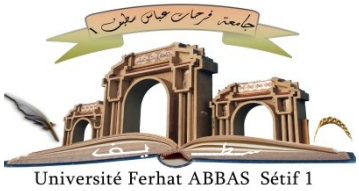
الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de L'Enseignement Supérieur et de la Recherche Scientifique



UNIVERSITÉ FERHAT ABBAS – SETIF1

FACULTÉ DE TECHNOLOGIE

THESE

Présentée au Département d'Electronique

Pour l'obtention du diplôme de

DOCTORAT EN SCIENCES

Option: Electronique

Par

KHOUNI Sadika

THÈME

Gestion optimale des WSN (Wireless Sensor Network), Application aux IOT (Internet Of Things)

Soutenue le 19/01/2023 devant le Jury:

BOULOUFA Abdelslam	**Professeur**	**Univ. Ferhat Abbas Sétif 1**	**Président**
CHEMALI Hamimi	**Professeur**	**Univ. Ferhat Abbas Sétif 1**	**Directeur de thèse**
ZIET Lahcene	**Professeur**	**Univ. Ferhat Abbas Sétif 1**	**Examinateur**
SARRA Mustapha	**Professeur**	**Univ. BBA**	**Examinateur**
BEKKOUCHE Tewfik	**MCA**	**Univ. BBA**	**Examinateur**
HACINE GHARBI Abdenour	**MCA**	**Univ. BBA**	**Examinateur**

Remerciements

Je remercie tout d'abord **ALLAH** le tout puissant de m'avoir donné la foi, la santé et le courage pour mener à terme ce modeste travail.

Mes chaleureux remerciements à mon directeur de thèse **Pr. CHEMALI Hamimi**, pour son intérêt et son soutien, sa grande disponibilité et ses nombreux conseils durant la réalisation de cette thèse.

Mes vifs remerciements s'adressent aussi aux membres de jury pour avoir accepté d'évaluer cette thèse:

Monsieur **BOULOUFA Abdelslam**, Professeur à l'Université de Sétif 1, d'avoir accepté de juger mon travail et de présider le jury de soutenance de cette thèse.

Messieurs **ZIET Lahcene,** Professeur à l'Université de Sétif 1, **SARRA Mustapha** Professeur, **BEKKOUCHE Tewfik** MCA, et **HACINE GHARBI Abdenour** MCA à l'Université de Bordj Bou-Arréridj, qui m'ont honoré par le fait d'avoir accepté d'être les examinateurs de cette thèse.

Mes aimables remerciements à mes chers parents pour leur amour et leur patience, mes chers frères et sœurs et toute ma famille pour leur soutien morale durant la période de la réalisation de ce modeste travail.

Mes plus vifs remerciements à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce modeste travail.

Sommaire

Remerciements II
Sommaire III
Liste des Figures IX
Liste des Tableaux XI
Liste des acronymes XII
Introduction Générale 1
Chapitre 01: Etat de l'art de l'Internet Of Things 5
1.1. Introduction 5
1.2. Définitions de l'Internet Of Things (IOT) 5
1.2.1. Définition de ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) 6
1.2.2. Définition de l'UIT (Union Internationale des Télécommunications) 6
1.2.3. Définition de l'IETF (Internet Engineering Task Force) 7
1.2.4. Définition de l'IEEE (Institute of Electrical and Electronics Engineers) 7
1.2.5. Définition de la CRP-IdO (Cluster des Projets européens de Recherche sur l'Internet des Objets) 7
1.2.6. Définition de l'OASIS (Organization for the Advancement of Structured Information Standards) 7
1.3. Les architectures d'IOT 8
1.4. L'IOT et les réseaux de communication sans fil 8
1.4.1. Les WPAN (Wireless Personal Area Networks) 8
1.4.1.1. Radio Frequency IDentification 9
1.4.1.3. IEEE 802.15.4 11
1.4.2. WLAN (Wireless Local Area Network) 14
1.4.3. Les LPWAN (Low Power Wide Area Networks) 15
1.4.4. L'IOT et les réseaux cellulaires 16
1.4.4.1. EC-GSM-IoT (EC : Extended Coverage) 17

1.4.4.2. eMTC (enhanced Machine Type Communication) (ou LTE-M) (Long-Term Evolution for Machines) 17
1.4.4.3. NB-IOT (stands for Narrowband Internet Of Things) 17
1.5. Les applications de l'IOT 17
1.5.1. La domotique 17
1.5.2. Environnement intelligent 18
1.5.3. Transport et logistique 18
1.5.4. Agriculture intelligente 18
1.5.5. Les Villes intelligentes 18
1.5.6. Les compteurs intelligents 18
1.5.7. Sécurité et Urgences 19
1.5.8. La Cybersanté 19
1.5.9. Le Contrôle industriel 19
1.5.10. Vente au détail 19
1.5.11. Gestion intelligente de l'eau 19
1.6. Les défis face à l'application d'IOT 19
1.6.1. Interopérabilité 20
1.6.1.1. Définition 20
1.6.1.2. Les Causes qui empêchent l'interopérabilité 20
1.6.2. La sécurité 20
1.6.2.1. Authentification 20
1.6.2.2. Confidentialité 21
1.6.2.3. Intégrité 21
1.6.2.4. Disponibilité 22
1.6.2.5. La Non ''répudiation'' 22
1.6.2.6. Le Non ''rejeu'' 22
1.6.2.7. La résilience 22
1.6.2.8. L'évolutivité 22
1.6.2.9. La tolérance aux pannes 22
1.7. Conclusion 23
Chapitre 02 : L'approche IOT-WSN 24

2.1. Introduction 24
2.2. Historique 24
2.3. Définition de Wireless Sensors Network (WSN) 25
2.4. L'Architecture physique d'un ''nœud capteur'' 26
2.4.1. Unité de capture (d'acquisition) 26
2.4.2. Unité de traitement 26
2.4.4. Unité de gestion de puissance 27
2.5. Les différents types de topologies des WSN 27
2.5.1. Topologie plate 27
2.5.2. Topologie hiérarchique 27
2.6. Les domaines d'application des réseaux WSN 28
2.7. Les types de WSN 29
2.7.1. Les WSN terrestres 29
2.7.3. Les WSN sous-marins 31
2.7.4. Les WSN mobiles 31
2.7.5. Les WSN multimédia 31
2.8. Consommation énergétique 32
2.9. Communication dans les WSN 33
2.9.1. Le modèle en couche adapté aux WSN 33
2.10. Les standards de communication adaptés aux WSN 34
2.11. Technologies des WSN 35
2.11.1. ANT technologie 35
2.11.2. Wavenis technologie 35
2.11.3. Dash7 technologie 36
2.11.4. EnOcean technologie 36
2.12. Conclusion 37
Chapitre 03 : Gestion optimale des WSN 38
3.1. Introduction 38
3.2. La gestion dans les WSN 38
3.2.1. Plan de gestion d'énergie 38
3.2.2. Plan de gestion de mobilité 39

3.2.3. Plan de gestion de tâche 39
3.3. L'optimisation des WSN 39
3.3.1. Optimisation de déploiement des nœuds 39
3.3.1.1. Approches centralisées (Node Centric) 40
3.3.1.2. Approches Distribuées 40
3.3.1.3. Approches hybrides 41
3.3.2. Optimisation par la sécurité de l'agrégation des données 42
3.3.3. Optimisation par la tolérance aux pannes 44
3.3.3.1. Optimisation au niveau de la sous-couche Mac de la couche liaison de données 44
3.3.3.1.1. Les protocoles ordonnancés (Scheduling protocols) 45
3.3.3.1.2. Protocoles à base de contention 46
3.3.3.2. Optimisation au niveau de la couche réseau 47
3.3.3.2.1. Les topologies plates 47
3.3.3.2.2. Les topologies hiérarchiques (Clustering) 49
3.4. Conclusion 50
Chapitre 04 : La technologie PSN 51
4.1. Introduction 51
4.2. Définition de la technologie PSN 51
4.3. La catégorisation des protocoles de routage dans PSN 52
4.3.1. Catégorie 1: Protocoles de routage basés sur les contacts 52
4.3.1.1 Protocole de routage ‘‘Direct Delivery’’ 52
4.3.2. Catégorie 2: Protocoles de routage basés sur l'inondation (Flooding) 54
4.3.2.1. Le protocole de routage Epidémique 54
4.3.2.2. Le protocole de routage SaW (Spray and Wait) 55
4.3.2.3. Le protocole de routage HMSaW (Human- Mobility Based Spray and Wait) 56
4.3.3. Catégorie 3: Protocoles de routage basés sur des modèles probabilistiques 57
4.3.3.1. Le protocole de routage PROPHET (Probabilistic ROuting Protocol using History of Encounters and Transitivity) 57
4.3.3.2. Le protocole de routage I-PROPHET (IMPROVED PROPHET) 60
4.3.3.3. Le protocole de routage PROPHET+ 61
4.3.4. Catégorie 4 : Protocoles de routage basés sur la communauté 62
4.3.4.1. Le protocole de routage ‘‘Bubble Rap’’ 62

4.3.4.2. Le protocole de routage HERO (HomE based Relay selectiOn) 63
4.3.4.2.1. Algorithme HERO de base 63
4.3.4.2.2. Algorithme HERO amélioré 63
4.3.4.3. Le protocole de routage PNGP (Popular Node Gateway Protocol) 64
4.3.5. Catégorie 5: Protocoles de routage basés sur les informations sociales 65
4.3.5.1. Le protocole de routage ‘‘Friendship Based Routing’’ 65
4.3.5.2. Le protocole de routage SANE (Social Aware Networking) 66
4.3.5.3. Le protocole de routage ‘‘Social Circle’’ 67
4.3.5.4. Le protocole de routage ‘‘ChitChat’’ 69
4.3.6.Catégorie 6: Protocoles de routage basés sur l’efficacité énergétique, ou les points d’accès (Hotspot or Energy Efficiency Based Routing Protocols) 70
4.4. Les défis face à la technologie PSN 71
4.4.1. La mobilité 71
4.4.2. Egoïsme 72
4.4.3. Transfert des données 72
4.4.4. La sécurité 72
4.4.5. Évolutivité et Regroupement 73
4.4.6. Gestion de l'énergie et du stockage 73
4.5. Application de PSN 74
4.5.1. Communication à distance 74
4.5.2. Gestion des catastrophes 74
4.5.3. L’analyse des réseaux sociaux 74
4.5.4. Détection des maladies 75
4.5.5. Détection de communauté 75
4.6. Le modèle de couches adapté au PSN 75
4.7. Conclusion 76
Chapitre 05 : Le modèle IOT-PSN 78
5.1. Introduction 78
5.2. Description du modèle 78
5.2.1. Topologie du modèle 78
5.2.2. Le degré de sécurité 79
5.2.3 Les scénarios de communication implantés 80

5.2.3.1. Le scénario de déplacement entre les communautés 80
5.2.3.2. Le scénario de recherche du ‘‘node-agent’’ 82
5.3.1. Description du SSEA 86
5.3. La simulation du modèle IOT-PSN 88
5.3.1. Comparaison de SEA avec SSEA 88
5.3.1.1 La comparaison pour des nœuds de même degré de sécurité 88
5.3.1.2. La comparaison pour des nœuds de différents degrés de sécurité 89
5.3.1.3. Influence de t_1 sur le temps d’infection 96
5.3.2. La Comparaison de SSEA avec GOSSIP 101
5.4. Conclusion 105
Conclusion Générale 107
Bibliographie 109

Liste des Figures

Chapitre 01: Etat de l'art de l'Internet Of Things

Figure 1. 1 L'IOT vue comme une fédération de réseaux autour de l'Internet. 6
Figure 1. 2 Technologies RFID : fonctionnalités en fonction de la capacité mémoire. 10
Figure 1. 3 Evolution des tags RFID, de haut en bas : un tag en lecture seule 12 bits, 1976 ; un tag en lecture seule de 128 bits, 1987 ; un tag en lecture écriture de 1024 bits, 1999. 10
Figure 1. 4 Piles technologiques ZigBee IP 2006 et ZigBee Pro 2007. 13
Figure 1. 5 Architecture du système SIGFOX. 16

Chapitre 02: L'approche IOT-WSN

Figure 2. 1 Wireless Sensor Network (WSN) 25
Figure 2. 2 Architecture physique d'un nœud capteur sans fil 26
Figure 2. 3 Topologie plate 28
Figure 2. 4 Topologie hiérarchique 28
Figure 2. 5 Taxonomie des applications des WSN 29
Figure 2. 6 Types de WSN 30
Figure 2. 7 modèle de couches adapté pour les WSN 34

Chapitre 03: Gestion optimale des WSN

Figure 3. 1.Disques unitaires et intersection entre deux nœuds (u,v) . 41
Figure 3. 2.Protocoles d'agrégation dans les réseaux de capteurs sans fils. 42
Figure 3. 3.Classification des solutions d'agrégation sécurisées. 44
Figure 3. 4.Sous-couche MAC dans le modèle OSI 45

Chapitre 04: La technologie PSN

Figure 4. 1. Mécanisme du routage ''Direct Delivery'' 53
Figure 4. 2. Mécanisme du routage épidémique. 55
Figure 4. 3. Procédure de l'algorithme de routage de PROPHET. 58
Figure 4. 4. Techniques de transfert de données ''Bubble Rap'' 62
Figure 4. 5. Les modèles de mobilité des nœuds. 67
Figure 4. 6. Un exemple de PSN(ChitChat), où les flèches en lignes continues représentent le mouvement des véhicules et les flèches en lignes pointées représentent l'établissement des connexions et l'échange d'information. 69
Figure 4. 7. La couche bundle. 76

Chapitre 05: Le modèle IOT-PSN

Figure 5. 1. La Topologie du modèle IOT Proposé. 80
Figure 5. 2. Organigramme du déplacement du ''member-agent'' entre les communautés. 81
Figure 5. 3. La détection d'appartenance à la communauté 3. 82
Figure 5. 4. Organigramme de la recherche du ''node-agent''. 85
Figure 5. 5. Trois cas de Nombre de ''node-agents'' différents. 86
Figure 5. 6. Les Nouveaux nœuds infectés par SSEA pour les différentes valeurs de d pour 100 nœuds. 89

Figure 5. 7. Le nombre total des nœuds infectés par SSEA pour les différentes valeurs de d pour n=100. 89
Figure 5. 8. Les nouveaux nœuds infectés par SSEA pour la sélection de nœuds de valeur d spécifique pour n=100. 91
Figure 5. 9. Le nombre total de nœuds infectés par SSEA pour la sélection de nœuds de valeur d spécifique pour n=100 92
Figure 5. 10. Les nouveaux nœuds infectés par SSEA pour la sélection de nœuds de valeur d spécifique pour n=200. 94
Figure 5. 11. Le nombre total de nœuds infectés par SSEA pour la sélection de nœuds de valeur d spécifique pour n=200 95
Figure 5. 12. Les nouveaux nœuds infectés par SEA pour différentes valeurs de n. 96
Figure 5. 13. Le nombre total de nœuds infectés par SEA pour différentes valeurs de n. 96
Figure 5. 14. Comparaison de SSEA et Gossip[18]. 104

Liste des Tableaux

Chapitre 01: Etat de l'art de l'Internet Of Things

Tableau1. 1. Tableau récapitulatif des technologies WPAN 14
Tableau1. 2. Tableau récapitulatif des normes 802.11 15

Chapitre 05: Le Modèle IOT-PSN

Tableau 5. 1 Nombre de nœuds coopératifs de différentes valeurs de d 90
Tableau 5. 2 Performance selon la variation du nombre total de nœuds par SSEA 93
Tableau 5. 3 Performance selon la variation du nombre total de nœuds par SEA 97
Tableau 5. 4 Variation de ''rounds'' d'infection selon d et t_1 98
Tableau 5. 5 Décalage de temps d'infection de SSEA par rapport à SEA 98
Tableau 5. 6 Décalage de temps d'infection de SSEA par rapport à SEA pour t_1=1/200(round) 98
Tableau 5. 7 Décalage de temps d'infection de SSEA par rapport à SEA pour t_1=1/100(round) 99
Tableau 5. 8 Décalage de temps d'infection de SSEA par rapport à SEA pour t_1=1/50(round) 99
Tableau 5. 9 Décalage de temps d'infection de SSEA par rapport à SEA pour t_1=1/20(round) 100
Tableau 5. 10 Décalage de temps d'infection de SSEA par rapport à SEA pour t_1=1/10(round) 100
Tableau 5. 11 Performance de GOSSIP[18] 101
Tableau 5. 12 Comparaison SEA et GOSSIP[18] 102
Tableau 5. 13 Comparaison de SSEA (d =1) et GOSSIP[18] 102
Tableau 5. 14 Comparaison de SSEA (d =0.75) et GOSSIP[18] 103
Tableau 5. 15 Comparaison de SSEA (d =0.5) et GOSSIP[18] 103
Tableau 5. 16 Comparaison de SSEA (d =0.25) et GOSSIP[18] 103

Liste des acronymes

API: Application Programmable Interface.
BT: BlueTooth.
BDA: Bernoulli Deployment Algorithm.
BLE: Bluetooth Low Energy.
B-MAC: Berkeley Media Access Control.
CSPM: Conditional Social Pressure Metric.
CRP-IdO: Cluster des Projets européens de Recherche sur l'Internet des Objets.
CSMA/CA: Carrier Sense Multiple Access/Collision Avoidance.
CDMA: Code Division Multiple Access.
CIWA: Chinese Industrial Wireless Alliance.
CoAP: Constrained Application Protocol.
CAN: Convertisseur Analogique Numérique.
CNA : Convertisseur Numérique Analogique.
CCA: Clear Channel Assessment.
CEDM-DR: Combined Energy and Distance Metrics Dynamic Routing.
CPEQ: Cluster-based Periodic, Even-driven, Query-based.
DOS: Denial Of Service.
DDOS: Distributed Denial Of Service.
DSN: Distributed Sensor Network.
DSP: Digital Signal Processing.
DTN: Delay Tolerant Network.
DSMAC: Distributed Scheduling Media Access Control.
EAR: Energy and Activity Aware Routing.
EAS: Electronic Article Surveillance.
EC: Extended Coverage.
eMTC: enhanced Machine Type Communication.
EPCWH: Energy Efficient Phone to phone Communication Method Based On Wifi Hotspot.
GPRS: General Packet Radio Service.
GSM: Global System for Mobile.
HMSaW: Human-Mobility Based Spray and Wait.
HTTP: HyperText Transfer Protocol.
HERO: HomE based Relay selectiOn.
IOT : Internet Of Things.
ICMANET: Intermittently Connected Mobile Ad hoc Network.
IBSG: Internet Business Solutions Group.
ISO: International Organization for Standardization
IEC: International Electrotechnical Commission.
IETF: Internet Engineering Task Force.
IEEE: Institute of Electrical and Electronics Engineers.
IAB: internet Architecture Board**.**
ISM: Industrial , Scientific and Medical frequencies band.
ISA: International Society of Automation.
I-PROPHET: IMPROVED PROPHET.
IP: Internet Protocol.

KAT mobility: K-mean And TSP-based mobility.
k-CDS: k-Connected k-Dominating Set.
LPWAN: Low Power Wide Area Networks
LTE-M: Long-Term Evolution for Machines.
LEACH : Low-Energy Adaptive Clustering Hierarchy.
LESCA: Location-Energy Spectral Clustering Algorithm.
MR-KSCA: Multi-Relay K-way Spectral Clustering Algorithm.
MHCA-SC: Multi-Hop Clustering Algorithm based on Spectral Classification.
MAC: Media Access Control.
M2M: Machine to Machine.
MIT: Massachusetts institute of Technology.
NFC : Near Field Communication.
NB-IOT: NarrowBand Internet Of Things.
NOAA: National Geographic and Atmospheric Administration.
OASIS: Organization for the Advancement of Structured Information Standards.
OFDMA: Orthogonal Frequency Division Multiple Access.
OSI : Open Systems Interconnection.
PSN: Pocket Switched Network.
PFDA: Potential Field Deployment Algorithm.
PEQ: Periodic, Even-driven, Query-based.
PROPHET: Probabilistic ROuting Protocol using History of Encounter and Transitivity.
PNGP: Popular Node Gateway Protocol.
QoS: Quality of Service.
UIT: Union Internationale des Télécommunications.
UDP: User Datagram Protocol.
RTP: Report.
RSA: Routage Sans Agrégation.
RAP: Routage Agrégation Partielle.
RAT: Routage Agrégation Totale.
RFID: Radio Frequency Identification.
RTSR: Real-time Transient Social Relationship.
S-MAC: Sensor Media Access Control.
SCF: Store-Carry-Forward.
SEA: Simple Epidemic Algorithm.
SSEA: Secure Simple Epidemic Algorithm.
SPM: Social Pressure Metric.
SANE: Social Aware Networking.
SI: Social Interests.
SP: Social Profile.
T-MAC: Timeout Media Access Control.
TSP: Transit Signal Priority.
TDMA: Time Division Multiple Access.
TEEN: Threshold sensitive Energy Efficient sensor Network.
TSCH: Time Slotted Channel Hopping.
TCP: Transmission Control Protocol.
TTL: Time To Live.

