réservé à l'IoT dans NetLogo.

Bibliographie

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[2] K. Rose, S. Eldridge, and L. Chapin, “The Internet of Things (IoT): An Overview,” *Int. J. Eng. Res. Appl.*, vol. 5, no. 12, pp. 71–82, 2015, [Online]. Available: https://crsreports.congress.gov

[3] Wethrill John, “What Does it Mean to be ‘On’ The Internet of Things?,” *The new stack*, 2015. https://thenewstack.io/what-does-it-mean-to-be-on-the-internet-of-things/ (accessed Feb. 05, 2023).

[4] Admin oracle, “internet-of-things,” *Oracle*. https://www.oracle.com/fr/internet-of-things/what-is-iot/#:~:text=Qu’est-ce que l’IoT %3F,échanger des données avec eux (accessed Feb. 05, 2023).

[5] H. Z. and W. Z. J. Lin, W. Yu, N. Zhang, X. Yang, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, 2017, doi: 10.1109/JIOT.2017.2683200.

[6] J. S. and H.-Y. Du Miao Wu, Ting-Jie Lu, Fei-Yang Ling, “Research on the architecture of Internet of Things,” *2010 3rd Int. Conf. Adv. Comput. Theory Eng.*, vol. 5, pp. V5-484-V5-487, 2010, doi: 10.1109/ICACTE.2010.5579493.

[7] P. Andrzejewski, “IoT Architecture Layers,” *WizzDev*. https://wizzdev.pl/blog/iot-architecture-layers/ (accessed Feb. 09, 2023).

[8] C. M. Sosa-Reyna, E. Tello-Leal, and D. Lara-Alabazares, “Methodology for the Model-Driven Development of Service Oriented IoT Applications,” *J. Syst. Archit.*, vol. 90, pp. 15–22, 2018, doi: https://doi.org/10.1016/j.sysarc.2018.08.008.

[9] M. Lombardi, F. Pascale, and D. Santaniello, “Internet of Things: A General Overview between Architectures, Protocols and Applications,” *Information.*, vol. 12, 2021, doi: https://doi.org/10.3390/info12020087.

[10] O. Mazhelis and P. Tyrväinen, “A framework for evaluating Internet-of-Things platforms: Application provider viewpoint,” *2014 IEEE World Forum Internet Things*, pp. 147–152, 2014, doi: 10.1109/WF-IoT.2014.6803137.

[11] A. Abdelgawad and Y. Kumar, “Internet of Things (IoT) Platform for Structure Health Monitoring,” *Wirel. Commun. Mob. Comput.*, vol. 2017, p. 10, doi: https://doi.org/10.1155/2017/6560797.

[12] “What is an Internet of Things platform?,” *AVSystem*, 2019. https://www.avsystem.com/blog/what-is-internet-of-things-platform/ (accessed Feb. 06, 2023).

[13] Admin oracle, “iot-platform,” *Oracle*. https://www.oracle.com/fr/cloud/iot-platform/ (accessed Feb. 05, 2023).

[14] D. Hanes and G. Slagueiro, *IoT Fundamentals: Networking Technologies, Protocols,*

and Use Cases for the Internet of Things. 800 East 96th Street Indianapolis, IN 46240 USA: Cisco Press, 2017.

[15] Y. Perwej, H. Kashiful, J. Uruj, and S. Sharad, "Some Drastic Improvements Found in the Analysis of Routing Protocol for the Bluetooth Technology Using Scatternet," *Ubiquitous Comput. Commun. J.*, vol. CCITA-2010, no. Special issue (CCITA-2010), pp. 86–95, 2010.

[16] A. Meijer and M. P. Rodriguez Bolivar, "Governing the smart city: a review of the literature on smart urban governance," *Int. Rev. Adm.*, vol. 82, pp. 392–409, doi: DOI: 10.1177/0020852314564308.

[17] S. K. Datta, C. Bonnet, and N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services," *2014 IEEE World Forum Internet Things*, pp. 514–519, 2014, doi: 10.1109/WF-IoT.2014.6803221.

[18] E. LIAO, "4 Commonly-Used Smart City Technologies," *earth.org*, 2023. https://earth.org/smart-city-technologies/ (accessed Feb. 07, 2023).