TSR: Transient Social Relationship.
VCO : Voltage-Controlled Oscillator.
VFA : Virtual Force Algorithm.
VTRP: Variable Transmission Range Protocol.
WPAN: Wireless Personal Area Networks.
WLAN: Wireless Local Area Networks.
WIA-PA: Wireless Networks for Industrial Automation –Process Automation.
WirelessHART: Wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol.
WSN: Wireless Sensors Network.
3GPP: 3 rd Generation Partnership project.
6LoWPAN: IPV6 over Low-power Wireless Personal Area Networks.

Introduction Générale

Les réseaux de capteurs sans fil (Wireless Sensors Networks : WSN) sont la fusion de deux pôles de l'informatique moderne: les systèmes embarqués et les communications sans fil. Un WSN est composé d'un ensemble d'unités de traitements embarquées, appelées ‘‘motes’’, communiquant via des liens sans fil. Le but général d'un WSN est la collecte d'un ensemble de paramètres de l'environnement entourant les ‘‘motes’’, telles que la température ou la pression de l'atmosphère, afin de les acheminer vers des points de traitement. Les WSN sont souvent considérés comme étant les successeurs des réseaux Ad Hoc, partageant ainsi plusieurs propriétés telles que l'absence d'infrastructure et la communication sans fil [1].

De nos jours l'utilisation des Smartphones s'élargie de plus en plus. Ces Smartphones sont souvent utilisés comme des points d'accès à l'Internet permettant ainsi le contrôle et la commande des instruments à distance ou même contrôler tout un organisme (les smart house). Les Smartphones sont dotés souvent de capteurs, Ils peuvent servir comme carte de paiement ou de transport ou même une carte d'accès via la technologie NFC (Near Field Communication). Un Smartphone peut aussi mesurer les battements du cœur ainsi que le taux d'oxygène dans le corps d'une personne. De cette définition analogue à celle des WSN, un ensemble de population doté de leurs Smartphones peut former un WSN.

Le pionnier britannique de la technologie Kevin Ashton a été le premier à utiliser le terme populaire Internet Of Things (IOT) en 1999. Il s'agit d'un réseau d'objets connectés au réseau Internet via des capteurs [2]. Chacun a une adresse IP (Internet Protocol) [3-4]. Plus tard, plusieurs définitions sont apparues. Pour William M. [5], c'est une philosophie sans description unique ni universelle. D'après Ruiz M. [6] et Jessa L. [7], IOT est une compilation de toutes les technologies de communication existantes en interaction avec les réseaux Internet. Plusieurs études de convergence entre l'IOT et WSN existent [8].

La technologie Pocket Switched Network (PSN) est une technologie descendante de la technologie DTN (Delay Tolerant Network) adaptée pour les réseaux mobiles ad hoc connectés par intermittence (ICMANET : Intermittently Connected Mobile Ad hoc Network). C'est une technique qui assure le lien quand la liaison bout en bout est corrompue. PSN utilise les

personnes (téléphone mobile) pour assurer l'acheminement de l'information. Cette technique fonctionne sans aucune aide et sans aucune structure spécifique qui la rend une technique plus adaptée aux réseaux ICMANET. Avec PSN, la transmission se fait sous forme de modèle Store-Carry-Forward (SCF) [9]. Le téléphone mobile sert de support de stockage des messages, le mouvement des personnes est pour les transporter. Des liaisons radio à courte portée [10-11] pour les transmettre. L'ultrason [12-13], le Bluetooth et le WIFI [14-15] font partie des technologies de transmission adaptées.

Le passage par les précédents paragraphes nous approche vers la définition d'une nouvelle structure des WSN. Dans cette définition, les nœuds sont les Smartphones assurant ainsi le maintien de connectivité entre eux même en absence de l'internet.

Comme les WSN sont pièce maîtresse du succès de l'IOT [16], alors cette approche est aussi incluse sous la définition d'un nouveau modèle d'IOT où les nœuds sont des personnes dotés de leurs Smartphones et la communication se fait via la technologie PSN. L'intérêt de ce modèle est de trouver des nœuds coopératifs lors d'absence de la connexion internet afin d'assurer l'envoi de l'information à la destination désirée via les réseaux de communication disponibles. Ce modèle peut servir comme exemple de villes intelligentes qui ne sont d'autre que des WSN hétérogènes. L'application de PSN pour les WSN, permet d'assurer le lien vers la station de base lorsque les chemins directs sont corrompus.

Le modèle est défini par les éléments suivants:

• La topologie du modèle : L'environnement est divisé en communautés et un ‘‘EXTERNAL’’. Chaque communauté est un petit réseau IOT local. ‘‘EXTERNAL’’ est un réseau IOT externe. À l'intérieur des communautés, chaque nœud (personne) se comporte comme un périphérique de réseau local. En ‘‘EXTERNAL’’, il devra conserver cette identité et sera également membre du réseau social Ad Hoc.

• Le paramètre degré de sécurité *d* : Dans ce modèle, ‘‘Humain’’ et ‘‘Objet’’ ont une relation commune quand ils appartiennent à la même famille ou à la même usine ou institution. Être souvent au même endroit à la même heure peut être une relation. Par conséquent, chaque nœud peut appartenir à plusieurs communautés. Cette multi-appartenance définit le paramètre de degré

de sécurité *d*. Ainsi, chaque nœud est doté d'un vecteur d'identité qui permet le calcul de la valeur *d*.

• La technologie PSN : En ‘‘EXTERNAL’’, lorsqu'un nœud perd une connexion Internet, il bascule vers la technologie PSN pour garder un lien avec sa communauté via d'autres nœuds. PSN traite et prend en charge tous les types d'articles IOT en l'absence de connexion Internet. C'est l'une des technologies utilisées pour découvrir et ajouter de nouveaux objets aux réseaux d'IOT existants [9]. L'algorithme d'épidémie simple (SEA : Simple Epidemic Algorithm) [17-18] est l'un des protocoles de routage adopté par la technologie PSN. A ce niveau on a proposé un SSEA (Secure Simple Epidemic Algorithm). Ce dernier est le SEA à qui on a ajouté une condition de la livraison de l'information paramétrée par le degré de sécurité *d*.

• La Coopération des nœuds : Puisque le PSN est basé sur le mouvement des personnes pour livrer l'information ; elle compte sur leur coopération pour établir des liens. On va traiter la communication entre les personnes (téléphones portables). Les éléments qui définissent la coopération de chaque nœud sont le niveau de batterie, la charge et la disponibilité. Un nœud disponible avec un niveau de batterie élevé et une charge élevée sera un excellent nœud coopératif.

Dans cette thèse, on exploitera notre modèle développé autour de la stratégie assurant une diffusion de messages sécurisés et de manière optimale, se basant sur une nouvelle reconfiguration de l'algorithme SEA (SSEA). La considération de communautés liées par des paramètres dédiés concoure à la production d'un mécanisme fonctionnel sur lequel on effectuera un ensemble de tests afin de déterminer la technique à adopter pour une large diffusion de messages émanant des IOT du futur. Cette dernière opération concernera inévitablement l'optimisation de l'énergie, la sécurité de messages, le transfert facilité de messages ainsi que l'aptitude à étendre le réseau produit sans ajout de contraintes limitatives. La validation de notre modèle est exclusivement par simulation.

Organisation du document

Le premier chapitre constitue l'état de l'art de l'IOT, où les différentes définitions et approches sont discutées ainsi que les différents standards de communication supportant l'IOT. Un deuxième est dédié à la description des réseaux WSN, ses différentes topologies, ses différents

types, ses différentes applications ainsi que les standards de communication utilisés par les WSN afin d'aboutir à une convergence entre l'IOT et les WSN.

On a réservé le troisième chapitre pour seulement la gestion optimale des WSN, où on a discuté l'influence de déploiement des nœuds sur la gestion des WSN, la consommation énergétique et son impact sur la durée de vie du réseau, l'agrégation des données et leur sécurisation, la tolérance aux pannes…etc.

Le Quatrième chapitre est conçu pour la technologie PSN. Dans ce chapitre on va donner un historique sur l'apparition de PSN, son développement ainsi que leur domaine d'application. On a aussi cité les différents algorithmes et protocoles de communication dédiés à cette technologie, tel que SEA (Secure Epidemic Algorithm) sur lequel est ajoutée une condition de sécurité pour la propagation de l'information afin de l'adopter à notre modèle d'IOT définis.

Un cinquième chapitre décrit notre contribution. Dans ce chapitre, on a commencé par décrire la topologie du modèle d'IOT proposé. On a aussi expliqué l'algorithme dit Secure Simple Epidemic Algorithm (SSEA) définis pour la technologie PSN. Ensuite, la simulation du modèle est présentée. Dans cette partie on a effectué une comparaison du SSEA avec l'algorithme Simple Epidemic Algorithm (SEA) définis dans les littératures afin de prouver l'efficacité et l'amélioration des mesures apportées par SSEA. Des comparaisons de SSEA avec des travaux similaires [18] sont aussi effectuées afin de confirmer l'efficacité de SSEA et du modèle proposé.

Enfin, on termine par une conclusion qui résume et discute les résultats des travaux réalisés. Quelques perspectives pour l'amélioration de la technique proposée sont citées.

Chapitre 01

Chapitre 01: Etat de l'art de l'Internet Of Things

1.1. Introduction

Plusieurs disciplines et plusieurs approches sont envisagées pour l'internet d'objet (Internet Of Things). Ce qui la rend sans définition précise. Le premier qui a utilisé le terme Internet Of Things (IOT) en 1999 est Kevin Ashton pour décrire les micropuces d'identification par radiofréquence (RFID). Depuis, l'IOT [19] n'a cessé de connaître une forte croissance. D'après une étude effectuée par une équipe de recherche de l'école polytechnique fédérale de Zurich (ETH Zurich), en dix ans, soit de 2015 à 2025, 150 milliards d'objets devraient se connecter entre eux, avec l'Internet et avec plusieurs milliards de personnes [20]; ce qui engendre une énorme quantité de données à gérer et à stocker [8]. Selon le groupe Cisco Internet Business Solutions (IBSG), l'IOT est né entre 2008 et 2009, au moment où plus de choses (ou d'objets) étaient connectés à Internet que de personnes.

La première application IOT est née à l'université de Cambridge en 1991; Il s'agissait d'une caméra pointée sur une cafetière et connectée au réseau local de l'université. Alors chaque informaticien pouvait connaitre la disponibilité de café depuis son écran.

Dans ce qui suit, on donnera les différentes définitions d'IOT, les différentes architectures, ainsi que les défis majeurs face à son adoption, tels que l'interopérabilité et la sécurité.

1.2. Définitions de l'Internet Of Things (IOT)

Plusieurs organismes et plusieurs institutions travaillent sur l'IOT. Cela conduit à une divergence des définitions d'internet d'objets. Pour Nicolas G. [21], une approche de l'IOT ne peut se faire sans la vision globale des enjeux et de l'historique du développement des technologies. Selon Jean-Pierre H. [22], l'IOT n'est pas une technologie mais un ensemble de technologies et elle est vue comme une fédération de réseaux autour de l'Internet (figure 1.1). D'après Guillaume G. [23], l'IOT est l'interconnexion de capteurs et d'actionneurs permettant de partager des informations à travers des plateformes via un cadre unifié, en développant une image opérationnelle commune pour permettre le développement d'applications innovantes. Selon Hend Ben H. [24], l'IOT est comme la convergence de tous les réseaux de communication sans fil.

On va ici citer quelques définitions d'IOT attribuées par les organismes les plus connues dans ce domaine.

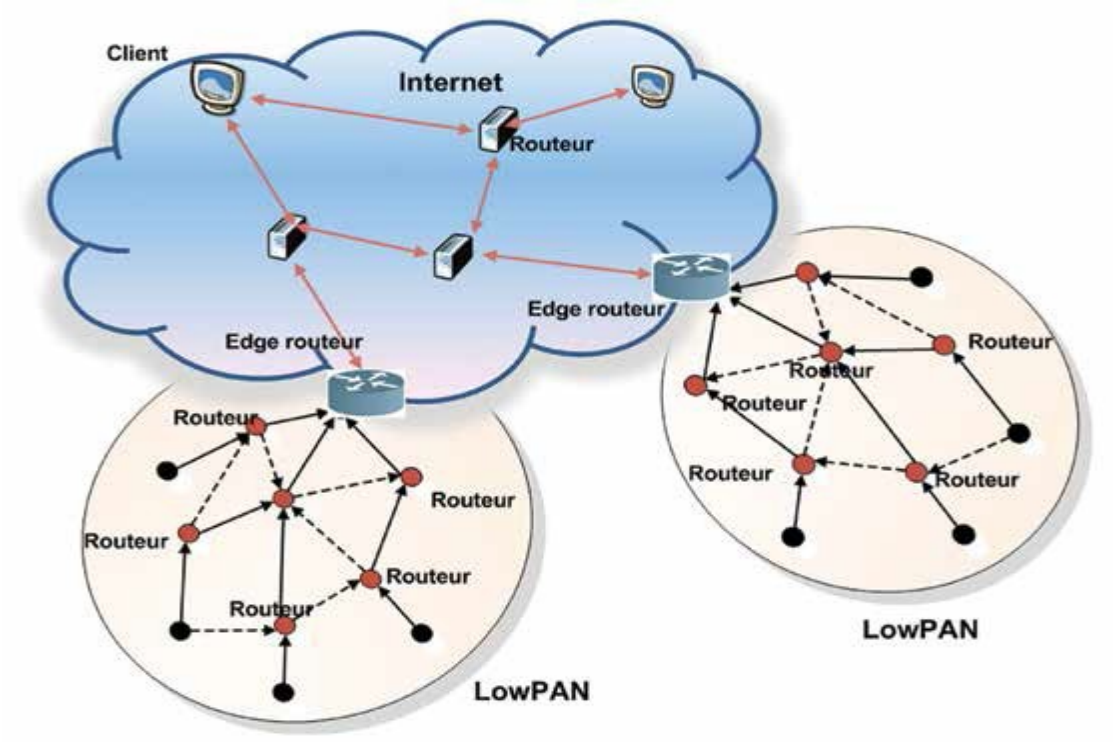


Figure 1. 1. L'IOT vue comme une fédération de réseaux autour de l'Internet [22].

1.2.1. Définition de ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)

Il s'agit d'une infrastructure d'objets, personnes, systèmes et ressources d'information interconnectées associés avec des services intelligents pour leur permettre d'analyser l'information provenant du monde physique et du monde virtuel afin de s'inter-réagir selon la situation adéquate [24].

1.2.2. Définition de l'UIT (Union Internationale des Télécommunications)

C'est une infrastructure mondiale pour la société de l'information qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution [25].

1.2.3. Définition de l'IETF (Internet Engineering Task Force)

L'IOT fait référence aux appareils, souvent de capacités limitées en communication, qui sont devenus de plus en plus connectés à Internet, et à divers services et autres exigences additionnelles répondant aux capacités maximales de ces appareils. L'objectif de ce développement est donc d'aboutir à une communication de machine à machine via Internet sans aucune intervention humaine [24].

1.2.4. Définition de l'IEEE (Institute of Electrical and Electronics Engineers)

L'IOT envisage une auto-configuration, c'est un réseau adaptatif et complexe qui interconnecte les objets à l'internet grâce à l'utilisation de protocoles de communication standards. Les objets interconnectés ont des identificateurs uniques, des propriétés physiques ou virtuelles représentées dans le monde numérique, une capacité de détection/actionnement, et une fonction de programmabilité. Cette représentation contient des informations y compris l'identité, le statut, l'emplacement de l'objet ou tout autres informations commerciales, sociales ou privées pertinentes. Les objets offrent des services, avec ou sans intervention humaine, à travers l'exploitation de l'identificateur unique, la saisie de données et la capacité de communication et d'actionnement [24].

1.2.5. Définition de la CRP-IdO (Cluster des Projets européens de Recherche sur l'Internet des Objets)

CRP-IdO définit l'IOT comme une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente [27].

1.2.6. Définition de l'OASIS (Organization for the Advancement of Structured Information Standards)

L'OASIS est sans but lucratif qui oriente les développements et l'adoption de standards ouverts pour la société de l'information. Les travaux de ce consortium sur l'internet des objets portent sur les technologies de réseau et de messagerie normalisées [28-29]. Alors, elle définit les architectures basées sur le ''Cloud'' utilisant des protocoles communs facilitant ainsi l'interconnectivité [29].

L'intérêt commun et important de l'ensemble de ces organismes est de définir une norme qui rendra l'IOT plus efficace, plus sûr, résilient et beaucoup plus sécurisé.

1.3. Les architectures d'IOT

Une architecture de référence de l'IOT permet d'uniformiser la conception des systèmes et favorise l'interopérabilité et la communication entre les différents écosystèmes d'IOT [26].

En mars 2015, le comité Internet Architecture Board (IAB) propose quatre modèles communs d'interactions entre des acteurs de l'IOT [26]:

-La communication entre objets, ce modèle est basé sur une communication sans-fil entre deux objets. Les informations sont transmises grâce à l'intégration d'une technologie de communication sans-fil telle que ZigBee ou Bluetooth, etc.

- La communication des objets vers le ''Cloud'' dans ce modèle, les données collectées par les capteurs sont envoyées à des plateformes de services via un réseau.

- La communication des objets vers une passerelle, ce modèle est basé sur un intermédiaire qui fait le lien entre les capteurs et les applications dans ''le Cloud ''.

- Des objets au partage des données en ''Back-End'', l'objectif de ce modèle permet le partage des données entre les fournisseurs de services. Il est basé sur le concept ''web programmable''. Les fabricants mettent en place une API (Une Application Programmable Interface) permettant l'exploitation des données agrégées par d'autres fabricants.

1.4. L'IOT et les réseaux de communication sans fil

La plupart des objets communicants fournissent leurs services sur un réseau local, industriel ou personnel [21]. Plusieurs réseaux existent bien avant l'apparition de l'IOT. Les WPAN (Wireless Personal Area Networks), les WLAN (Wireless Local Area Networks), et les LPWAN (Low Power Wide Area Networks) dérivés de la classification de l'IEEE [22] sont des réseaux sur lesquels appuis l'IOT.

1.4.1. Les WPAN (Wireless Personal Area Networks)

Ils sont des réseaux à faible portée (inferieure à 100 m). Ces réseaux ont des débits relativement faibles. Pour les technologies sans-fil, seules les bandes de fréquences utilisables en Europe sont indiquées. Par exemple, la bande de fréquences Industrielles, Scientifiques et

Médicales (ISM) 915 MHz n'est disponible qu'aux États-Unis. Son équivalent européen est la bande de fréquences ISM 868 MHz [30].

1.4.1.1. Radio Frequency IDentification [30,31]

Radio Frequency Identification (RFID) est une méthode de stockage de données et de communication sans fil. Un système RFID se compose à minima d'un lecteur et d'une radio-étiquette (ou tag RFID). Cette radio-étiquette est généralement composée d'une puce et d'une antenne. RFID utilise un ensemble de bandes de fréquences (125 kHz, 13,56 MHz, 433 MHz, 865-868 MHz, 2,45-5,8 GHz et 3,1-10 GHz). Le débit disponible augmente en fonction de la fréquence. La RFID supporte 3 types de fonctionnements : actif, semi-actif et passif.

*****En mode passif, le tag utilise l'énergie de l'onde émise par le lecteur comme alimentation. Il n'utilise pas de batteries.

*****Les tags semi-actifs utilisent l'énergie de l'onde émise par le lecteur uniquement pour générer la réponse à la requête du lecteur. La puce est alimentée par une alimentation auxiliaire.

*****Les tags actifs fonctionnent uniquement grâce à une source d'énergie auxiliaire. Les tags actifs offrent une meilleure portée ainsi qu'une plus grande capacité de mémoire.

La figure 1.2 montre quelques normes de RFID ainsi que leur utilisation. Par exemple, la norme ISO/IEC 14443 sert de support pour la technologie NFC (Near Field Communication). EAS signifie Electronic Article Surveillance (Applicable pour les antivols présents en magasin).

La figure 1.3 montre l'évolution des tags, en termes de surface de mémoire. Une des faiblesses de technologies RFID concerne l'attaque par relais [33]. Il existe aussi la possibilité de ‘‘rejeu’’, de déni de service, d'usurpation, de clonage, d'écoute... [34,35].

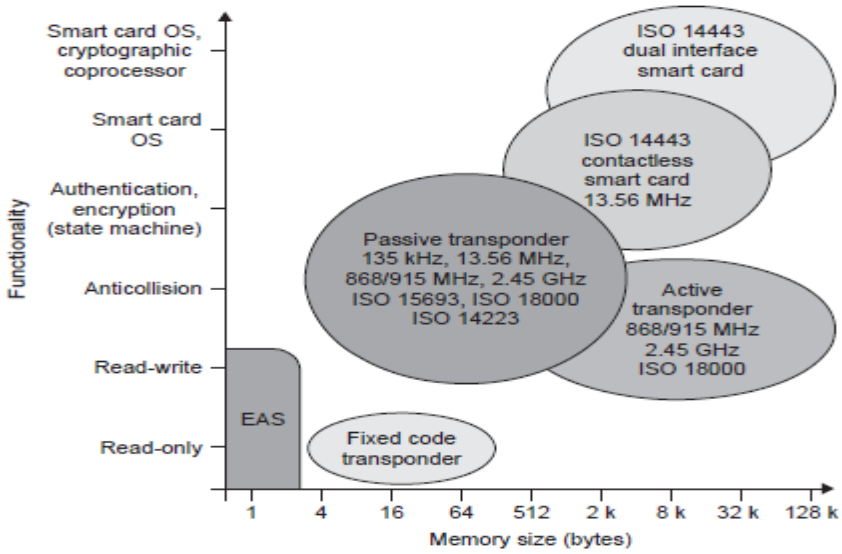


Figure 1. 2. Technologies RFID : fonctionnalités en fonction de la capacité mémoire [31,32].