[19] M. Dohler, I. Vilajosana, X. Vilajosana, and J. LLosa, "Smart Cities: An Action Plan," *Proc. Barcelona Smart Cities Congr.*, pp. 1–6, 2011.

[20] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things J.*, vol. 1, pp. 22–32, 2014, doi: 10.1109/JIOT.2014.2306328.

[21] N. Ouerhani, N. Pazos, M. Aeberli, J. Senn, and S. Gobron, "Dynamic Street Light Management - Towards a citizen centered approach," *3rd Int. Conf. Hybrid City*, 2015.

[22] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An Information Framework for Creating a Smart City Through Internet of Things," *IEEE Internet Things J.*, vol. 1, pp. 112–121, 2014, doi: 10.1109/JIOT.2013.2296516.

[23] A. R. Al-Ali, I. Zualkernan, and F. Aloul, "A Mobile GPRS-Sensors Array for Air Pollution Monitoring," *IEEE Sensors J.*, vol. 10, pp. 1666–1671, 2010, doi: 10.1109/JSEN.2010.2045890.

[24] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[25] "What the heck is a Smart City?," *aliga*. https://aliga.sk/en/what-the-heck-is-a-smart-city/ (accessed Feb. 07, 2023).

[26] N. Zhu et al, "Bridging e-Health and the Internet of Things: The SPHERE Project," *IEEE Intell. Syst.*, vol. 30, pp. 39–46, 2015, doi: 10.1109/MIS.2015.57.

[27] R. Loftus, "The hospital of the future: Could smart hospitals deliver better healthcare?," *Secure futures by Kaspersky*, 2021. https://www.kaspersky.com/blog/secure-futures-magazine/smart-hospitals-healthcare/38830/ (accessed Feb. 08, 2023).

[28] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans Ind. Informat*, vol. 10, pp. 1578–1586, 2014, doi: 10.1109/TII.2014.2306382.

[29] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sens. J.*, vol. 16, pp. 1368–1376, 2016, doi:

10.1109/JSEN.2015.2502401.

[30] D. Dimitrov, "Medical internet of things and big data in healthcare," *Healthc. Inform. Res.*, vol. 22, no. 3, pp. 156–163, 2016.

[31] B.-O. Nazmiye, D. Rosemary, B. Martha, and L. Whitmarsh, "Social barriers to the adoption of smart homes," *Energy Policy*, vol. 63, pp. 363–374, 2013, doi: https://doi.org/10.1016/j.enpol.2013.08.043.

[32] Y. Perwej, "A Literature Review of the Human Body as a Communication Medium using RedTacton," *Commun. Appl. Electron.*, vol. 9, pp. 7–17, 2016, doi: 10.5120/cae2016652161.

[33] Y. Perwej, "The Next Generation of Wireless Communication Using Li-Fi (Light Fidelity) Technology," *J. Comput. Networks*, vol. 4, pp. 20–29, 2017, doi: 10.12691/jcn-4-1-3.

[34] G. Thomas, W.-J. Yi, E. Monsef, and J. Saniie, "Home Automation Device Protocol (HADP): A protocol Standard for Unified Device Interactions," *Adv. Internet Things*, vol. 5, pp. 27–38, 2015, doi: 10.4236/ait.2015.54005.

[35] Jao Lima, "Behold the 10 biggest IoT investments," *Computer Business Review*, 2015. https://techmonitor.ai/hardware/behold-the-10-biggest-iot-investments-4549522 (accessed Feb. 07, 2023).

[36] "Smart Home," *Visioforce Automation Systems*. http://visioforce.com/smarthome.html (accessed Feb. 09, 2023).

[37] T. R. Gondaliya, "A Survey on an Efficient IoT Based Smart Home," *Int. J. Rev. Electron. Commun. Eng.*, vol. 4, 2016.

[38] D. Boban and L. Aleksandra, "A smart home system based on sensor technology," *Electron. Energ.*, vol. 29, pp. 451–460, 2016, doi: 10.2298/FUEE1603451D.