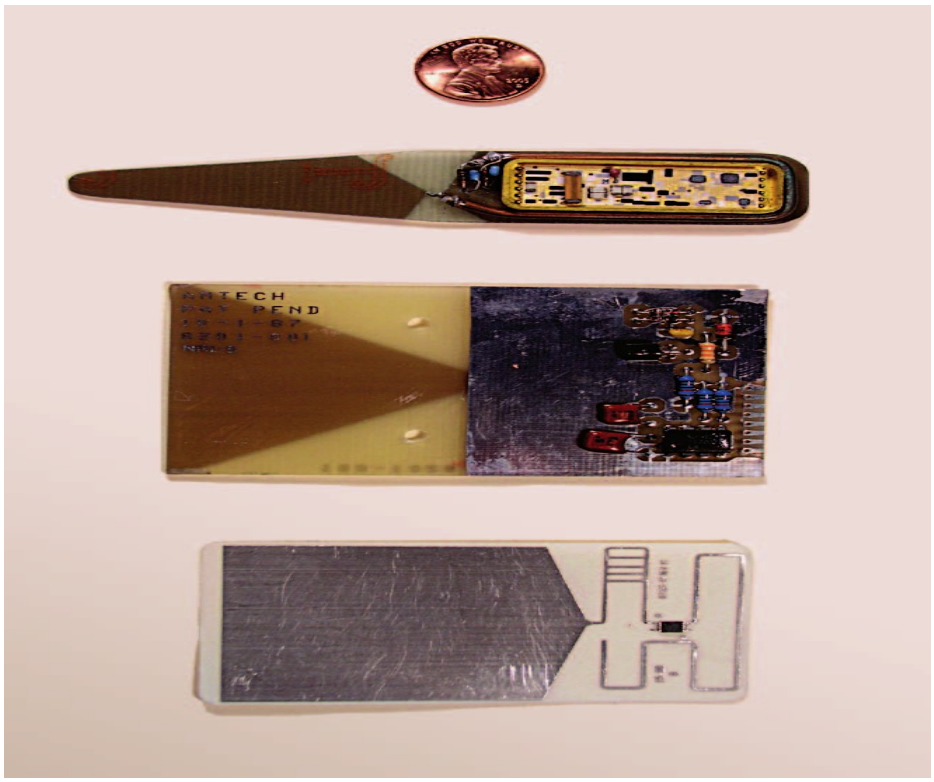


Figure 1. 3. Evolution des tags RFID, de haut en bas : un tag en lecture seule 12 bits, 1976 ; un tag en lecture seule de 128 bits, 1987 ; un tag en lecture écriture de 1024 bits, 1999 [32].

1.4.1.2. Z-Wave

Z-Wave est un protocole réseau sans-fil développé par Zensys, en 2001. Zensys est une société danoise qui a été rachetée par la société américaine Sigma Designs en 2008. Pour Z-Wave, qui est une technologie propriétaire. Ce protocole a été développé principalement pour une application domotique. Z-Wave fonctionne sur les bandes de fréquences 868 MHz et 2,4 GHz [36]. Le débit peut atteindre 200 kbit/s. La portée est de 30 m en intérieur et 100 m en extérieur [37]. Une dernière révision s'appelle Z-Wave+, entièrement rétrocompatible avec Z-Wave.

1.4.1.3. IEEE 802.15.4

IEEE 802.15.4 est un protocole de communication sans-fil standardisé par IEEE en 2003. Les amendements g [38], k [39] et leurs dérivés sont avec des portées de l'ordre du kilomètre, ils s'apparentent aux technologies à faible consommation et à grande portée (LWPAN) et sont donc distincts des technologies WPAN.

Le standard IEEE 802.15.4 définit la couche physique et liaison. IEEE 802.15.4 fonctionne sur les bandes de fréquences ISM 868 MHz et 2,4 GHz. La portée maximale est de 100 m. Le débit maximal est de 250 kbit/s. Il dépend de la technique d'étalement du spectre. IEEE 802.15.4 dispose de deux systèmes d'adressage différents. Le premier système est statique, sur 64 bits, le deuxième est un adressage dynamique sur 32 bits [40].

IEEE 802.15.4 définit plusieurs modes d'accès. Le premier est opportuniste avec évitement de collision CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Alternativement, il peut aussi utiliser des balises de synchronisation. Il dispose aussi d'un créneau de communication garantie [40]. Dans ce cas, le mode d'accès s'apparente au TDMA(Time Division Multiple Access). En 2012, l'amendement IEEE 802.15.4e apporte des améliorations à la couche liaison [41]. Il apporte notamment le mode TSCH (Time Slotted Channel Hopping). Il s'agit d'un fonctionnement proche du TDMA couplé à du multi-canal et du saut de fréquences. Les technologies utilisant IEEE 802.15.4 sont:

- ✓ Le **6LoWPAN (**IPv6 over Low-Power Wireless Personal Area Networks) : Il permet l'utilisation de l'IPv6 sur IEEE 802.15.4 [42,43].
- ✓ **WIA-PA** (Wireless Networks for Industrial Automation–Process Automation**):** est un protocole réseau sans-fil, développé par la Chinese Industrial Wireless Alliance (CIWA)

et approuvé en 2007 [44]. Puis standardisé en 2011 par l'IEC (International Electrotechnical Commission) sous la norme IEC 62601.

- ✓ **ISA100.11a :** est une pile technologique réseau sans-fil développée par l'International Society of Automation (ISA) en 2009. En 2010, ISA100.11a a été standardisé par l'IEC sous le nom d'IEC 62734. ISA100.11a s'appuie sur la couche physique et la partie inférieure de la couche liaison (la couche MAC) d'IEEE 802.15.4 [45].
- ✓ **WirelessHART (wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol (HART)):** est une pile technologique de réseau sans-fil développée par HART publiée en 2007 [46]. Il est standardisé comme IEC 62591 en 2010, et reprend la couche physique d'IEEE 802.15.4 ainsi que la partie inférieure de la couche liaison (couche MAC).
- ✓ **ZigBee :** ZigBee est une pile technologique réseau sans-fil destinée à la domotique. Elle est conçue par ZigBee Alliance. ZigBee a été développé en 1998 et finalisé en 2004. Il est à l'origine de la norme IEEE 802.15.4 [47]. La pile est complétée par une couche réseau et application spécifiée dans ZigBee 1.0. Des révisions ont été apportées afin de rendre ZigBee utilisable dans d'autres secteurs. ZigBee ne supporte pas IP dans sa spécification initiale. Pour cette raison, deux solutions complémentaires ont été développées : ZigBee Pro et ZigBee IP [48] : ZigBee Pro permet la communication entre le domaine ZigBee et le domaine IP via une passerelle. ZigBee IP inclut le support natif d'IP pour tous les nœuds. Il permet donc HTTP (HyperText Transfer Protocol) sur TCP (Transmission Control Protocol) et optionnellement CoAP (Constrained Application Protocol) sur UDP (User Datagram Protocol). CoAP est un protocole équivalent à HTTP, mais destiné à l'IOT [49]. Pour optimiser l'efficience, il est possible d'utiliser la couche d'adaptation 6LoWPAN. La figure 1.4 résume l'organisation des piles ZigBee Pro et ZigBee IP.

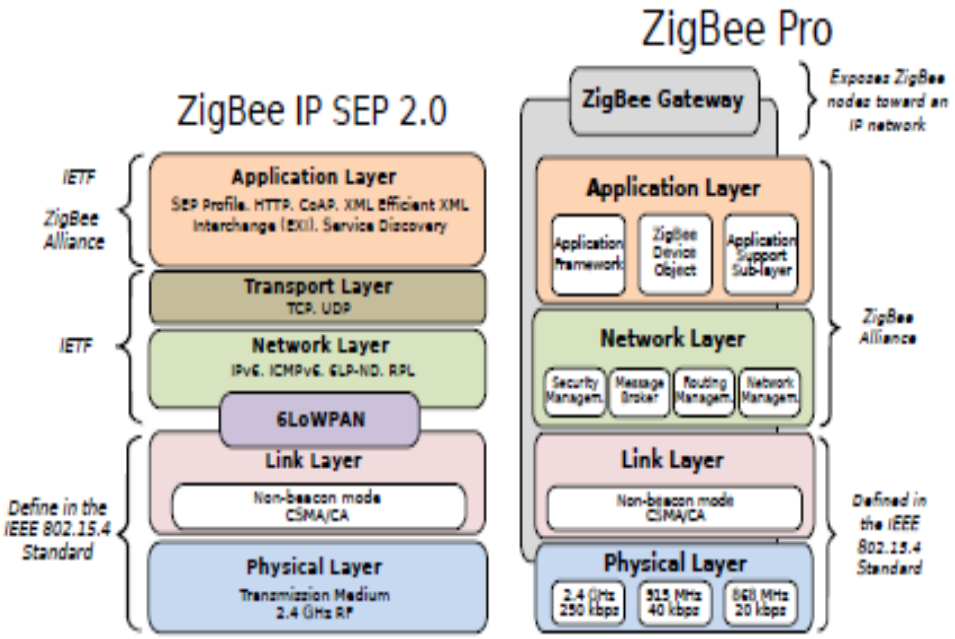


Figure 1. 4. Piles technologiques ZigBee IP 2006 et ZigBee Pro 2007 [48].

1.4.1.4 Bluetooth

Bluetooth (BT) est une pile technologique pour les réseaux sans-fil. Bluetooth a été créé par l'entreprise suédoise Ericsson en 1994. Il est maintenant maintenu par Bluetooth Special Interest Group. Les versions 1.1 et 1.2 ont été normalisées sous le nom IEEE 802.15.1 [47]. La standardisation IEEE n'est plus maintenue. La cinquième et la dernière version est publiée en 2016. Bluetooth utilise la bande de fréquences ISM 2,4 GHz. La portée maximale est de 200 m pour la version 5, et 100 m pour les versions précédentes [50]. Le débit maximal est de 2 Mbit/s en version 5. Une version plus économique a été crée sous le nom Bluetooth Low Energy (BLE) [51]. Cette déclinaison est principalement destinée à l'IOT. Les performances sont plus modestes mais cela permet une durée de vie accrue. D'autres fonctionnalités comme le mode TDMA ont été ajoutées à BLE. Les adresses Bluetooth sont sur 48 bits (adresses MAC) avec une partie dépendante du constructeur.

Le tableau1.1 récapitule les différentes technologies WPAN.

Tableau1. 1. Tableau récapitulatif des technologies WPAN

Technologie	Bandes de fréquences	Débit max.	Portée max.	Méthode de contrôle d'accès
RFID	125 kHz		10 cm	
	13.56 MHz		1 m	
	433 MHz		100 m	
	868KHz		10 m	
Z-Wave	868KHz et 2.4GHz	200 kbits/s	100 m	CSMA
IEEE 802.15.4	868KHz et 2.4GHz	250 kbits/s	100 m	TDMA/CSMA
WIA-PA	2.4GHz	250 kbits/s	100 m	TDMA+CSMA+FDMA
ISA100.11a	2.4GHz	250 kbits/s	100 m	TDMA (+CSMA)
WirelessHART	2.4GHz	250 kbits/s	100 m	TDMA (+CSMA)
Bluetooth 5	2.4GHz	2 Mbits/s	200 m	CSMA/FDMA
Bluetooth LE	2.4GHz	1 Mbits/s	100 m	TDMA/FDMA

1.4.2. WLAN (Wireless Local Area Network)

Dans cette catégorie, il n'existe pour le moment qu'une seule famille des normes IEEE 802.11. IEEE 802.11 a été standardisé par l'IEEE en 1997. Il définit à la fois la couche physique et la couche liaison [52]. La norme IEEE 802.11-1997 fonctionnait sur la bande de fréquences ISM 2,4 GHz [53]. En 1999, la norme IEEE 802.11-1997 prend le nom Wi-Fi (ou wifi : Wireless Fidelity) une marque détenu par Wi-Fi Alliance. Le débit était de 2 Mbit/s. En pratique, cette norme a été très peu utilisée.

La deuxième version d'IEEE 802.11 (IEEE 802.11a) fonctionne sur la bande de fréquences ISM 5 GHz [54]. Son débit maximum théorique est de 54 Mbit/s, ce qui la rend nettement plus intéressante que la version précédente. Le tableau 1.2 résume les informations essentielles sur les différentes normes IEEE 802.11.

Ce standard utilise des adresses sur 48 bits (adresses MAC), dépendantes du constructeur. IEEE 802.11 supporte différentes topologies. IEEE 802.11 peut fonctionner au mode ad-hoc. IEEE 802.11 fonctionne en mode CSMA/CA puis une variante à partir IEEE 802.11e [55]. En 2017, Cheng et al. [56] proposent d'utiliser le fonctionnement TDMA au lieu du CSMA/CA. Le fonctionnement TDMA permet une amélioration des performances en multi-saut. Pour la version améliorée IEEE 802.11ax-2019, Boris B. [57] propose l'utilisation de l'OFDMA (Orthogonal Frequency Division Multiple Access) afin de permettre la transmission en parallèle.

IEEE 802.11af [58], contrairement au Wi-Fi fonctionnant uniquement sur les bandes de fréquences non-licenciées ISM (Industriel, Scientifique et Médical) ; IEEE 802.11af est une norme un peu particulière. Elle fonctionne entre 470 MHz et 710 MHz, c'est à dire une bande de fréquences réservée à la diffusion télévisuelle. IEEE 802.11af utilise donc la radio cognitive pour

récupérer des bandes de fréquences inutilisées. Le débit est dépendant de l'utilisation du spectre (Non supérieurs à 12 Mbit/s) [59]. Sa portée peut atteindre quelques kilomètres.

IEEE 802.11ah est la norme destinée à l'IOT et aux M2M (Machine to Machine) [60,61]. Elle porte le nom commercial de Wi-Fi Halow. Le débit est volontairement plus faible afin d'augmenter la durée de vie des batteries sur équipements. Sa portée permet d'avoir une solution intermédiaire pour la transition vers les réseaux cellulaires.

Tableau1. 2. Tableau récapitulatif des normes 802.11

Normes	Année	Bande de fréquences	Débit théorique max. (Mbits/s)	Portée (m)
IEEE 802.11-1997	1997	2.4 GHz	2	100
IEEE 802.11a	1999	5 GHz	54	120
IEEE 802.11b	1999	2.4 GHz	11	140
IEEE 802.11g	2003	2.4 GHz	54	140
IEEE 802.11n	2009	2.4 GHz et 5 GHz	600	250
IEEE 802.11ad	2012	60 GHz	6757	10
IEEE 802.11ac	2013	5 GHz	3466,8	35
IEEE 802.11af	2013	470 MHz-710 MHz	12	qq km
IEEE 802.11ah	2016	868 MHz	8	1000
IEEE 802.11ax	2019	2.4 GHz et 5 GHz	NC	NC

1.4.3. Les LPWAN (Low Power Wide Area Networks) [22]

Le Wi-Fi Halow constitue une transition vers les réseaux LPWAN (Low Power Wide Area Networks). Le champ d'application visé est celui des réseaux de capteurs et plus généralement celui de l'Internet des objets. Apparus à partir de l'année 2015 afin de réaliser à faible coût, sur de grandes distances, des réseaux de capteurs alimentés par batterie. Ce sont donc des réseaux à faible débit qui permet de gérer avec une qualité de service acceptable des budgets de liaisons allant jusqu'à 160 dBm (decibels per milliwatt). Deux solutions d'origine française reconnus au niveau mondial, y compris aux Etats-Unis sont LoRa et SIGFOX:

LoRa, solution ouverte fondée sur le protocole LoRaWAN promu par la LoRa Alliance. LoRa est un réseau étoile bas débit, fonctionnant en France dans la bande des 868 MHz, utilisant des composants d'une très grande sensibilité et permettant de mettre en connexion, de façon bidirectionnelle, des capteurs distants de plusieurs kilomètres avec un relais servant de gateway qui transfère ensuite les informations, en mode IP, vers l'Internet. LoRa utilise des canaux de 125 kHz en étalement de spectre. Les débits annoncés vont de 300 bit/s à 50 kbit/s (en Europe).

SIGFOX, repose sur un modèle différent. SIGFOX est un opérateur qui, directement ou par l'intermédiaire de partenaires, propose un service de connexion IOT dans le monde entier (en

2016, dans 24 pays). La technologie est également différente : le système SIGFOX utilise une transmission à bande très étroite (Ultra Narrow Band) permettant à un capteur d'envoyer des impulsions très courtes (12 octets de charge utile, au maximum 140 fois par jour) sur des micro-canaux dans la bande des 868 MHz. Les trames sont envoyées trois fois, sur trois fréquences, en direction de toutes les stations de base, sachant que, typiquement, trois d'entre elles pourront les capter, avant d'être récupérées par les serveurs SIGFOX (figure1.5). En "downlink" la charge utile est limitée à 8 octets, quatre fois par jour.

Compte tenu des débits limités (équivalents à environ 100 bit/s), les applications préférentielles sont celles du comptage, de la maintenance préventive, de l'agriculture, de l'environnement, etc.

D'autres initiatives ont vu le jour, simultanément ou avant LoRa et SIGFOX, avec plus ou moins de succès : Qovisio (Opérateur IOT basé à Angers), Neul, Ingenu, Weighless N et P, nWave, etc.

1.4.4. L'IOT et les réseaux cellulaires

Pour les réseaux cellulaires dés la publication du communiqué 13 du 3GPP (3rd Generation Partnership Project), le consortium qui établit et publie les standards de 3e et 4e génération, trois solutions fonctionnant dans des fréquences sous licence se trouvent homologuées:

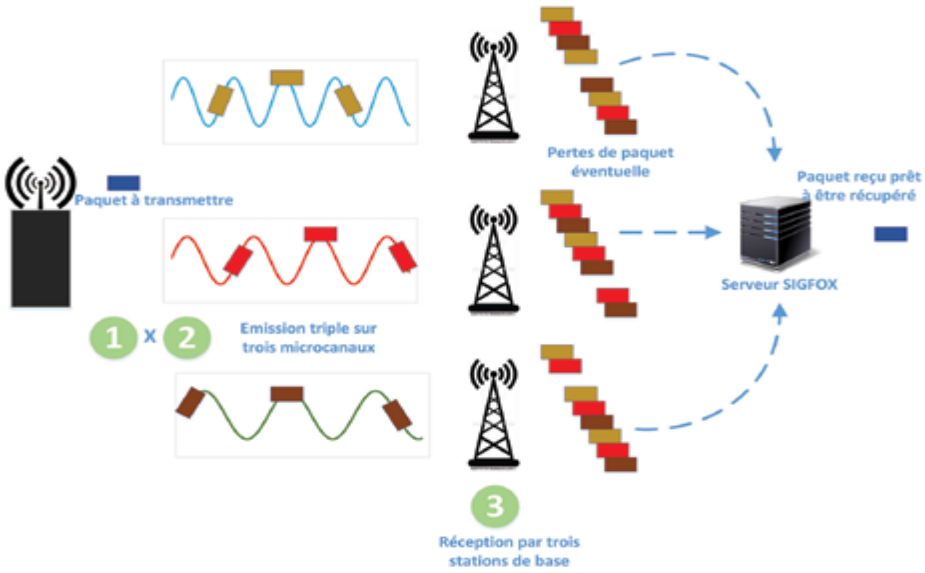


Figure 1. 5. Architecture du système SIGFOX.

1.4.4.1. EC-GSM-IoT (EC : Extended Coverage) [22]

C'est un complément logiciel du GPRS(General Packet Radio Service) permettant d'offrir, grâce à la base installée GSM (Global System for Mobile), des services LPWAN dans des fréquences sub-GHz. EC-GSM-IOT utilise des canaux de 200 kHz en half duplex. Le gain de couverture escompté est de 20 dBm pour un débit de 10 kbit/s.

1.4.4.2. eMTC (enhanced Machine Type Communication) (ou LTE-M) (Long-Term Evolution for Machines) [22]

C'est une extension logicielle de 4G LTE. eMTC requiert un canal de 1,4 MHz (à l'intérieur d'un canal LTE de 20 MHz) et permet des débits de 1 Mbit/s. C'est une solution adaptée au trafic M2M.

1.4.4.3. NB-IOT (stands for Narrowband Internet Of Things)

Il s'agit d'une norme radio développée pour le réseau étendu de faible puissance (LPWAN: low-power wide-area network) afin de prendre en charge les technologies IOT [29]. Elle est intégrée dans LTE (Long-Term Evolution) mais, elle utilise une interface radio spécifique. Elle requiert un canal de 200 kHz et permet des débits de quelques dizaines de kbit/s. Le GPP [62] est le groupe qui réunie l'ensemble des organisations de normalisations télécoms produisant des spécifications pour la communication cellulaire par le biais de NarrowBand IOT (NB-IOT) [63-65].

NB-IOT est conçu pour une couverture en intérieur utilisant un grand nombre d'appareils connectés avec une longue autonomie énergétique. Les principales caractéristiques sont, la faible consommation d'énergie, le coût réduit des composants, et le faible débit de données.

1.5. Les applications de l'IOT

Il existe plusieurs applications d'IOT. Elles peuvent être classées selon leurs domaines d'application. On trouvera IOT dans la domotique, les villes intelligentes, le transport…etc.