[39] P. Yusuf, K. Haq, and F. Parwej, "The Internet of Things (IoT) and its Application Domains," *Int. J. Comput. Appl.*, vol. 182, no. 49, pp. 36–49, 2019, doi: 10.5120/ijca2019918763.

[40] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013, doi: https://doi.org/10.1016/j.comnet.2012.12.018.

[41] M. Skubic, G. Alexander, M. Popescu, M. Rantz, and J. Keller, "A smart home application to eldercare: Current status and lessons learned," *Technol. Heal. Care*, vol. 17, no. 3, pp. 183–201, 2009, doi: 10.3233/THC-2009-0551.

[42] C. Badica, M. Brezovan, and A. Badica, "An overview of smart home environments: architectures, technologies and applications," *BCI*, vol. 78, 2013.

[43] D. Bregman and L. Rishon, "Smart Home Intelligence - The eHome that Learns," *Int. J. Smart Home*, vol. 4, pp. 35–46, 2010.

[44] Y. Perwej, M. Ahmed, B. Kerim, and H. Ali, "An Extended Review on Internet of Things (IoT) and its Promising Applications," *Commun. Appl. Electron.*, vol. 7, no. 26, pp. 8–22, Feb. 2019, doi: 10.5120/cae2019652812.

[45] L.D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind.*

Informatics, vol. 10, pp. 2233–2243, 2014.

[46] J. J. M. Wollschlaeger, T. Sauter, *The future of industrial communication: Automation networks in the era of the internet of things and Industry 4.0*, vol. 11. 2017.

[47] Integral System, "QU'EST-CE QUE L'INTERNET INDUSTRIEL DES OBJETS (IIOT) ?," *blog.integral-system*, 2019. https://blog.integral-system.fr/quest-ce-que-linternet-industriel-des-objets-iiot/ (accessed Apr. 23, 2023).

[48] B. Leal and L. Atzori, *Objects Communication Behavior on Multihomed Hybrid Ad Hoc Networks.* New York, NY: Springer, New York, NY, 2010. doi: https://doi.org/10.1007/978-1-4419-1674-7_1.

[49] G. et al Cristian González, "Midgar: Generation of heterogeneous objects interconnecting applications. A Domain Specific Language proposal for Internet of Things scenarios," *Comput. Networks*, vol. 64, pp. 143–158, 2014, doi: https://doi.org/10.1016/j.comnet.2014.02.010.

[50] J. Kiljander et al, "Semantic Interoperability Architecture for Pervasive Computing and Internet of Things," *IEEE Access*, vol. 2, pp. 856–873, 2014, doi: 10.1109/ACCESS.2014.2347992.

[51] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[52] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, Mar. 2019, doi: 10.1016/j.iot.2018.11.003.

[53] S. Hugot, "Monitoring temps réel : quelle supervision choisir ?," *Organisation Performante*, 2019. https://www.organisation-performante.com/supervision-temps-reel-quel-monitoring-choisir/ (accessed Mar. 19, 2023).

[54] La Rédaction TechTarget, "Surveillance IT (IT monitoring)," *LeMagit*, 2018. https://www.lemagit.fr/definition/Surveillance-IT-IT-monitoring (accessed Mar. 19, 2023).

[55] "Surveillance du réseau et alertes en temps réel," *World-Connected service*. https://world-connect.ch/services-informatique/monitoring/ (accessed Apr. 20, 2023).

[56] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[57] S. Li, L. Da Xu, and S. Zhao, "internet of things : a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, Apr. 2015, doi: 10.1007/s10796-014-9492-7.

[58] FJALADE, "Les enjeux de la supervision IOT (Internet of Things)," 2019.

[59] J. Hernantes, G. Gallardo, and N. Serrano, "IT Infrastructure- Monitoring Tools," *Softw. Technol.*, pp. 88–92, 2015.

[60] D. Russell, Brian, V.Duren, *Practical Internet of Things Security*, Packt Publ. 2016.

[61] D. B. R. Rituparna Chaki, *Security in IoT: The Changing Perspective*, CRC Press. 2022.

[62] S. Pirbhulal *et al.*, “A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network,” *Sensors*, vol. 17, no. 12, p. 69, Dec. 2016, doi: 10.3390/s17010069.