1.5.1. La domotique

Cette catégorie regroupe les appareils de contrôle à distance. On trouve comme exemples, Google Home, Nest, Lockitron, Tado, Hue, Goodnightlamp [62-63,69-71].

1.5.2. Environnement intelligent

Cette catégorie regroupe la détection précoce des tremblements, les glissements de terrain et la prévention des avalanches, la surveillance du niveau de neige, la détection des incendies de forêt, la pollution…etc. Insightrobotics [72] est un exemple très démonstratif.

1.5.3. Transport et logistique

Cette catégorie regroupe la détection d'incompatibilité de stockage, le contrôle du suivi des itinéraires pour les marchandises sensibles, l'emplacement des articles, la qualité des conditions d'expédition…etc. Quelques exemples de cette catégorie sont HiKoB, Alltraffic solutions, Cantaloupe Systems, Senseaware, H-IoT platform framework, intelligent identification system of railway logistics by means of the IOT [73-79].

1.5.4. Agriculture intelligente

L'agriculture devient de plus en plus complexe et interconnectée. Cette catégorie regroupe le contrôle de compost, des stations météorologiques, des serres et d'hydroponique. Comme exemples d'application dans ce domaine on trouve OnFarm, Bumblebee ,Hydropoint, et greenhouse-site monitoring [80-83].

1.5.5. Les Villes intelligentes

Cette catégorie regroupe le contrôle des niveaux de champs électromagnétiques, la santé structurelle, la gestion des déchets, la détection de Smartphones, les routes intelligentes, le stationnement intelligent, l'éclairage intelligent, les embouteillages, la cartographie urbaine du bruit…etc. Comme exemples on cite, Streetline, Livehoods, BigBelly Solar, Road Condition Monitoring App, Smart Streets IOT Hub, integrated IOT retractable bollard management system, SmartSantander et M2M Communication Platform for Smart Cities [84-91].

1.5.6. Les compteurs intelligents

Cette catégorie regroupe la mesure de la pression de l'eau dans les systèmes de transport d'eau, des niveaux des réservoirs, le suivi et gestion de la consommation d'énergie [92,93], la mesure du niveau de vide et du poids des marchandises dans les silos et la surveillance et l'optimisation de la performance dans les centrales solaires. Comme titre d'exemples on cite, Echelon, Wattics [94-95].

1.5.7. Sécurité et Urgences

Cette catégorie regroupe les mesures de niveaux de rayonnement, Le contrôle d'accès périmétrique, les gaz explosifs et dangereux .etc. Comme exemples de cette catégorie on trouve, Aircasting, Airqualityegg, Netatmo, et Emergency Management System [96-99].

1.5.8. La Cybersanté

Cette catégorie regroupe le rayonnement ultraviolet, les soins aux sportifs, le suivi des personnes seules, la surveillance des patients, les réfrigérateurs médicaux. Pour ce domaine d'application on trouve, l'Electronic Healthcare Records (EHR), Smart Hospital, pervasive healthcare, L'assistant sportif individuel BioHarness, Le Chal, Le moniteur bébé Mimo, Ubi et L'assistant médical ElectricFoxy [100-108].

1.5.9. Le Contrôle industriel

Dans cette catégorie l'IOT est utilisée pour la mesure de la qualité de l'air intérieur, la surveillance de la température, l'auto-diagnostique du véhicule, la localisation à l'intérieur. Parmi les applications dans cette catégorie on trouve : Yanzi, Engauge, Google Glass, SmartStructures [109-112].

1.5.10. Vente au détail

Cette catégorie regroupe les applications de magasinage intelligentes, le paiement sans contact, la gestion intelligente des produits et le contrôle de la chaîne d'approvisionnement. Une meilleure application pour cette catégorie est Motionloft [113].

1.5.11. Gestion intelligente de l'eau

Cette catégorie regroupe les mesures de niveaux de pollution maritime, la détection de fuite chimique dans les rivières, les inondations, la mesure à distance des piscines, les fuites d'eau, et la surveillance de l'eau potable. Comme application pour cette catégorie on trouve: TDMPAS, Intelligentriver, Shoal, le réseau de capteurs flottants [114-117].

1.6. Les défis face à l'application d'IOT

Les défis majeurs face à cette technologie sont la sécurité et l'interopérabilité entre les objets.

1.6.1. Interopérabilité

L'IOT est caractérisé par une très grande hétérogénéité des dispositifs, des technologies et des protocoles, ce qui nécessite une importante propriété qui est l'interopérabilité afin d'assurer la fiabilité de la communication.

1.6.1.1. Définition

L'interopérabilité est la capacité intrinsèque que possède un système à pouvoir fonctionner avec d'autres systèmes via la définition de ses interfaces. Dans le cadre des télécommunications, c'est plus précisément la capacité des systèmes à pouvoir communiquer avec d'autres systèmes existants ou futurs par la définition d'interfaces de communication [21]. Selon Guillaume G. [23], l'interopérabilité peut être définie selon deux axes:

-l'**interopérabilité syntaxique**: être capable d'utiliser différentes technologies de manière transparente et homogène en intégrant des technologies hétérogènes et incompatibles.

-l'**interopérabilité sémantique**: permettre aux systèmes de comprendre de manière automatique les différentes données produites par des capteurs hétérogènes aux formalismes de données disparates.

1.6.1.2. Les Causes qui empêchent l'interopérabilité

Les principales causes qui empêchent l'interopérabilité sont [21]:

- ✓ Le financement indépendamment des projets et leur concurrence les uns avec les autres.
- ✓ La deuxième raison est que pour avoir une politique globale, il faut une entité spécialisée sur les problématiques d'IOT et ayant comme mission de chercher à mutualiser les ressources, les protocoles, les plateformes, …etc.

1.6.2. La sécurité

La sécurité représente l'ensemble de politiques et pratiques adoptées pour prévenir et surveiller l'accès non autorisé, l'utilisation abusive, la modification ou le refus d'une opération informatique [16].

1.6.2.1. Authentification [16]

L'authentification est le mécanisme de sécurité qui permet de prouver l'identité d'une entité. En effet, il existe plusieurs méthodes d'authentification qu'on peut classer en 4 catégories:

- ✓ L'authentification ''avec ce qu'on sait'', c'est à dire que l'entité prouve son identité avec une information secrète, qui n'est connue que par un nombre limité d'objets légitimes. Généralement le nombre d'objets concernés ne dépasse pas 2 (ex. un client et un serveur). Les mécanismes les plus utilisés dans cette catégorie sont les mots de passe et les numéros personnels d'identité (Personal Identity Number (PIN));
- ✓ L'authentification ''avec ce qu'on possède''. Dans cette catégorie, une entité s'authentifie grâce à une donnée stockée. Cette donnée peut être secrète comme les clés pré-partagées (Pre-Shared Key (PSK)), ou publique comme les certificats numériques et les jetons;
- ✓ L'authentification ''avec ce qu'on est''. Ça concerne généralement les utilisateurs humains, qui ont des caractéristiques biométriques qui leurs sont uniques telles que la voix, l'empreinte digitale, l'iris, et les veines;
- ✓ L'authentification avec comment on se comporte. Cette dernière catégorie est basée sur les profiles comportementaux de chaque utilisateur.

1.6.2.2. Confidentialité

La confidentialité est le mécanisme qui permet de cacher une donnée, et de cacher même l'information de son existence. Ainsi, empêcher toutes entités non autorisées d'avoir accès à cette donnée. Généralement, on assure ce service en utilisant le chiffrement de données. Ce dernier est basé sur des algorithmes mathématiques permettant de déformer un texte en clair est le remettre à sa forme initiale grâce à une ou plusieurs clés cryptographiques. La confidentialité dite de caractéristique cryptographique persistante (forward secrecy) doit garantir que la découverte d'une information secrète (ex. clé privée) d'un objet légitime par un utilisateur malicieux ne compromet pas la confidentialité des communications passées.

1.6.2.3. Intégrité

L'intégrité est un mécanisme assurant qu'une donnée ne soit pas : falsifiée, modifiée, altérée ou supprimée par une entité non autorisée. Dans la plupart des cas, ce service est réalisé en utilisant des fonctions de hachage avec des propriétés de signature de données.

1.6.2.4. Disponibilité

La disponibilité est le mécanisme qui permet de garantir la bonne exécution d'un service et le bon fonctionnement du système. Afin de garantir la disponibilité d'un service, on utilise des mécanismes qui le protègent contre les arrêts intentionnels tels que les attaques de dénis de service et dénis de service distribués (Denial/Distributed Denial of service (Dos/DDos)), et non intentionnels (ex. les erreurs humaines).

1.6.2.5. La Non ''répudiation''

La non répudiation est un mécanisme qui permet de garantir qu'une opération ne peut être niée par celui qui l'avait établi. On garantie ce service grâce aux signatures numériques combinées avec des mécanismes qui assurent le non ''rejeu '' de données.

1.6.2.6. Le Non ''rejeu''

Le non ''rejeu'' est un mécanisme qui permet de garantir qu'un message échangé entre deux entités A et B, ne doit pas être réutilisé par une entité non autorisée C. La plupart des systèmes intègrent des compteurs et des numéros de séquence différents au niveau des messages échangés, ce qui fait qu'un message ne peut pas avoir le même numéro de séquence que ses n messages précédents (n un nombre de message qui varie selon la politique de sécurité utilisée), sinon il sera automatiquement rejeté.

1.6.2.7. La résilience

On peut définir la résilience par la capacité d'un système à surmonter une altération de son environnement. Par exemple dans le cas de l'IOT, si un objet est compromis, cela ne devrait pas influencer l'ensemble du réseau.

1.6.2.8. L'évolutivité

L'évolutivité représente l'aptitude d'un système à maintenir des bonnes performances lorsque des ressources (notamment ressources matérielles) lui sont ajoutées.

1.6.2.9. La tolérance aux pannes

La tolérance aux pannes est un mécanisme permettant à un système de continuer à fonctionner lorsque l'un de ses composants tombe en panne.

1.7. Conclusion

Dans ce chapitre, on a essayé de donner l'ensemble des définitions de l'IOT qui différent selon l'organisme développeur et l'architecture adaptée. On a aussi présenté l'ensemble des réseaux de communication sans fil sur lesquels l'IOT s'appuie dans les différents domaines d'application. Des exemples d'application ont été cités. La conclusion tirée est que l'IOT n'a pas encore une définition standard. Le succès de l'IOT [16] grâce au rapprochement IOT-WSN est présenté dans le deuxième chapitre.

Chapitre 02

Chapitre 02 : L'approche IOT-WSN

2.1. Introduction

L'Internet des Objets repose sur l'interconnexion des objets dotés d'une intelligence propre et d'une identité unique (adressage) et on parle d'objets intelligents ou d'objets connectés tels que les Smartphones. Les objets connectés sont capables de mesurer des phénomènes naturels du monde qui nous entoure, de les convertir en numérique et d'estimer leur valeur. Ainsi, ils nous aident à prendre les décisions adéquates face aux situations qui peuvent dégrader notre confort. Les éléments centraux de l'IOT sont les capteurs qui sont des composants électroniques, de plus en plus miniaturisés. Malgré leurs ressources limitées en mémoire, puissance de calcul et énergie, ils peuvent former un réseau et coopérer entre eux ou avec Internet sous différentes topologies et architectures [118]. Lorsqu'ils communiquent en mode sans fil, on parle de réseaux de capteurs sans fil (RCsF) ou en anglais WSN (Wireless Sensor Networks) [119]. Les réseaux de capteurs sans fil (WSN) ont été reconnus comme une technologie cruciale et habilitante dans le monde de l'Internet des objets (IOT) [120]. Selon Nacer K. [42] les WSN seront une partie intégrante de l'IOT par l'adaptation d'IPV6, ce qui veut dire que chaque nœud sera doté de sa propre adresse IPV6. Dans ce chapitre, On donnera un petit historique sur l'apparition des WSN, leur architecture, les standards de communication adoptés et leur domaine d'application afin de prouver l'approche IOT- WSN.

2.2. Historique

Le dispositif de surveillance sonore (SOSUS) de l'armée américaine a été l'un des premiers systèmes de détection à distance développés durant la guerre froide. SOSUS qui est constitué de capteurs immergés au fond des océans, permettait de détecter les mouvements des sous-marins soviétiques. Actuellement, ce système est utilisé par la National Geographic and Atmospheric Administration (NOAA) pour surveiller des mouvements dans les océans liés à l'activité terrestre ou animale. On peut aussi dire que la recherche moderne sur les réseaux de capteurs a commencé vraiment dans les années 80 avec le programme sur les réseaux distribués de capteurs (Distributed Sensor Network : DSN) lancé par le département recherche du ministère de la défense américaine (DARPA). L'identification des composants technologiques applicables

au DSN (les senseurs ou capteurs, les outils de communication, les techniques et algorithmes de traitement des données et les suites de logiciels distribués) a été décidée durant le workshop DSN de 1978. Les chercheurs de l'Université de Carnegie Mellon (CMU) et de l'Institut de Technologie du Massachussets (MIT) ont travaillé sur les systèmes d'exploitation de ces réseaux [121].

2.3. Définition de Wireless Sensors Network (WSN)

Un réseau WSN est un réseau composé d'un ensemble d'unités de traitements embarquées, appelées capteurs (nœuds). Ces nœuds communiquant via des ondes radio, afin de surveiller un phénomène bien précis (température, pression, mouvement…) dans une zone de captage ''sensing field''. Les données récoltées par l'ensemble des nœuds sont ensuite aiguillées vers un nœud médiateur dit puits (sink) pour pouvoir y appliquer des traitements spécifiques avant de les transmettre à l'utilisateur final via internet ou liaison satellitaire (figure 2.1). En plus de leur fonction initiale qui consiste à relever des mesures, les capteurs sans fil sont dotés de moyens de traitement et de communication de l'information. Cela représente désormais une révolution technologique des instruments de mesure issus de la convergence des systèmes électroniques miniaturisés et des systèmes de communication sans fil.

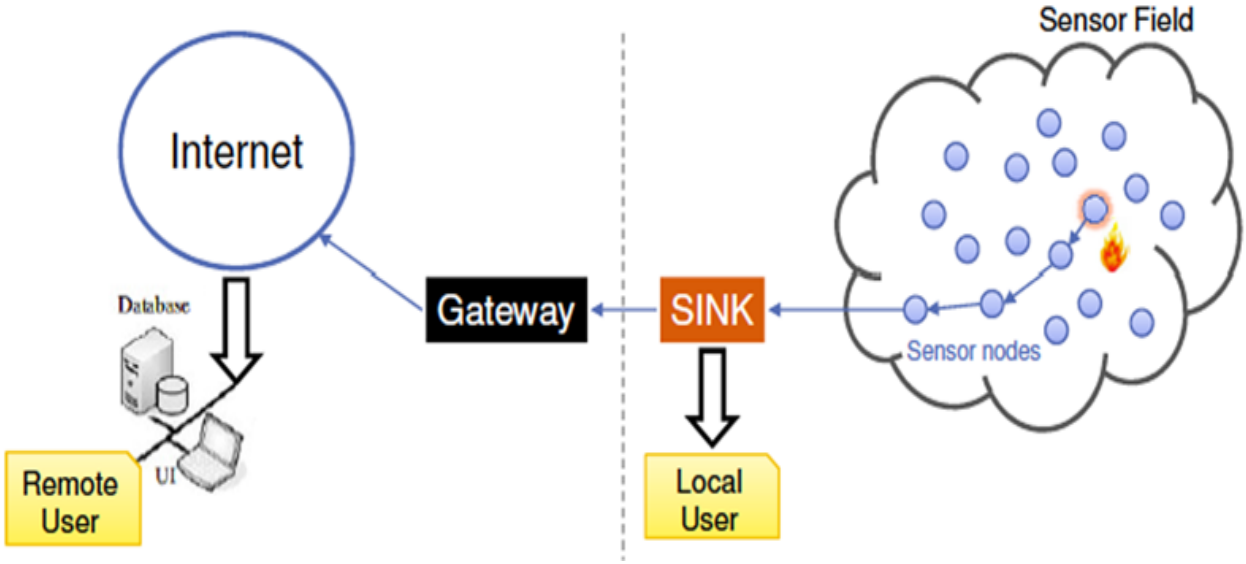


Figure 2.1. Wireless Sensor Network (WSN) [122].

2.4. L'Architecture physique d'un ''nœud capteur''

Un nœud capteur se compose de quatre unités de base [1] (figure 2.2):

2.4.1. Unité de capture (d'acquisition)

Cette unité est constituée d'un capteur électronique et d'un convertisseur analogique numérique. Cette unité se charge de convertir la grandeur prélevée en une valeur numérique, qui sera ensuite présentée à l'unité de traitement [1].

2.4.2. Unité de traitement

Elle inclut les types de processeur et mémoire adaptés pour exécuter les protocoles de communication qui permettent de mener la bonne collaboration inter-nœuds. Les données captées peuvent ainsi être analysées afin d'alléger les traitements au niveau du nœud sink. Notons qu'il y a plusieurs systèmes d'exploitation dédiés aux WSN. Le TinyOS est l'un des plus répandus pour les WSN. Omnet, Omnet + +, Contiki, Mantis OS sont aussi développés pour y concurrencer [1].

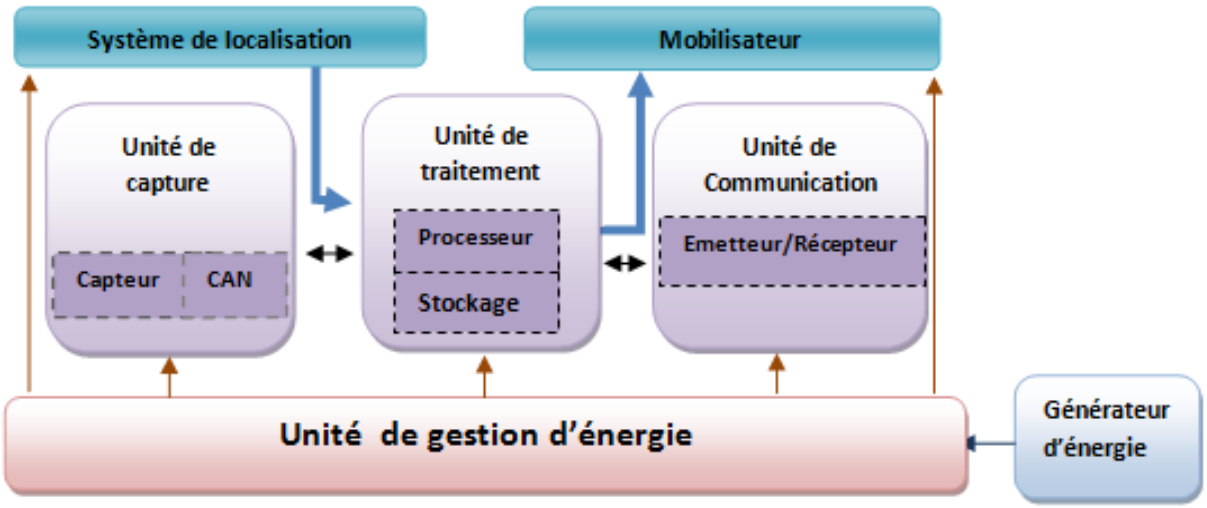


Figure 2. 2. Architecture physique d'un nœud capteur sans fil.

2.4.3. Unité de communication (de transmission)

Elle est composée essentiellement d'une antenne qui permet l'émission et la transmission des données.

2.4.4. Unité de gestion de puissance

Elle est chargée de répartir l'énergie disponible sur l'ensemble des modules. Elle peut actionner le mode ''veille'' aux composants inactifs, tout en minimisant les consommations et réduisant les pertes énergétiques. Elle peut aussi gérer les mécanismes de rechargement d'énergie utilisés pour augmenter la durée de vie du nœud et en conséquence la vie du réseau.

Un WSN peut également intégrer des modules supplémentaires tels qu'un système de localisation pour identifier sa position géographique (récepteur GPS), un système générateur d'énergie (cellule solaire), ou encore un système mobilisateur pour qu'il puisse se déplacer.

2.5. Les différents types de topologies des WSN

La topologie détermine l'organisation des capteurs dans le réseau. Il existe deux principales topologies dans les protocoles de routage pour les WSN.

2.5.1. Topologie plate

Dans une topologie plate, tous les nœuds possèdent le même rôle. Les nœuds sont semblables en termes de ressources, et la communication est de point à point (figure 2.3) [122]. Dans cette architecture, il est impossible de donner à chaque nœud un identificateur global, mais les protocoles de routages utilisés récoltent les informations de différentes sources minimisant ainsi la redondance et les multiples transmissions pour économiser de l'énergie et prolonger la durée de vie des nœuds [1,122].

2.5.2. Topologie hiérarchique

Afin d'augmenter la scalabilité du système, les topologies hiérarchiques (figure 2.4) ont été introduites en divisant les nœuds en plusieurs niveaux de responsabilité. L'une des méthodes les plus employées est le clustering, où le réseau est partitionné en groupes appelés "clusters". Un cluster est constitué d'un chef (cluster-head) et des nœuds qualifiés de membres. L'avantage de cette topologie est qu'elle élimine le problème d'auto-organisation du réseau et réduit la quantité d'information qui circule.