[63] G. Alasdair, *IoT Security Issues*, G-Press. 2017.

[64] D. P. Li, Kuan-ching, Gupta, Brij , Agrawal, *Recent advences in security, privacy, and trust for internet of things (IoT) and cyber-physical systems (CPS)*. CRC Press, 2021.

[65] S. Jaydip and P. Sujata, *Security and privacy in internet of things : models, algorithms and implementations*, Springer. 2017.

[66] (1983) Pal, Souvik, Garcia Diaz, Vicente, (1981) Le, Dac-Nhuong, *IoT : security and privacy paradigm*, CRC Press. 2020.

[67] S. Krushang and H. Upadhyay, “A Survey: DDOS Attack on Internet of Things,” *Int. J. Eng. Res. Dev.*, vol. 10, no. 11, pp. 58–63.

[68] T. Aditya Sai Srinivas and S. S. Manivannan, “Prevention of Hello Flood Attack in IoT using combination of Deep Learning with Improved Rider Optimization Algorithm,” *Comput. Commun.*, 2020, doi: 10.1016/j.comcom.2020.03.031.

[69] S. G. Akhil Dubey, Deepak Meena, “A Survey in Hello Flood Attack in Wireless Sensor Networks,” *Int. J. Eng. Res. Technol.*, vol. Vol. 3, no. Issue 1, pp. 1882–1887.

[70] B. Bellatar, *Modélisation & Simulation sur Ordinateur (Thése de Doctorat)*. Université de Batna, 2004.

[71] B. CALVEZ, *Le calibrage de modèles à base d’agents pour la simulation de systèmes complexes. These de doctorat*. Université d’Evry Val d’Essonne, 2007.

[72] S. BENKHEDDA, *Simulation multi agents d’un comportement humain face à une situation d’urgence(Diplôme de Magister)*. Université des sciences et de la technologie d’Oran Mohamed Boudiaf USTOMB, 2012.

[73] M. W. Maier, “Architecting Principles for Systems-of-Systems,” *Syst. Eng.*, vol. 1, no. 4, pp. 267–284, 1998, doi: https://doi.org/10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D.

[74] S. Tisue and U. Wilensky, “NetLogo: A Simple Environment for Modeling Complexity,” p. 10, 2004.

Résumé

L'IoT a révolutionné notre interaction avec l'environnement en connectant les objets à internet, offrant de nombreuses possibilités. Notre projet met en évidence l'importance de la sécurité des systèmes IoT dans les maisons intelligentes. Malgré les avantages offerts par l'IoT, les maisons intelligentes sont vulnérables aux attaques malveillantes telles que l'attaque Hello Flood, qui menace la confidentialité et l'intégrité des données. Pour renforcer la sécurité, les pares-feux jouent un rôle essentiel en filtrant le trafic réseau et en bloquant les intrusions. De plus, un monitoring constant est crucial pour détecter les activités suspectes et prendre des mesures correctives immédiates. Nous avons utilisé le simulateur NetLogo afin de modéliser et évaluer les performances des systèmes IoT, en optimisant leur fonctionnement global. Bien qu'il ne soit pas spécifiquement conçu pour les simulations de réseaux à l'origine, nous avons réussi à créer une simulation répondant à cet objectif.

Mots clés : Internet des objets, Maison intelligente, Sécurité des systèmes ; Simulateur Netlogo, Attaque hello flood, Pare-feu, Monitoring.

Abstract

The IoT has revolutionized our interaction with the environment by connecting objects to the internet, opening up a wealth of possibilities. Our project highlights the importance of security for IoT systems in smart homes. Despite the advantages offered by the IoT, smart homes are vulnerable to malicious attacks such as the Hello Flood attack, which threatens data confidentiality and integrity. To enhance security, firewalls play an essential role in filtering network traffic and blocking intrusions. In addition, constant monitoring is crucial to detect suspicious activity and take immediate corrective action. We used the NetLogo simulator to model and evaluate the performance of IoT systems, optimizing their overall operation. Although it was not originally designed specifically for network simulations, we succeeded in creating a simulation that met this objective.

Keywords: Internet of Things, Smart Home, Systems security; Netlogo simulator, Hello flood attack, Firewall, Monitoring.