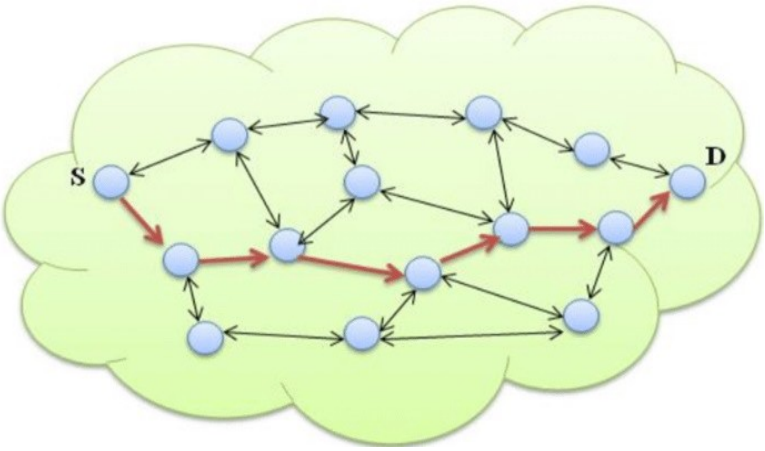


Figure 2. 3. Topologie plate.

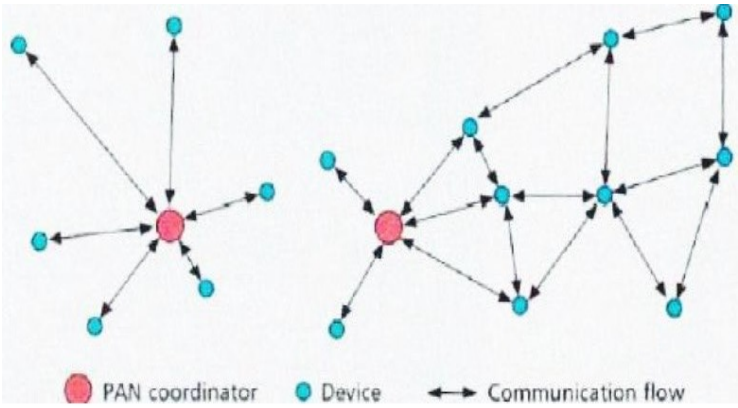


Figure 2. 4. Topologie hiérarchique.

2.6. Les domaines d'application des réseaux WSN

Le domaine d'application des WSN s'est accrue considérablement grâce à différents facteurs, tels que la minimisation de la taille des capteurs, la réduction de leur coût, et le nombre élevé de capteurs de différentes gammes existantes (thermique, chimique, cinétique, optique,….). Une application est dite de type ''time-driven'', lorsqu'elle nécessite des prélèvements périodiques de données. Cela est nécessaire en monitoring (exemples : feu, météo) afin d'établir des rapports périodiques.

Pour les applications de types event-driven relatives au temps réel, les capteurs doivent réagir immédiatement aux changements brusques des valeurs captées.

Les applications des WSN peuvent être catégorisées selon leur domaine d'application. Elles peuvent se définir alors en différentes options(figure 2.5):

- ✓ Les applications militaires.
- ✓ Les applications liées à la sécurité.
- ✓ Les applications environnementales.
- ✓ Les applications industrielles.
- ✓ Les applications d'urbanisme.
- ✓ Les applications médicales.

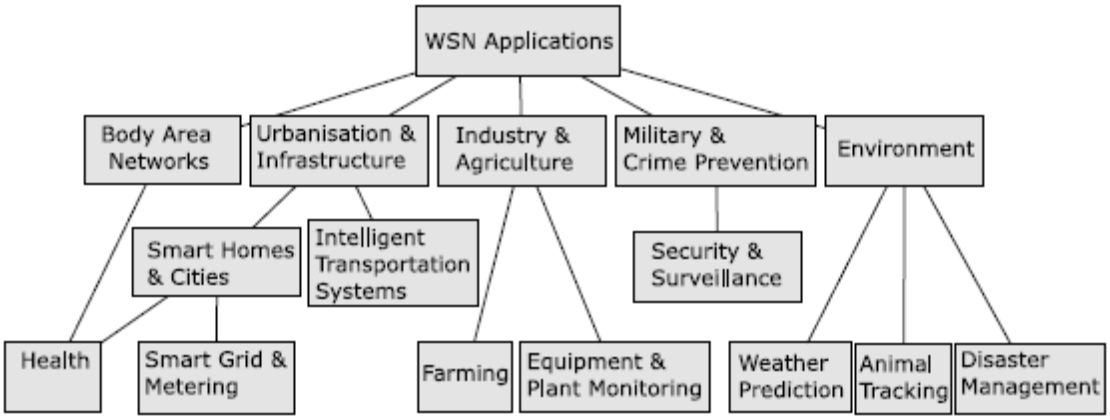


Figure 2. 5. Taxonomie des applications des WSN.

2.7. Les types de WSN

Les WSN se différencient selon leurs domaines d'applications. Dans la figure 2.6, ils sont répartis en WSN terrestres, souterrains, sous-marins, multimédia, et mobile [123]. Pour tous les domaines d'application les nœuds doivent acheminer l'information de la source vers la station de base [124].

2.7.1. Les WSN terrestres

Ils sont constitués d'un grand nombre (des centaines à des milliers) de nœuds déployés sur terre dans une zone bien définie, généralement de manière ad hoc (par exemple, des nœuds jetés par un avion). Dans les WSN terrestres [125], les nœuds capteurs doivent pouvoir retransmettre les données à la station de base dans un environnement dense. Comme la puissance de la batterie est limitée et généralement non rechargeable, les nœuds de capteurs terrestres peuvent être équipés de sources d'alimentation secondaires telles que des cellules solaires. L'énergie peut être économisée par l'exploitation d'un routage optimal multi-sauts, d'une courte

portée de transmission, d'une architecture réseau d'agrégation de données, et des opérations à faible cycle de service. Les applications des WSN terrestres concernent la détection et la surveillance de l'environnement, la surveillance industrielle et la surveillance d'explorations de surfaces.

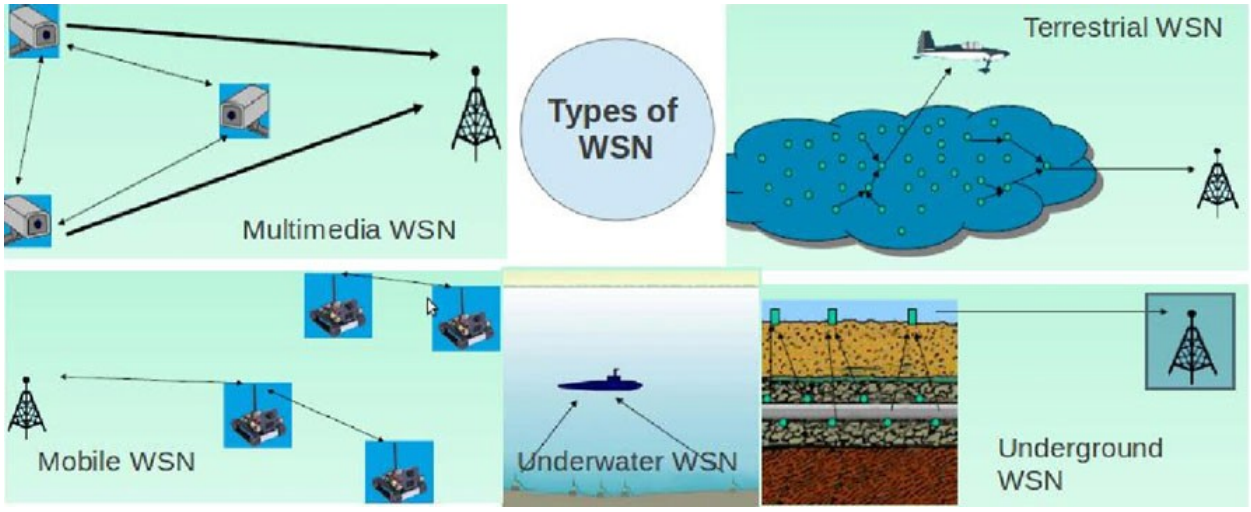


Figure 2. 6. Types de WSN [125].

2.7.2. Les WSN souterrains

Ils se composent d'un certain nombre de nœuds de capteurs déployés dans des grottes ou des mines ou sous terre pour surveiller les conditions souterraines [126,127]. Afin de relayer l'information des nœuds capteurs souterrains à la station de base, des nœuds puits supplémentaires sont situés au-dessus du sol. Ils sont plus chers que les WSN terrestres car ils nécessitent des équipements appropriés pour assurer une communication fiable à travers le sol, les roches, et l'eau. La communication sans fil est un défi dans un tel environnement en raison d'atténuation et de perte de signal. De plus, il est difficile de recharger ou de remplacer la batterie de nœuds cachés sous terre, il est donc important pour une durée de vie prolongée, de concevoir un protocole de communication économe en énergie. Les WSN souterrains sont utilisés dans de nombreuses applications telles que la surveillance de l'agriculture, la gestion du paysage, la surveillance souterraine du sol, de l'eau ou des minéraux, et la surveillance militaire des frontières [127].

2.7.3. Les WSN sous-marins

Ils se composent de nœuds capteurs déployés sous l'eau, par exemple dans l'environnement océanique [128-129]. Comme étant coûteux, seuls quelques nœuds sont déployés et des véhicules sous-marins autonomes sont utilisés pour explorer ou recueillir les données des nœuds. La communication sans fil sous-marine utilise des ondes acoustiques qui présentent divers défis tels qu'une bande passante limitée, un long délai de propagation, une latence élevée et les problèmes d'évanouissement du signal. Ces nœuds doivent pouvoir s'auto-configurer et s'adapter à des conditions extrêmes du milieu océanique. Les nœuds sont équipés d'une batterie limitée qui ne peut pas être remplacée ou rechargée nécessitant une communication sous-marine et des techniques de mise en réseau économique en termes d'énergie. Les applications des WSN sous-marins comprennent la surveillance de la pollution, la surveillance et l'exploration sous-marines, la prévention des catastrophes, la surveillance sismique, et la surveillance des équipements et de la robotique sous-marine [129].

2.7.4. Les WSN mobiles

Ils se composent de nœuds de capteurs mobiles qui peuvent se déplacer et interagir avec l'environnement physique [123]. Les nœuds mobiles peuvent se repositionner et s'organiser dans le réseau en plus de pouvoir détecter, calculer et communiquer. Un algorithme de routage dynamique doit donc être employé contrairement au routage fixe appliqué au WSN statique. Les WSN mobiles sont confrontés à divers défis tels que le déploiement, la gestion de la mobilité, localisation avec mobilité, navigation et contrôle des nœuds mobiles, le maintien de la couverture de la détection adéquate, minimiser la consommation d'énergie dans la locomotion, et le maintien de la connectivité du réseau et la distribution des données. Les principales applications des WSN mobiles sont la surveillance (environnement, habitat, sous-marin), surveillance militaire, suivi de cible, recherche et sauvetage. Un degré plus élevé de couverture et de connectivité peut être obtenu avec des nœuds de capteurs mobiles par rapport aux nœuds statiques [123].

2.7.5. Les WSN multimédia

Un WSN multimédia se compose de nœuds de capteurs à faible coût équipés de caméras et de microphones, déployés de manière planifiée pour garantir la couverture [130]. Ces capteurs multimédia sont capables de stocker, de traiter et de récupérer des données multimédia sous

forme de vidéo, d'audio et d'images. Ils doivent faire face à divers défis tels que la demande d'une large bande passante, consommation d'énergie élevée, fourniture de qualité de service (QoS), les techniques de traitement et de compression des données, et la conception inter-couches. Il nécessite des techniques de transmission assez développées prenant en charge une large bande passante et une faible consommation d'énergie afin de diffuser un contenu multimédia tel qu'un flux vidéo. Bien que l'amélioration de la QoS soit difficile dans les WSN multimédias en raison de la capacité et du délai de liaisons variables, un certain niveau de QoS doit être atteint pour une livraison fiable de contenu. Les WSN multimédia améliorent substantiellement les applications WSN existantes telles dédiées au suivi et à la surveillance (sécurité).

2.8. Consommation énergétique

L'une des contraintes de conception des nœuds WSN est la consommation énergétique. Comme la majorité des capteurs sont conçus par le domaine de recherche, alors leurs caractéristiques de consommation d'énergie sont bien connues. La consommation d'énergie doit être amoindrie pour que le réseau survive le plus longtemps possible, qu'il s'adapte aux différents environnements (fortes chaleurs, eau,..), qu'il soit autonome et très résistant vu qu'il est souvent déployé dans des environnements hostiles [1].

Les nœuds d'un WSN inclus des cartes DSP (Digital Signal Processing), des CAN (Convertisseurs Analogiques Numériques) et des CNA (Convertisseurs Numériques Analogiques) qui opèrent à une basse fréquence avec une consommation moins de 1mW ainsi qu'un transceiver (transmetteur/récepteur). Au démarrage du transceiver, un certain temps doit être alloué au synthétiseur de fréquence et à l'oscillateur de contrôle de voltage VCO (Voltage-controlled Oscillateur) afin de cerner la fréquence de la porteuse [132].

Le bloc de RF (radio-frequency) inclut l'amplificateur de puissance, l'amplificateur de LNA (Low-noise amplifier) et le mélangeur qui ont un temps de démarrage négligeable, alors ils peuvent rester verrouillés au mode de démarrage. Les composantes actives du récepteur sont : LNA, le mixeur, le synthétiseur de fréquence, le VCO, l'amplificateur de fréquence intermédiaire (IF amp) et le démodulateur (Demod). Le transmetteur comporte le modulateur (Mod), le synthétiseur de fréquence, le VCO (partagé avec le récepteur) et l'amplificateur de puissance [132].

2.9. Communication dans les WSN

2.9.1. Le modèle en couche adapté aux WSN

Le médium de transmission est un dispositif commun pour tous les nœuds du réseau, il nécessite donc un mécanisme qui gère l'accès aux nœuds afin de déterminer le droit d'émettre à partir de chacun d'entre eux dans le réseau. Le modèle de couche adapté pour les WSN possède 5 couches qui ont les mêmes tâches que celles du modèle OSI (Open Systems Interconnection) et 3 autres couches qui permettent la gestion de la puissance d'énergie, la gestion de la mobilité ainsi que la gestion des tâches (figure 2.7) [1]. Chaque couche utilise ainsi les services des couches inférieures, et en fournit à celles de niveau supérieur. Ces couches ont les spécificités ci-dessous:

La couche physique (physical Layer): Elle dispose des spécifications concernant les caractéristiques matérielles, des fréquences porteuses, …etc.

La couche liaison de données (Data Link Layer): Spécifie comment les données sont expédiées entre deux nœuds. Elle est responsable du multiplexage des données, du contrôle d'erreurs, de l'accès au media,... Elle assure la liaison point à point et multipoints dans un réseau de communication.

La couche réseau (Network Layer) : Dans la couche réseau, le but principal est de trouver une route et une transmission fiable des données captées par des nœuds capteurs vers le puits "sink" en optimisant l'utilisation de l'énergie des capteurs.

La couche de transport (Transport Layer): Elle est chargée du transport des données, de leur découpage en paquets, du contrôle de flux, de la conservation de l'ordre des paquets et de la gestion des éventuelles erreurs de transmission.

La couche application (Application Layer): Cette couche assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, et donc géré directement par les logiciels.

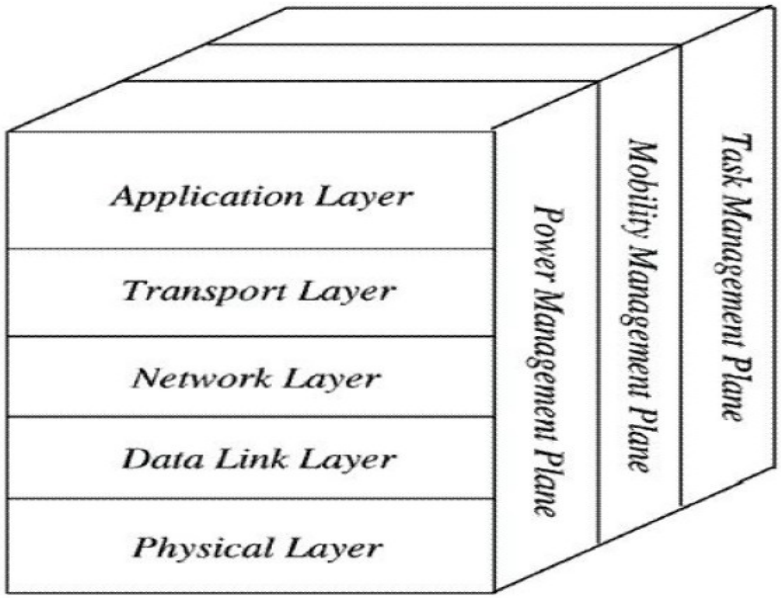


Figure 2. 7. Modèle de couches adapté pour les WSN.

2.10. Les standards de communication adaptés aux WSN

Le choix du standard de communication varie selon l'application ciblée. Il y a des applications qui nécessitent des batteries à durée de vie longue, d'autres nécessitent une haute sécurité, une basse latence…etc. Le développement de nouveaux standards de communication permet l'introduction des WSN dans de nouvelles structures. La majorité des standards listés sont adoptés dans l'IOT. Cette liste comprend:

- ✓ le **Z-Wave** développé principalement pour une application domotique.
- ✓ **La RFID** utilisée par les technologies NFC (Near Field Communication) et EAS (Electronic Article Surveillance).
- ✓ **IEEE 802.15.4 ,** les technologies utilisant ce standard sont :

  ZigBee : une pile technologique réseau sans-fil destinée à la domotique [133,134].

  WirelessHART : est une pile technologique réseau sans-fil développée par HART Communications Foundation et publiée en 2007**.**
- ✓ **IEEE 802.11ah** destinée aux réseaux M2M (Machine to Machine) [135,136]
- ✓ **ISA100.11a** est une pile technologique réseau sans-fil développée par l'International Society of Automation (ISA) en 2009**,**
- ✓ **6LoWPAN,** le but est que chaque nœud d'un WSN dispose de sa propre adresse IP.

- ✓ **WIA-PA** développé par la Chinese Industrial Wireless Alliance (CIWA) et approuvé en 2007. Il est conçu pour la communication sans fil des systèmes industriels automatisés.
- ✓ **Bluetooth,** normalisé sous le nom IEEE 802.15.1 et BLE.

L'utilisation d'IPv6 dans le monde entier a été estimée pour l'an 2020, mais des problèmes politiques, économiques et surtout ethniques se dressent contre sa généralisation. L'application des 6LoWPAN est toujours limitée. Le reste des standards appliqués pour WSN, et appliqués aussi aux réseaux d'IOT permettent de noter que les WSN forment le support d'IOT, et donc l'IOT n'est d'autre que la fonction et la gestion des WSN modernes [1].

2.11. Technologies des WSN

2.11.1. ANT technologie

C'est une technologie propriétaire qui utilise ''une pile protocole de communication sans fil'' pour les applications de mise en réseau à très faible consommation. Elle est conçue pour fonctionner sur des microcontrôleurs et émetteurs-récepteurs à faible consommation d'énergie sur la bande ISM 2,4 GHz [137].

ANT prend en charge diverses topologies, y compris point à point , étoile, arbre et d'autres types de réseaux maillés dans les réseaux personnels (PAN) adaptés aux sports, au ''fitness'', et les applications de santé à domicile. Il convient également aux réseaux locaux (LAN) pour les applications domestiques et d'automatisation industrielle. ANT est économe en énergie et fournit un débit de données de 1 Mbps [137].

2.11.2. Wavenis technologie

Wavenis est une technologie sans fil ultra basse consommation et longue portée développée par Coronis [138] pour les applications WSN dans lesquelles la capacité de communication et l'autonomie des appareils présentent des exigences contradictoires. Elle est développée à l'origine en tant que technologie propriétaire, puis promue par la Wavenis Open Standard Alliance. Les nœuds Wavenis sont utilisés dans la télémétrie, l'automatisation industrielle, la surveillance à distance des compteurs, soins à domicile, contrôle d'accès et suivi de la chaîne de froid. Ses principales caractéristiques comprennent la fiabilité, les économies d'énergie, la coexistence du réseau et la robustesse contre les interférences. Wavenis opère dans le monde entier dans les bandes ISM 868, 915 et 433 MHz. Les débits de programmation des

données sont de 4,8 kbps à 100 kbps. La plupart des applications Wavenis communiquent à 19,2 kbps [138].

2.11.3. Dash7 technologie

C'est une technologie WSN open source, avec une ultra basse consommation et longue portée basée sur la norme ouverte ISO 18000-7. Elle opère dans la bande sans licence ISM 433 MHz. Elle est promue par l'Alliance DASH7 travaillant sur l'interopérabilité entre les appareils Dash7. Le réseau DASH7 utilise un nouveau concept technologique appelé BLAST (Bursty, Light, Asynchronous, Transitive) qui le rend très adapté aux utilisations nécessitant une communication asynchrone de hauts débits entre les appareils. Les appareils du système Dash7 sont portables et centrés sur le téléchargement, donc pas d'infrastructure fixe (c'est à dire pas de stations de base). Les principales caractéristiques de Dash7 incluent une autonomie de plusieurs années, une portée de communication allant jusqu'à 10 km, faible latence pour la connexion avec des objets en mouvement, prise en charge de la sécurité, débit de données jusqu'à 200 kbps et une précision de localisation en temps réel à moins de 4 m [130].

Les applications majeures de Dash7 incluent la gestion de la chaîne d'approvisionnement, la gestion des stocks, les paiements mobiles, optimisation de la fabrication et des entrepôts, surveillance des matières dangereuses, services avancés basés sur la localisation, compteur intelligent et automatisation des bâtiments [130].

2.11.4. EnOcean technologie

EnOcean est une technologie WSN émergente promue par EnOcean Alliance. La norme sans fil EnOcean [139] est optimisée pour les solutions à ultra-basse consommation et la récolte d'énergie. La technologie EnOcean sans pile réunit la détection sans fil et la récolte d'énergie afin d'avoir un WSN récolteur d'énergie. L'objectif de cette technologie est de tirer de l'énergie de l'environnement, par exemple du mouvement, de la pression, de la lumière ou variation de température et les convertir en énergie utilisable électriquement.

La technologie EnOcean est utilisée dans l'automatisation industrielle. Elle travaille dans les bandes 868 MHz et 315 MHz et prend en charge une portée de transmission allant jusqu'à 30 m en intérieur et 300 m en extérieur. Les produits EnOcean disponibles sur le marché incluent l'auto-alimentation sans batterie des capteurs et interrupteurs sans fil. Les modules EnOcean sans

batterie avec récolte d'énergie disponibles, réduisent le coût du cycle de vie car ils ne nécessitent aucun entretien.

La revue de l'ensemble de ces technologies et leurs domaines d'application nous fait rappeler les domaines d'application de l'IOT déjà mentionnés dans le chapitre 1, tels que la domotique, le contrôle industriel, la surveillance, la sécurité, les compteurs intelligents, et les stations météorologiques...etc.

2.12. Conclusion

On constate que l'ensemble des standards de communication adoptés par les WSN font partie de ceux adoptés par l'IOT. Les WSN dans leur fonction servent aussi de support pour l'IOT et que les applications des WSN sont l'IOT dans sa fonctionnalité. On peut alors affirmer qu'il y a une synergie entre les WSN et les différents standards de communication dans l'accomplissement de la fonction d'IOT. Alors, la gestion optimale des WSN fera l'objet du prochain chapitre.

Chapitre 03

Chapitre 03 : Gestion optimale des WSN

3.1. Introduction

Les problèmes majeurs dans les WSN sont fondamentalement liés à la consommation énergétique (durée de vie des nœuds), à la sécurité de l'agrégation des données, et à la tolérance aux pannes (la redondance). Plusieurs études et solutions sont envisagées pour résoudre ces problèmes et aboutir à une gestion optimale [1]. Dans ce chapitre, les technologies et les points clés sur lesquels repose la gestion optimale des structures WSN sont expliqués.

3.2. La gestion dans les WSN

La gestion dans les WSN s'articule sur trois plans: Contrôle d'énergie, contrôle de mobilité des nœuds et distribution des tâches [1].

Ces plans aident les ''nœuds limites'' (capteurs) à coordonner la tâche de captage et à minimiser la consommation d'énergie. Il est donc impératif que les nœuds capteurs collaborent ensemble, pour acheminer les données dans un réseau mobile en se partageant les ressources mises en œuvre, et en utilisant efficacement l'énergie disponible. Ainsi, le réseau pourrait prolonger sa durée de vie.

3.2.1. Plan de gestion d'énergie

Il y a focus sur l'utilisation rationnelle de l'énergie et donc un contrôle des modes opératoires de la batterie. Comme déjà mentionné, les nœuds des WSN sont formés de cartes DSP dédiées et surtout de type faible consommation énergétique. Pour y voir de près et considérer un exemple, dans la phase de démarrage, quelques blocs ne sont pas alimentés tels que le mélangeur et le bloc RF (radio frequency) [132]. Aussi, après réception d'un message, le capteur éteint son récepteur afin d'éviter la duplication des messages déjà reçus. En outre, si le niveau d'énergie devient bas, le nœud capteur diffuse à ses voisins une alerte les informant ainsi qu'il ne peut pas participer au prochain routage. L'énergie restante est donc réservée au captage [1]. La majorité des technologies de WSN sont développées sous la règle d'optimiser la consommation énergétique. Parmi ces technologies, On trouvera ANT [137], Wavenis [138],

Dasht [130] et EnOcean. Cette dernière est une technologie qui récolte l'énergie au près de son entourage.

3.2.2. Plan de gestion de mobilité

Ce plan détecte et enregistre le mouvement du nœud capteur. Ainsi, un retour arrière vers l'utilisateur est toujours maintenu et le nœud capteur peut garder trace de ses voisins. La mise à jour de la table des voisins permet de libérer sa mémoire et réduire la consommation énergétique en arrêtant l'émission inutile de messages. Pour des WSN hybrides (nœuds statiques et nœuds mobile), en addition aux protocoles de routage statique, des protocoles de routage dynamique sont nécessaires pour actualiser le lien entre la source et la destination [140].

3.2.3. Plan de gestion de tâche

Ce plan distribue et ordonnance les différentes tâches de captage de données dans une région spécifique. Il n'est pas nécessaire que tous les nœuds capteurs de cette région effectuent la tâche de captage au même temps; certains nœuds exécutent cette tâche plus que d'autres selon leur niveau de batterie [118].

La gestion de tâche peut être approuvée avec la topologie envisagée au réseau. Pour les topologies plates, tous les nœuds sont de même ordre de ressources et la gestion de tâche est organisée selon le principe de la reconfiguration de nœud à partir de son emplacement où l'événement est survenu et de l'état de sa batterie [1].

3.3. L'optimisation des WSN

Une gestion optimale des WSN concerne surtout la réduction de la consommation d'énergie et la réduction du temps de communication. L'optimisation des WSN est établie avant et après la création du réseau WSN. Alors, la phase de déploiement des nœuds est une phase primordiale pour le bon fonctionnement et la prolongation de la durée de vie des nœuds. C'est dans cette étape que la topologie du réseau est décidée, ainsi que le type de protocole de routage à adapter et la planification de la consommation énergétique [118].

3.3.1. Optimisation de déploiement des nœuds

L'optimisation des WSN commence par penser à un déploiement optimal des nœuds. Ce déploiement est réparti sur trois étapes:

- ✓ Etape de pré-déploiement et de déploiement, concerne le placement manuel des nœuds par un humain, par un robot, ou le lancement des nœuds à partir d'un hélicoptère.
- ✓ Une étape de post-déploiement, cette étape est nécessaire dans le cas où le changement de topologie est survenu à cause du déplacement des nœuds.
- ✓ Une étape de redéploiement où de nouveaux nœuds sont ajoutés au réseau pour remplacer les nœuds défectueux ou en panne.

Le déploiement des nœuds peut être aléatoire ou contrôlé [1,141]. Mnasri S. [141] a cité presque la majorité des critères et problématiques de déploiements de nœuds dans les WSN. Parmi ces problématiques, il y a les cas stationnaires ou mobiles, les cas mono et multi objectifs, statiques et dynamiques…etc. Parmi les différentes approches pour résoudre ces problématiques on trouve:

3.3.1.1. Approches centralisées (Node Centric)

Ces approches reposent sur des algorithmes comme les algorithmes de Bernoulli (BDA : Bernoulli Deployment Algorithm), les algorithmes dits à champs potentiel (PFDA : Potential Field Deployment Algorithm), les algorithmes de force virtuels (VFA : Virtual Force Algorithm)…etc. Dans cette approche centralisée, la communication est basée sur l'identification du nœud [118].

3.3.1.2. Approches Distribuées

Pour cette approche, deux cas sont possibles:

Cas 1: la communication est basée sur l'information échangée pour optimiser la couverture réseau (''Data Centric'').

Cas 2: la position géométrique (Position Centric) [118,141] est le moyen principal d'adressage et de routage dans le réseau [1,118]. Pour cette approche, les connexions se font au gré de la transmission radio. Un signal est reçu s'il est K fois plus fort que le bruit (K= 10 typiquement). Rappelons que l'atténuation des ondes radio avec la distance est : $1/r^{\propto}$

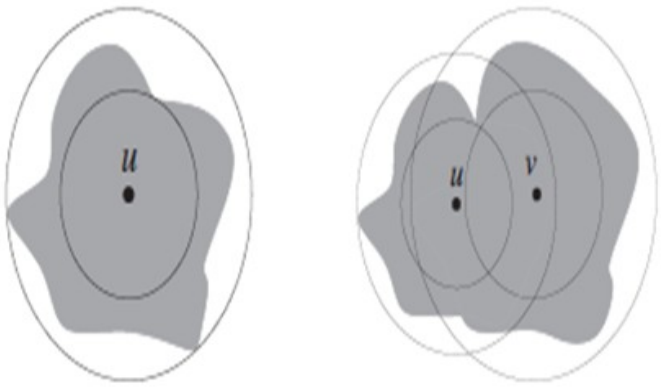
Où r est la distance (séparant l'émetteur et le récepteur) et α est le terme d'affaiblissement (dépend de l'environnement, α= 2 dans l'air, mais peut augmenter avec les obstacles).

Ainsi, si P_e est la puissance d'émission du signal, et B le bruit ambiant constant, un émetteur radio sera reçu jusqu'à une distance R (équation (3.1)) [131]:

$$R = \left(\frac{P_e}{KB}\right)^{1/\propto} \qquad (3-1)$$

Pour un espace homogène (α constant), l'ensemble des positions d'où l'on peut recevoir le signal constitue un disque centré sur l'émetteur. Cet ensemble est plus complexe lorsqu'il y a des obstacles (murs, bureaux…..). Le modèle classique (le plus simple) est un graphe de disques unitaires (disk unit graph).

Deux nœuds d'un réseau WSN peuvent communiquer s'ils sont à distance inférieure à R. Les distances sont normalisées pour que R= 2, un disque unitaire est centré sur chaque nœud, et deux nœuds peuvent communiquer si leurs disques s'intersectés. La figure 3.1(a) montre que la région de transmission du nœud u est définie par le disque $D(u, R_u)$ incluant le disque $D(u, r_u)$. La figure 3.1(b) montre que la communication entre deux nœuds u *et* v appartenant à deux disques unitaires différents ne peut être établie que si la distance euclidienne entre eux est inferieure ou égale à min (R_u,R_v).



(a) (b)

Figure 3. 1. Disques unitaires et intersection entre deux nœuds (u,v) [132].

3.3.1.3. Approches hybrides

Les approches hybrides consistent à utiliser deux techniques ou plus pour résoudre la problématique voulue. Il reste à trouver le bon schéma d'hybridation et savoir combiner ces méthodes pour en tirer des avantages. Pour cette approche hybride, des routages dynamiques et statiques sont utilisés [141].

3.3.2. Optimisation par la sécurité de l'agrégation des données

L'agrégation des données est une technique utilisée dans les réseaux WSN afin de réduire la charge de trafic en combinant des informations sur des nœuds intermédiaires pour une future transmission [1, 36, 142]. Elle est utilisée dans les approches ‘‘Data Centric’’ pour les réseaux M2M [93]. La figure 3.2 englobe la majorité des protocoles d'agrégation des données.

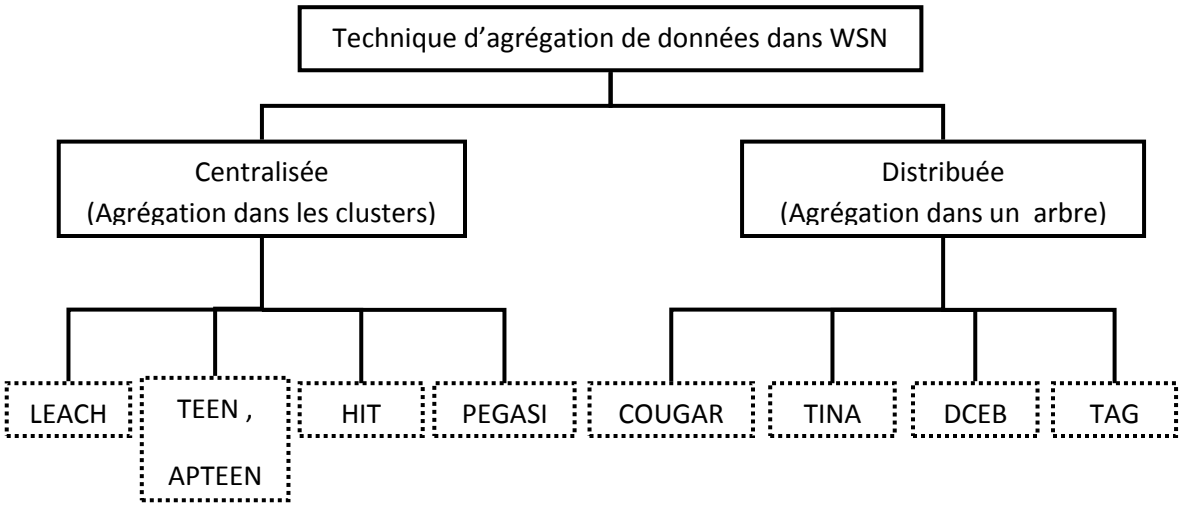


Figure 3. 2. Protocoles d'agrégation dans les réseaux de capteurs sans fils [1].

-Le protocol LEACH(Low-Energy Adaptive Clustering Hierarchy): C'est un protocole de routage hiérarchique, employant un procédé de clustering qui divise le réseau en deux niveaux : les cluster-heads et les nœuds membres. Le protocole se déroule en ‘‘rounds’’. Chaque round se compose de deux phases : construction et communication [143]. En utilisant TDMA, le protocole LEACH est destiné aux applications ‘‘time-driven’’. Dans ce type d'application, la donnée est propagée d'une manière périodique. Cependant, ce genre de protocole est inadapté pour les applications ‘‘event-driven’’, où un comportement réactif est nécessaire pour le bon fonctionnement du système [1].

-Le protocole TEEN (Threshold sensitive Energy Efficient sensor Network protocol): Ce protocole a été développé pour modeler LEACH afin de répondre aux exigences des applications ‘‘event-driven’’ [1].

-Le protocole COUGAR: Dans COUGAR, les données produites par le réseau de capteurs sont modélisées comme une table relationnelle. Dans cette table, chacun des attributs représente soit des informations sur le nœud capteur ou bien des données produites par ce nœud capteur. L'approche COUGAR fournit une agrégation partielle au niveau des nœuds capteurs. Chaque nœud capteur maintient une liste d'attente contenant les nœuds capteur fils qui doivent lui envoyer les paquets. Ce nœud récolteur d'information doit attendre jusqu'il reçoive tous les paquets des nœuds fils. Une fois les paquets agrégés, il émet le paquet au prochain saut. Cependant, ce nœud agrégateur peut devenir inaccessible à cause du mouvement ou d'un problème de batterie. Pour cela, COUGAR utilise un ‘‘timer’’ afin d'éviter une attente indéfinie.

La sécurité de cette technique d'agrégation a un impact capital pour l'optimisation des applications WSN. Claude C. [142] a provoqué ce problème dans les applications médicales qui ont une relation directe avec la sécurité de vie des patients, tel que l'agrégation de mesures d'un pacemaker qui doivent être sécurisées via des techniques de cryptage robuste. El Hanafi T. [144] a proposé une solution de Cryptographie à base de courbes elliptiques pour la sécurisation des traitements et des échanges d'informations dans les WSN. Il a proposé deux schémas de chiffrement homomorphes utilisant respectivement un groupe multiplicatif sur un corps fini et sur les courbes elliptiques. Mandicou B. [145] décrit une solution pour le routage et l'agrégation de données dans les réseaux de capteurs sans fil structurés en clusters auto-stabilisants afin de réduire la consommation énergétique en adaptant trois scénarios de routage intégrant différents niveaux d'agrégation:

*Un premier niveau dit, ‘‘Routage Sans Agrégation’’ (RSA), permet de minimiser les délais de communication.

*Un deuxième niveau qui est ‘‘Routage avec Agrégation Partielle’’ (RAP) permettant la réduction de la consommation énergétique totale.

*Un troisième niveau de Routage nommé ‘‘Agrégation Totale’’ (RAT, prolonge la durée de vie des cluster-heads.

Pour Challal Y. [1], les solutions de sécurité d'agrégation sont classées en deux grandes catégories selon le mécanisme cryptographique utilisé (figure 3.3):

- Solutions basées sur le cryptage de bout en bout : dans cette catégorie, on utilise des mécanismes cryptographiques qui sécurisent l'information captée de bout en bout tout en permettant aux nœuds intermédiaires de réaliser les opérations d'agrégation. Dans cette

catégorie, la vérification de l'information ne se fait généralement qu'au niveau du collecteur, ce qui engendre une forte contamination de la fausse information.

- Solutions basées sur le cryptage de proche en proche : dans ce cas, la véracité de la l'information est vérifiée de proche en proche et son rejet peut se faire à n'importe quel niveau de l'arbre couvrant le WSN.

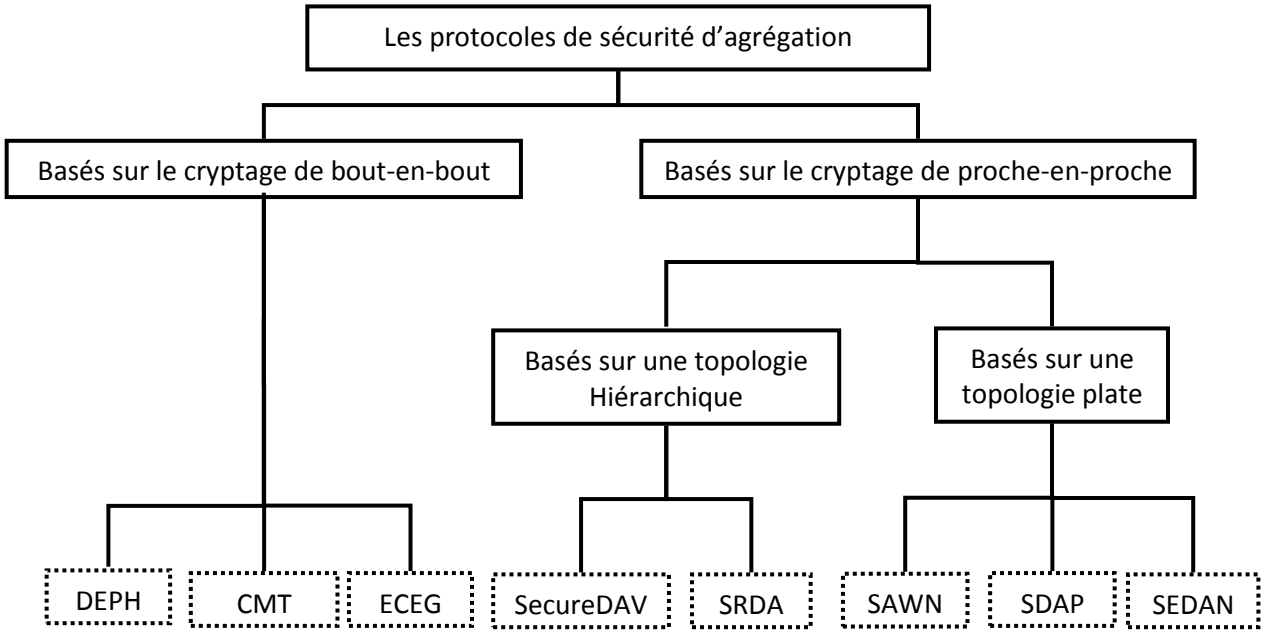


Figure 3. 3. Classification des solutions d'agrégation sécurisées [1].

Par exemple le protocole SAWN (Secure Aggregation for Wireless Networks) se base sur la vérification à deux sauts: un nœud vérifie si l'agrégation des données de ses petits fils, réalisée par son fils, est correcte.

3.3.3. Optimisation par la tolérance aux pannes

La topologie des WSN est tolérante aux pannes c'est à dire que quand un nœud est supprimé (détruit ou la batterie est à plat), le réseau continue son fonctionnement. La tolérance aux pannes se fait au niveau des couches réseau et MAC.

3.3.3.1. Optimisation au niveau de la sous-couche Mac de la couche liaison de données

La couche MAC (Medium Access Control) est une sous-couche de la couche liaison de données, elle est responsable de la transmission radio des données (figure 3.4).

Dans la plupart des plates-formes matérielles, la transmission radio est la source principale de consommation d'énergie et l'activité radio est en grande partie commandée par la couche MAC. En ce qui concerne le protocole MAC, les sources principales de perte d'énergie sont les collisions, l'écoute (idle listening) pour recevoir des données possibles, overhearing, réception de données destinées à d'autres nœuds, le contrôle de l'overhead et over-emitting, et les cas de transmissions de messages quand le destinataire n'est pas prêt.

Donc, pour économiser au mieux l'énergie de la batterie d'un capteur, il faudrait que les transmetteurs radio soient le plus souvent possible éteints. Cependant, ceci pourrait poser le problème de la synchronisation des capteurs et la répartition des périodes de réveil. Ainsi, il faudrait que la couche MAC permette aux capteurs d'avoir des périodes de sommeil assez longues, mais sans perturber les communications [133].

Le protocole MAC dédié aux réseaux de capteurs devrait être efficace en terme d'énergie, stable lorsque la taille du réseau augmente, et adaptatif aux changements de la topologie et de la connectivité du réseau lorsque les capteurs cessent de fonctionner, ou de se déplacer.

Deux catégories de protocoles au niveau de la couche MAC se distinguent:

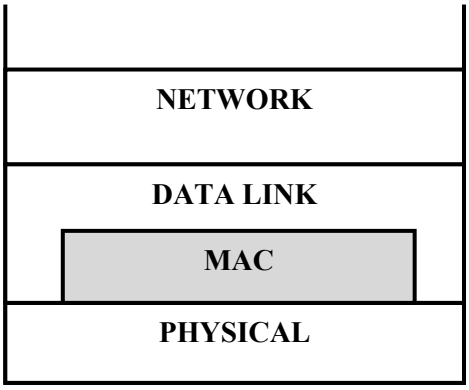


Figure 3. 4. Sous-couche MAC dans le modèle OSI.

3.3.3.1.1. Les protocoles ordonnancés (Scheduling protocols)

Ces protocoles sont efficaces en consommation d'énergie parce qu'ils évitent les collisions et ''overhearing''. Ils ne permettent pas les communications point-à-point et exigent généralement aux nœuds de former des clusters. La communication inter-cluster est réalisée par

les approches: TDMA, FDMA, et CDMA. Ces approches manquent d'adaptabilité aux changements de la topologie ainsi que l'ordonnancement d'activité des nœuds relais [133].

3.3.3.1.2. Protocoles à base de contention

Les protocoles d'accès au médium basés sur ''la contention'' sont plus flexibles aux changements de la topologie. Ils permettent la communication pair-à-pair, et n'exigent aucune synchronisation. Néanmoins, ils n'utilisent pas souvent efficacement les ressources à cause des collisions et de l'écoute inutile [133]. Parmi les protocoles cités dans la littérature, on trouvera: S-MAC (Sensor MAC) [134] particulièrement conçu pour les systèmes d'alerte dans lesquels les applications ont de longues périodes d'inactivité et peuvent tolérer la latence.

Le T-MAC (Timeout MAC) [134] un protocole qui a été conçu pour améliorer les performances de S-MAC avec une charge de trafic variable.

B-MAC (Berkeley MAC) [146] est un autre protocole MAC qui a été développé par l'Université de Berkeley. Dans ce protocole, les nœuds capteurs utilisent la technique LPL (Low Power Listening) afin d'alterner entre périodes actives et périodes inactives. Dans la technique LPL, l'état actif de chaque nœud est généralement d'une durée très courte, permettant juste au nœud de vérifier l'état du canal (CCA: Clear Channel Assessment). La limitation de B-MAC [146] est la ''sur-écoute'' du canal due à l'envoi d'un long préambule qui doit être nécessairement reçu par tous les voisins de communication (récepteurs potentiels) d'une source donnée, même si ces données ne sont pas destinées à tout le voisinage de cette source.

X-MAC [146] est une amélioration du protocole B-MAC pour régler le problème de la ''sur-écoute'' du canal causée par la transmission de longs préambules. Pour ce faire, chaque préambule dans X-MAC est divisé en une série de préambules plus petits contenant chacun l'adresse du destinataire. Un certain intervalle de temps est inséré entre deux préambules successifs afin de permettre au destinataire adéquat d'envoyer un ACK dès la réception d'un préambule donné. Alors l'émetteur est assuré que le récepteur est dans l'état actif après avoir reçu l'ACK de ce dernier, et pourra démarrer automatiquement sa transmission. Aussi ce protocole performe la consommation énergétique en réduisant la ''sur-écoute'' du canal.

Z-MAC [146] est un protocole MAC hybride qui combine les techniques CSMA et TDMA. Ce protocole permet d'éviter les interférences d'émissions de nœuds voisins.

DSMAC (Distributed Scheduling Medium Access Control) [146], est un algorithme proposé pour permettre l'ordonnancement au niveau de la couche MAC selon l'emplacement des nœuds ; cet algorithme permet une couverture de 100% de la zone de couverture.

Une solution hybride (une solution centralisée et une solution distribuée) est proposée par Diery N. [147] pour le recouvrement d'une panne dédiée à la tolérance aux pannes dans un WSN à grande échelle pour l'agriculture de précision. Ces solutions permettent:

• La réduction du taux d'interférences en utilisant une communication multi-canal.

• Le recouvrement des pannes pour rétablir le fonctionnement normal du réseau.

• La réduction de l'impact des pannes sur le reste du réseau.

• Le respect des caractéristiques des nœuds capteurs.

Mehdi B. [148] propose le routage CEDM-DR (Combined Energy and Distance Metrics Dynamic Routing Protocol). CEM-DR permet la prolongation de la durée de vie du réseau. Pour cela, il utilise une combinaison de métriques qui sont l'énergie résiduelle dans les nœuds ainsi que les distances entre les nœuds intermédiaires et la distance par rapport au point de collecte dans l'objectif d'avoir une consommation d'énergie équilibrée pour tous les nœuds du réseau WSN.

Karla B. [149] propose des solutions pour l'optimisation des WSN hétérogènes du point de vue de la portée de transmission et cela en décidant des chemins respectant la contrainte sur la longueur mais dont le coût est inférieur à celui du plus court chemin en nombre de sauts.

3.3.3.2. Optimisation au niveau de la couche réseau

Pour Challal Y. [1], l'optimisation au niveau de la couche réseau dépend de la topologie adaptée, plate ou hiérarchique. Pour les deux topologies, les protocoles de routages sont à mieux pour réduire la consommation énergétique, la latence et recouvrir au mieux le réseau lors de pannes inattendues.

3.3.3.2.1. Les topologies plates

Cette topologie qui est une approche ‘‘Data Centric’’ permet la réduction de l'énergie de consommation (prolongation de la durée de vie des nœuds) [149]. Ces topologies sont souvent sujet de WSN de forte densité, de large recouvrement et mobilité tel que les WSN de surveillances. Parmi de protocoles de routage de topologies plates on trouve:

A. Le protocole PEQ (Periodic, Event-driven, Query-based)

Cet algorithme est fiable et de faible latence [1]. Il présente un recouvrement rapide en cas de panne en conservant l'énergie. PEQ combine la conservation d'énergie avec le routage multi-chemins en sélectionnant parmi toutes les routes disponibles, celles qui consomment moins d'énergie. En plus de ce mécanisme préventif qui permet un routage fiable, un mécanisme de recouvrement de pannes est implémenté. Si un chemin est rompu, il le remplace par une autre route qui présente des liens fiables et consomme moins d'énergie.

B. Le protocole EAR (Energy and Activity Aware Routing)

C'est une solution hybride pour la tolérance aux pannes [147]. C'est un protocole préventif qui offre une meilleure conservation d'énergie et définit plusieurs chemins de routage afin de garantir une fiabilité de transport et d'augmentation de la durée de vie du réseau. En outre, un mécanisme de recouvrement de pannes est implémenté. Le protocole EAR supporte des réseaux de capteurs avec de nœuds capteurs multiples. Chaque nœud capteur génère un paquet RPT (Report) contenant des informations pour les intérêts et préférences de l'utilisateur. Les paquets RPT peuvent être envoyés vers n'importe quel collecteur. Ce protocole offre aux nœuds capteurs les meilleurs chemins en termes de réduction d'énergie de consommation et de latence. Ce protocole offre un recouvrement de panne.

C. Le protocole VTRP (Variable Transmission Range Protocol)

C'est une solution de variation du rayon de transmission pour une meilleure propagation de données [1]. Afin d'éviter le problème d'obstacles, VTRP augmente le rayon de transmission. Ce dernier augmente la probabilité d'atteindre des nœuds capteurs limites actifs quand le rayon actuel utilisé ne couvre aucun nœud capteur à cause de pannes ou d'inactivité des nœuds capteurs voisins, ou encore dans le cas des réseaux à faible densité. Alors, VTRP offre une meilleure longévité du réseau en évitant l'utilisation fréquente des nœuds capteur critiques (les voisins proches du collecteur). Ceci permet donc d'alléger la fonction de routage, de conserver la batterie et d'augmenter ainsi la durée de vie de tout le réseau.

L'ensemble de ces protocoles trouvent leurs applications dans les WSN mobiles qui sont de forts changements de topologies.

3.3.3.2.2. Les topologies hiérarchiques (Clustering)

Les protocoles adaptés à cette topologie éliminent le problème d'auto-organisation du réseau. Ils divisent le réseau en un ensemble de clusters ayant chacun un coordinateur (cluster head) qui récupère les données depuis tous les nœuds capteurs de son cluster puis les achemine vers le collecteur. Cette solution permet de mieux gérer le trafic de réseau. Ils permettent aussi de réduire la quantité d'information qui circule, en effectuant des traitements au sein du cluster avant de propager les données vers le reste du réseau pour les transmettre au collecteur. Ces topologies sont de couvrement moyen et de mobilité modérée.

A. Protocole CPEQ (Cluster-based PEQ)

Il y a ajout d'un module de clustering au protocole PEQ pour offrir une meilleure gestion de routage. Les nœuds capteurs ayant le plus d'énergie résiduelle sont sélectionnés comme nœuds agrégateurs (appelés aussi cluster head ou hub) [1]. Un nœud agrégateur établit son cluster, et les nœuds capteurs appartenant à ce dernier envoient leurs données au nœud agrégateur qui effectue d'éventuel traitement sur les données brutes puis les achemine vers le collecteur. Chaque nœud capteur du réseau peut devenir agrégateur pendant une certaine période de temps selon son niveau de batterie. Le but principal de CPEQ est la distribution uniforme de dissipation d'énergie entre les nœuds capteurs, et la réduction de la latence et du trafic de données dans le réseau.

B. Le protocole k-CDS

L'algorithme K-CDS utilise une approche préventive basée sur le clustering. Il propose une construction d'un ensemble k-connexe dominant k-CDS (k-Conncted k-Dominating Set) comme un ‘‘backbone’’ virtuel pour offrir une efficacité de routage aussi bien qu'une bonne tolérance aux pannes [1].

C. Le protocol ‘‘KAT mobiliy’’ (K-means And TSP-based mobility)

En plus du clustering, le concept de mobilité est implémenté au niveau des nœuds collecteurs. Ensemble, ‘‘K-means’’ et ‘‘TSP-based mobility’’ définissent une technique préventive hybride tolérante aux pannes qui offre une meilleure gestion d'énergie et augmente donc la durée de vie du réseau. Après réorganisation du réseau en clusters, la méthode proposée pilote le collecteur mobile pour se déplacer à travers les centres des clusters en prenant le chemin

optimal [1]. Le collecteur mobile récupère donc les données depuis les capteurs des clusters visités. Le principe de ‘‘KAT mobility’’ se résume en deux procédures: clustering et optimisation du chemin de routage.

D’autres protocoles de routage hiérarchique basés sur la classification spectrale dans les WSN existent, tels que les protocoles proposés par Ali J. [143] :

- ✓ LESCA (Location-Energy Spectral Clustering Algorithm).
- ✓ MR-KSCA (Multi-Relay K-way Spectral Clustering Algorithm).
- ✓ MHCA-SC (Multi-Hop Clustering Algorithm based on Spectral Classification).

Ces protocoles divisent le réseau WSN en clusters locaux, disjoints et équilibrés, et affectent un Coordinateur (Cluster head) pour chacun. Ces protocoles permettent d'optimiser la consommation d'énergie des capteurs par:

1. La définition d’un nombre optimal de clusters.
2. Eviter la formation périodique des clusters.
3. Le placement uniformément des Cluster head à travers le WSN.
4. La distribution de la dissipation d'énergie sur l'ensemble des nœuds capteurs.

3.4. Conclusion

Cette revue quasi-exhaustive permet de situer et comprendre les enjeux et défis dans la gestion des WSN. Dans la littérature consultée, tous les auteurs supposent qu’il y a toujours un chemin vers la station de base via des nœuds intrinsèques, et dans les pires cas, ils pensent au ré-déploiement (exemple : situation où des nœuds sont détruits) [141].

Les WSN comme déjà prouvé constituent désormais la plateforme de l’IOT. Les objets diffèrent en technologie et en fonction, ce qui induit des WSN de nœuds hétérogènes qui doivent communiquer ensemble. Après une consultation très exhaustive de toutes les techniques publiées et de celles prises en charge dans certaines applications et surtout de l’urgence en termes d’objet IOT nouveaux et à promouvoir, on a pensé à l’adaptation de la technologie PSN (Pocket Switched Network) pour y mettre en œuvre des mécanismes qui garantissent particulièrement un lien sécurisé vers un nœud cible ou vers la station de base. Cette technique PSN constituera le prochain chapitre.

Chapitre 04

Chapitre 04 : La technologie PSN

4.1. Introduction

La technologie Pocket Switched Network (PSN) est dérivée de la catégorie d'un des plus anciens réseaux connus sous le nom ICMANET (Intermittently Connected Mobile Ad hoc Network) qui est un réseau mobile ad hoc dont les connexions sont par intermittence, il est également connu sous le nom de Delay Tolerant Network (DTN) [150]. Rappelons qu'ICMANET/DTN est l'un des domaines bien établis dans le patrimoine de la communication sans fil. L'architecture de réseau est ainsi proposée pour fonctionner correctement avec des délais d'attentes de connectivité et de ressources de point-à-point limités [151]. Les réseaux de cette classe sont potentiellement déployés dans des environnements difficiles conçus d'appareils mobiles isolés ayant des ressources limitées. Donc il est différent des réseaux ad hoc mobiles traditionnels (MANET). Dans un ICMANET, les chemins entre deux nœuds sont intermittents et la communication est établie uniquement par des chemins à sauts multiples entre deux nœuds. Cela signifie qu'il n'y a pas de chemins directs de bout en bout entre les nœuds. L'architecture DTN peut résoudre les problèmes d''interopérabilité entre les réseaux contestés (caractérisés par la latence, la limitation de la bande passante, la probabilité d'erreur et la distance entre les nœuds ou la stabilité du chemin). Les concepts de région et de passerelle sont inclus dans l'architecture DTN et les nœuds situés à la limite des régions sont utilisés comme points d'interconnexion entre des protocoles de réseaux différents. DTN peut être utilisé pour changer le modèle de base du service, l'interface du système et enrichir les performances dans certains réseaux [151].

Dans ce chapitre, on commencera par définir la technologie PSN. Un aperçu général sur les différents principaux protocoles de routage classés en six grandes catégories et les défis face à l'application de la technologie PSN seront présentés. On terminera ce chapitre par lister les domaines d'application de PSN et le standard de communication adapté.

4.2. Définition de la technologie PSN

Comme on a déjà parlé, le PSN appartient à la catégorie des DTN. PSN et DTN diffèrent principalement au niveau de leurs transporteurs d'informations. Le PSN est indépendant de la connectivité de bout en bout entre humains, et il peut fournir de meilleurs résultats dans un environnement dur que TCP/IP ne peut pas gérer. En DTN, les déconnexions radio entre les

appareils présentent le problème récurrent majeur [152,153]. Le DTN utilise des équipements intelligents pour fournir des informations [154], tandis que le PSN n'utilise que des personnes (téléphones mobiles ou plus précisément, les smartphones). Il fonctionne sans aucune aide et sans aucune structure spécifique. Dans le PSN, la transmission se fait sous forme de modèle Store-Carry-Forward (SCF) [9]. Le téléphone mobile est pour stocker les messages. Le mouvement des personnes est pour le transporter. Des liaisons radio à courte portée [10,11] devaient l'acheminer. L'ultrason [12,13], le Bluetooth et le WIFI [14,15] en font partie. Le problème dans le réseau mixte est comment accomplir l'interopérabilité entre leurs différents nœuds [155,156]. Abdelkarim C. [157] et Scott B. [158] proposent des protocoles Bundle pour résoudre ce problème.

4.3. La catégorisation des protocoles de routage dans PSN

Il y a six grandes catégories de protocoles de routage utilisés dans la technologie PSN[159]:

4.3.1. Catégorie 1: Protocoles de routage basés sur les contacts

Cette catégorie contient les protocoles de routage les plus simples pour lesquels l'historique de réseau n'est pas nécessaire pour la réussite de la transmission de données. Ils sont très faciles à comprendre et à mettre en œuvre. Ils ne transfèrent les messages que lorsqu'ils sont en contact avec les nœuds destinataires ou dans certains cas avec les nœuds relais choisis en fonction de divers critères. Parmi les protocoles de cette catégorie, il y a le routage ‘‘Direct Delivery’’ et le protocole de routage ‘‘First Contact’’ [160-161].

4.3.1.1 Protocole de routage ‘‘Direct Delivery’’

Pour ce protocole, le message du nœud source est livré au nœud cible via une communication directe. Une seule transmission de message est effectuée entre le nœud source et le nœud de destination par contact direct. Donc, c'est un protocole à saut unique, pas de nœuds intermédiaires [160, 162, 163]. Ainsi, ce protocole n'a pas besoin de connaissances préalables sur le réseau (Historique de transmission des messages précédents des nœuds, nombre de nœuds dans le réseau, etc.). La figure 4.1 illustre le processus de ce routage. Ici, le nœud source A sauvegarde un message pour le nœud de destination D. Avant d'atteindre le nœud cible, le nœud source A accumule le message dans sa mémoire tampon [164].

Avantages: Ce protocole garantit un coût de communication minimal. Le taux de réplication des messages est nul, ce qui élimine le problème de congestion.

Inconvénients: ‘‘Direct Delivery’’ présente des inconvénients tels que les retards de livraison élevés et les faibles taux de livraison (fortes chances que le nœud source ne contacte jamais le nœud de destination) [162].

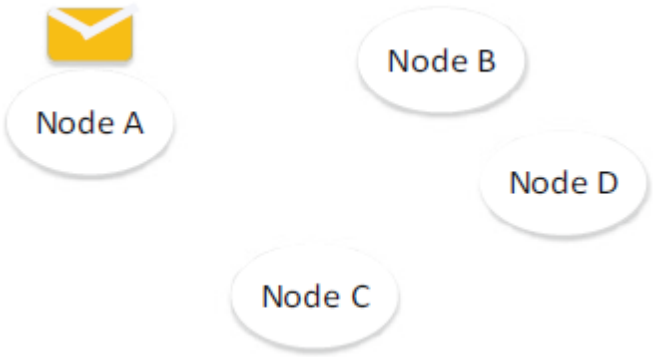


Figure 4. 1. Mécanisme du routage ‘‘Direct Delivery’’ [159].

4.3.1.2. Protocole de routage ‘‘First Contact’’

Le protocole de routage ‘‘First Contact’’ est presque similaire au protocole de routage ‘‘Direct Delivery’’ [160, 162, 163]. Mais dans ce protocole de routage, le message source n'est transféré qu'au premier nœud qui se trouve dans la plage de contact et qui lui-même va prendre la responsabilité de transmission du message au nœud destination [160-162, 165]. Après la réussite de transmission du message, le nœud source ou le nœud intermédiaire supprime la copie de message de sa mémoire tampon. Cela assure qu'une seule copie du message est présente dans le réseau et garantie ainsi l’utilisation minimale des ressources réseau. La possibilité de perdre cette seule copie du message est souvent due à la défaillance de nœuds ainsi que les débordements de buffer [160]. En outre, les nœuds relais qui transmettent les messages sont sélectionnés de manière complètement aléatoire sauf le premier nœud. Les nœuds du prochain saut ne sont sélectionnés que sur la base d'éventuelles caractéristiques des nœuds ou du réseau tels comme l'historique de sélection du nœud relais précédent, la probabilité d'atteindre la destination, …etc. Par conséquent, le meilleur nœud de routage n'est pas toujours sélectionné [160-162]. De plus, un seul nœud n'est sélectionné qu'une seule fois. Cela signifie que si un nœud a déjà transmis un message, il ne sera plus sélectionné pour le transfert du même message.

Avantages : l'avantage de ce protocole est que le plan de transfert de message est simple, unique, et facile à mettre en œuvre. Pas de congestion grâce à l'utilisation minimale des ressources réseau; une surcharge minimale de transmission des messages, le besoin seulement des connaissances sur le réseau local et un taux de réplication des messages nul.

Inconvénients: Le choix correct des nœuds de sauts n'étant pas toujours assuré, ceci entraîne des retards de livraison élevés(latence). Ce protocole n'est donc pas capable de garantir la bonne livraison du message au nœud cible produisant, ainsi, un faible rapport de livraison [160].

4.3.2. Catégorie 2: Protocoles de routage basés sur l'inondation (Flooding)

Ces protocoles de routage basés sur l'inondation fonctionnent principalement en inondant le réseau par la propagation des messages. Divers types d'algorithmes de routage basés sur l'inondation ont été introduits tout en exploitant le nombre de répliques de messages avec les nouveaux concepts de la mobilité humaine [166] et le contrôle de la vitesse de diffusion des messages [167]. Pour cette catégorie, on trouve le protocole de routage Epidémique [168], ''Spray and Wait'' [167], ''Human- Mobility Based Spray and Wait'' (HMSaW) [166].

4.3.2.1. Le protocole de routage Epidémique

Le protocole de routage Epidémique est parmi l'un des protocoles de routage basés sur l'inondation les plus populaires et les plus utilisés dans DTN [168-170]. Son mécanisme de travail comprend la réplication du message source et son transfert avec succès à tous les nœuds à sa portée de communication. Chaque nœud recevant ce message est dit infecté par le nœud source. Chaque nœud infecté sera, à son tour, un nœud infectant les autres nœuds à sa portée de communication et ainsi de suite.

Sur la figure 4.2, les cercles gris représentent les nœuds mobiles d'un réseau particulier. Les régions en pointillés sont utilisées pour représenter la portée de communication de chaque nœud. S est le nœud source, D est le nœud de destination et C1, C2 et C3 sont les nœuds voisins. Le nœud source inonde les messages vers les nœuds relais C1 et C2 (figure 4.2.a). Ensuite, le nœud C2 rencontre un nouveau nœud C3 qui transmet enfin le message au nœud de destination D (figure 4.2.b) [168].

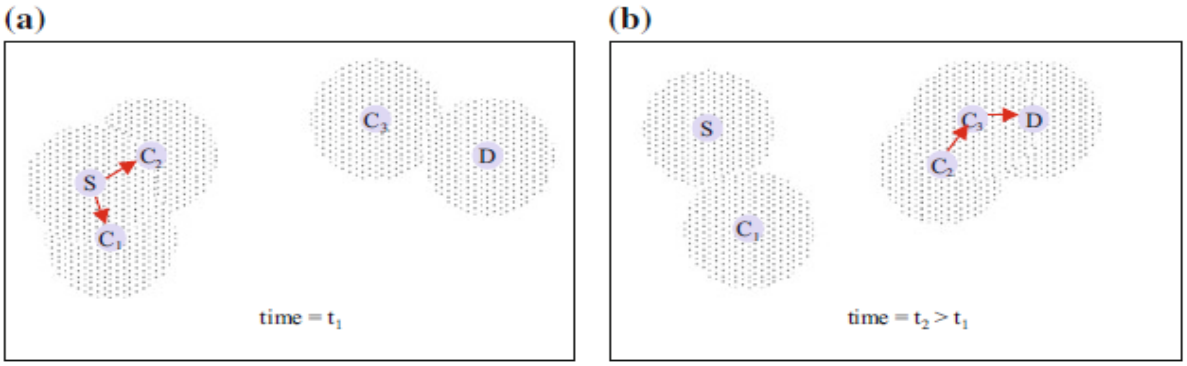


Figure 4. 2. Mécanisme du routage épidémique [9].

Après avoir atteint le nœud cible, pour contrôler la propagation des répliques de message, un system dit ‘‘IMMUNE’’ est maintenu où un ‘‘anti-paquet’’ est conservé à chaque nœud pour l'arrêt de l'inondation supplémentaire de ce message [170].

Avantages: Ce protocole présente un taux de livraison élevé, une faible latence, et une technique de transfert relativement moins compliquée.

Inconvénients: Les inconvénients majeurs de ce protocole sont la réutilisation des ressources, la congestion du trafic et la surcharge de transmission de message élevée. Ces inconvénients sont dus éventuellement à la transmission du message à tous les nœuds du réseau. Le message source continue d'être transféré et répliqué dans le réseau même après que la copie du message a atteint avec succès le nœud destination [162].

4.3.2.2. Le protocole de routage SaW (Spray and Wait)

Il utilise la rapidité du protocole de routage épidémique [161, 168] avec un nombre limité de copies de message. Il est simple et utilise le minimum de ressources réseau. L’énergie appliquée est celle du protocole de routage ‘‘Direct Delivery’’ [160, 162, 163]. Ce protocole fonctionne en deux phases [167]:

Phase Spray: Tous les messages générés à partir du nœud source auront un nombre N de ‘‘réplicas’’ qui seront transférés aux N premiers nœuds de transfert rencontrés.

Phase Wait : Lorsque le nœud cible n'est pas atteint pendant la phase Spray, chaque nœud relais ayant des copies de message attend jusqu'à ce qu'ils aient la chance ou la possibilité de

communiquer directement avec le nœud de destination (le message sera transféré en utilisant la transmission ‘‘Direct Delivery’’).

Ce protocole dispose de deux modes : Le mode normal et le mode ‘‘Binary Spray and Wait’’.

A-Mode normal : un nœud porteur de message transférera ce dernier à chaque nœud rencontré n’ayant pas la copie du message dans son buffer [171].

B-Le mode ‘‘Binary Spray and Wait’’ : Si un nœud P a plusieurs copies de message, et que le suivant nœud de transfert Q n'a pas de copies de message dans ses tampons, alors le nœud P transférera la moitié de ses copies à ce dernier. D'autre part, si le nœud P n'a qu'une seule copie du message, alors P passera en phase Wait et adaptera le protocole de transmission ‘‘Direct delivery’’ (transfert uniquement vers le nœud de destination). Sinon, le nœud P continuera à transférer la moitié de ses copies de message aux nœuds du prochain saut. Ce modèle de transmission continuera jusqu'à ce que le buffer du nœud P n'ait qu'une seule copie du message [160, 162, 166].

Avantages: Ce protocole présente un taux de livraison élevé, un nombre limité de messages répliqués, une latence moyenne, utilisation limitée des ressources, moins de congestion du trafic, et une surcharge limitée du nombre de messages transmis par rapport au routage Epidémique [162, 171].

Inconvénients: Malgré ces avantages, ‘‘Spray and Wait’’ a Peu d’efficacité dans les grands réseaux réels. La détermination de nombre de messages répliqués est difficile, car il nécessite des connaissances préalables sur l'ensemble du réseau. La sélection aléatoire du nombre de nœuds relais empêche la connaissance réelle du taux de livraison global [162, 171].

4.3.2.3. Le protocole de routage HMSaW (Human- Mobility Based Spray and Wait)

C’est l’amélioration de l'algorithme de routage ‘‘Spray and Wait’’ [167] en utilisant le concept du modèle de mobilité des humains. Une métrique dite ‘‘Weight Relay’’ est évaluée pour tous les nœuds résidant dans le réseau jusqu'au nœud de destination. Cette métrique est mesurée au moyen des marches humaines métriques qui aideront éventuellement à déterminer les probabilités de livraison [166]. Le système de routage HMSaW comporte également deux phases [167], la phase Spray et la phase Wait.

A-Phase Spray: Le choix d'un nœud inactif comme nœud relais soulève de nouveaux problèmes tels que le transfert de la moitié des messages vers ce type de nœud relais et qui finira par diminuer le taux global de livraison. Initialement, un nombre fixe de messages répliqués est généré. Tous les nœuds du réseau à l'aide du message de découverte de voisin déterminent leurs nœuds voisins et transfèrent les messages aux voisins de ‘‘Weight Relay’’ les plus élevés dans la plage de transmission. De plus, le message sera supprimé du buffer d'un nœud s'il a été reconnu par un nœud de transfert ou si la taille de sa mémoire est pleine.

B-Phase Wait: La phase Wait commencera au moment où il reste une seule copie du message à transférer. Le message sera transféré via le processus de transmission ‘‘Direct Delivery’’ au nœud cible.

L’avantage de ce protocole est la résolution des problèmes associés au protocole de routage ‘‘Spray and Wait’’ [167], tel que le taux de livraison qui est plus élevé. Il présente aussi une limitation de la surcharge de messages transmis, et une latence relativement faible que PROPHET (détaillé dans la section 4.3.3.1) [172].

4.3.3. Catégorie 3: Protocoles de routage basés sur des modèles probabilistiques

Les protocoles de routage de cette catégorie doivent calculer la probabilité de choix du nœud de transfert le plus approprié pour transférer le message vers la destination en fonction de divers facteurs ou paramètres. Ces facteurs sont l'état de la connexion entre une paire de nœuds, la taille de la mémoire tampon, la consommation d'énergie, la bande passante, la vitesse, la popularité …etc. Les routages les plus connus de cette catégorie sont PROPHET (Probabilistic ROuting Protocol using History of Encounters and Transitivity) [172], I-PROPHET [173] et PROPHET+ [174].

4.3.3.1. Le protocole de routage PROPHET (Probabilistic ROuting Protocol using History of Encounters and Transitivity)

Pour ce protocole la probabilité de livrer le message d’information à un nœud transitif est basée sur l’historique de la rencontre des nœuds [172]. Ici, le modèle de mobilité des utilisateurs a été considéré comme aléatoire; où les nœuds ou les utilisateurs qui se rencontrent ont régulièrement une probabilité plus élevée d'atteindre le nœud de destination que les autres. Cette probabilité est utilisée pour transférer les messages vers le nœud cible ainsi que pour réduire la congestion du trafic dans le réseau. Mais aussi pour diminuer la surcharge des messages de

communication pour chaque nœud [160,166, 175]. La figure 4.3 illustre la procédure de travail de l'algorithme de routage de type PROPHET. Le nœud source est A alors que le nœud de destination est D. Le nœud B, ainsi que le nœud C fonctionnent comme des nœuds intermédiaires pour transférer le message du nœud A au nœud D en fonction de leur probabilité de la livraison du message [172].

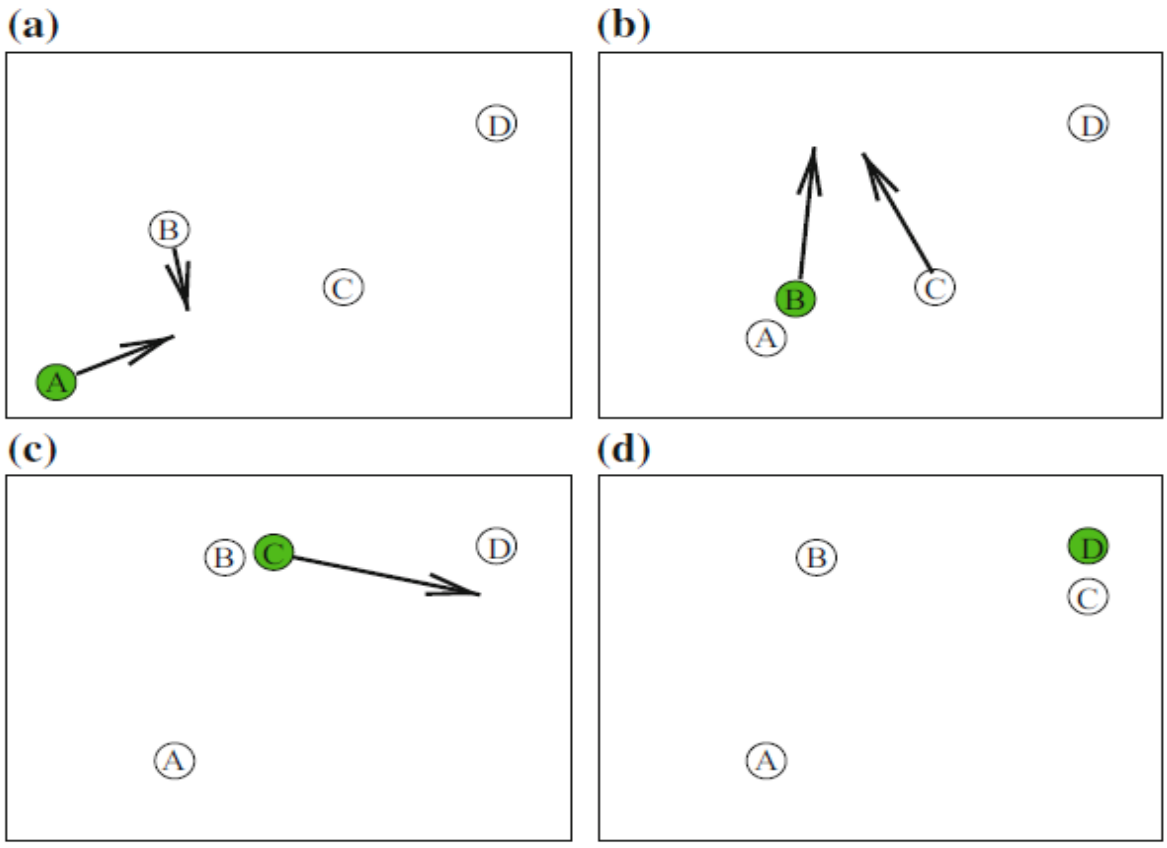


Figure 4. 3. Procédure de l'algorithme de routage de PROPHET.

Le calcul des probabilités de livraison s'établit sur trois parties différentes.

Partie 1 : Lorsque deux nœuds se rencontrent, ils partagent leur information de prévisibilité de livraison des copies du message. Ces informations sont transférées dans la forme d'une métrique probabiliste nommée '' prévisibilité de livraison'' qui est ajustée après chaque rencontre de nœuds, ce qui aide à déterminer les nœuds de saut appropriés (illustrés dans l'équation (4-1)). Ici, P_{init} est la constante d'initialisation.

$$P_{(a,b)} = P_{(a,b)_{old}} + \left(1 - P_{(a,b)_{old}}\right) \times P_{init} \qquad (4-1)$$

Partie 2 : Si deux nœuds sont déconnectés pendant un certain temps, la valeur métrique probabiliste commence à se dégrader, comme indiqué en (4-2). Ici, $P_{(a,b)}$ définit la métrique de probabilité d'un nœud a, pour chaque nœud de destination inconnu b. La constante de vieillissement est γ^k où k est le temps écoulé depuis le dernier vieillissement de la métrique.

$$P_{(a,b)} = P_{(a,b)_{old}} \times \gamma^k \qquad (4-2)$$

Partie 3 : Les multiples rencontres de nœuds sont également utilisées pour calculer la propriété de la prévisibilité de la livraison transitive. L'équation (4-3) montre que si des fréquentes réunions ont eu lieu entre le nœud a et le nœud b ainsi que pour le nœud b et le nœud c, alors le nœud c est un nœud apte pour un saut du nœud a. β est la constante d'échelle.

$$P_{(a,b)} = P_{(a,b)_{old}} + \left(1 - P_{(a,b)_{old}}\right) \times P_{(a,b)} \times P_{(b,c)} \times \beta \qquad (4-3)$$

Lorsque deux nœuds se rencontrent, leurs probabilités de livraison sont échangées. Si la probabilité du nœud rencontré est plus élevée que le nœud porteur, alors le message est transféré à ce dernier. Sinon, le message reste dans la mémoire buffer du nœud transporteur jusqu'à ce qu'il rencontre un nœud avec une probabilité de livraison plus élevée [172].

Trouver un nœud de saut efficace dans un temps limité (TTL: Time To Live) avec une probabilité de livraison plus élevée est une tâche difficile. De plus, il y a un risque de ne jamais trouver le meilleur nœud relai [172].

Avantages : Ce protocole de routage a des performances plus élevées que celles des protocoles de routage : ''Direct Delivery'' [160, 163], Epidémique [161, 168] et ''First Contact'' [160]. Il est parfaitement adapté aux réseaux étendus. Le PROPHET présente une transmission de messages modérée avec un faible coût de frais de communication et un rapport de livraison élevé que le protocole de routage Epidémique [172].

Inconvénients : l'historique des rencontres de nœuds ou la prévisibilité de la livraison des messages est calculé et stocké dans chaque nœud ; par conséquent, ce protocole de routage est caractérisé par une utilisation de mémoire des ressources trop élevée, en particulier dans les réseaux larges et denses [162, 172]. La copie du message n'est transmise qu'aux nœuds rencontrés avec des probabilités de livraison élevées, ainsi les nœuds ayant des voisins avec des

probabilités de livraison élevées perdent parfois leur chance de fonctionner en tant que nœuds relais. Ce mode présente aussi une latence élevée [173].

4.3.3.2. Le protocole de routage I-PROPHET (IMPROVED PROPHET)

Ce mode améliore le protocole de routage initial PROPHET [172] en essayant de réduire ses limitations. I-PROPHET a été initialement proposé par Fuquan Z. [173]. Pour ce protocole, la découverte d'un nœud relai ne dépend pas seulement de la probabilité de se rencontrer, mais aussi des connexions affectées par le temps et la distance entre les nœuds afin d'atteindre le nœud de destination [173].

L'équation (4-4) est utilisée pour calculer la probabilité de livraison entre deux nœuds. Ici, le cycle de communication est T_{sum}, le temps de connexion de la communication est T_{con} et P_{init} est une constante d'initialisation.

$$P_{(a,b)} = P_{(a,b)_{old}} + \left(1 - P_{(a,b)_{old}}\right) \times P_{init} \times (T_{con} / T_{sum}) \qquad (4-4)$$

Si les nœuds a et b ne se rencontrent pas pendant un certain temps, la probabilité de la livraison décroit en fonction de γ (la constante de vieillissement) et T_{brk} est le temps de déconnexion (break) de la communication (équation (4-5)).

$$P_{(a,b)} = P_{(a,b)} \times \gamma^{T_{brk}} \qquad (4-5)$$

L'équation (4-6) qui est la même que celle du modèle PROPHETE [172] montre que la propriété transitive de la probabilité de livraison et son impact sont déterminés par la constante d'échelle β. Si le nœud a visité à plusieurs reprises le nœud b et que le nœud b rencontre souvent le nœud c, alors le nœud b peut fonctionner comme un pont de communication entre le nœud a et le nœud c.

$$P_{(a,b)} = P_{(a,b)_{old}} + \left(1 - P_{(a,b)_{old}}\right) \times P_{(a,b)} \times P_{(b,c)} \times \beta \qquad (4-6)$$

Avantages : Il y a résolution des problèmes associés à l'état du lien ou à l'état du chemin. De meilleures performances, par rapport au PROPHET [172] en termes de taux de livraison, de taux de surcharge (taux de messages envoyés) et la latence, peuvent être obtenues.

Inconvénients : La prévisibilité de la livraison et le tableau d'état des liens sont calculés et stockés dans chaque nœud ; par conséquent, une utilisation élevée de mémoire et de ressources réseau, en particulier dans les réseaux larges et denses [162, 172, 173].

4.3.3.3. Le protocole de routage PROPHET+

Ting-Kai Huang et al. [174] ont proposé un algorithme de routage étendu de PROPHET [172] appelé PROPHET+. Ils ont essayé d'améliorer l'algorithme du PROPHET [172] en introduisant une nouvelle fonction pondérée ; cependant, la valeur de prévisibilité de l'algorithme PROPHET [172] a encore plus d'importance dans les événements de décisions de routage. Leur fonction pondérée permet de déterminer la valeur de livraison pour sélectionner les meilleurs chemins de routage en tenant compte de la taille du buffer, de la puissance, de la bande passante, et la popularité. Cette fonction est décrite par l'équation (4-7). Ici V_D est la valeur de livraison et V_R est la valeur de prévisibilité du PROPHET [172], où W_B, W_P , W_A, W_O et W_R représentent respectivement les poids de la taille du tampon, de la consommation d'énergie, de la vitesse de la bande passante, la popularité d'un nœud particulier et la valeur de prévisibilité. Ces poids pourraient être modifiés pour s'adapter aux différents types d'environnement et situations. Leur système de routage proposé a réussi à réduire le délai de la transmission tout en augmentant le taux de livraison.

$$V_D = W_B(V_B) + W_P(V_P) + W_A(V_A) + W_O(V_O) + W_R(V_R) \qquad (4-7)$$

Avantages : Ce protocole fournit des taux de livraison élevés et une faible latence par rapport à PROPHET [172]. Il détermine les meilleurs chemins de routage pour la transmission des messages en considérant d'autres paramètres en plus avec la valeur de prévisibilité du contact [174].

Inconvénients : PROPHET+ n'avait été évalué que par la mesure des paramètres de performances du taux de livraison et de délai de transmission; cependant, le taux de réplication des messages, le coût de surcharge de transmission et le taux des messages abandonnés n'ont pas été pris en compte. En plus, ce schéma de routage n'avait été comparé qu'à l'algorithme du PROPHET [172], cela ne garantit donc pas qu'il puisse fonctionner mieux que les autres algorithmes de routage. Enfin, l'ensemble de données utilisé est pris sur une longue durée de contact et selon leur hypothèse, les nœuds étaient tous des ‘‘meilleurs nœuds relais’’. Mais rappelons que pour PSN, ce genre de scénario n'est pas possible tout le temps et que le calcul des poids avant chaque transmission augmente la charge sur chaque nœud [174].

4.3.4. Catégorie 4 : Protocoles de routage basés sur la communauté

Les humains ou les nœuds qui se visitent fréquemment sont considérés comme appartenir à la même communauté. Avec ce concept, des communautés se forment, elles peuvent être de petites ou de grandes tailles en fonction du nombre de nœuds rencontrés. Ces communautés peuvent être à la fois séparées comme elles peuvent se chevaucher. Les communications entre ces communautés sont gérées par un nœud particulier ou un groupe de nœuds de la communauté locale [175]. Selon la variation du nombre de ces nœuds locaux utilisé pour la propagation du message au sein de chaque communauté locale, plusieurs protocoles ont été proposés. Parmi eux, ‘‘Bubble Rap’’ [176], HERO [177], et PNGP [178].

4.3.4.1. Le protocole de routage ‘‘Bubble Rap’’

Les communautés humaines sont formées en raison des modèles de mouvement social des humains et des caractéristiques de leurs comportements [9,179]. Des informations sur ces communautés humaines ainsi que les données du réseau social aident à prendre les décisions de transfert de message dans ce protocole de routage [9, 179]. Pour distinguer et identifier clairement chaque communauté, ‘‘Bubble Rap’’ utilise la méthode k-Clique qui n'est conçue que pour les graphes binaires. Mais les gens peuvent appartenir à plusieurs communautés simultanément, alors la gestion de ces graphes de contact devient cruciale [176,180]. Les techniques de transfert de données de ‘‘Bubble Rap’’ sont illustrées dans la figure 4.4. Ici, les cercles noirs représentent le nœud source et le nœud de destination. Le grand cercle est la communauté locale. Les cercles rouges sont les nœuds relais servant pour transmettre les données au nœud cible [178]. Les flèches vertes désignent la communication locale. Les flèches noires désignent la communication globale.

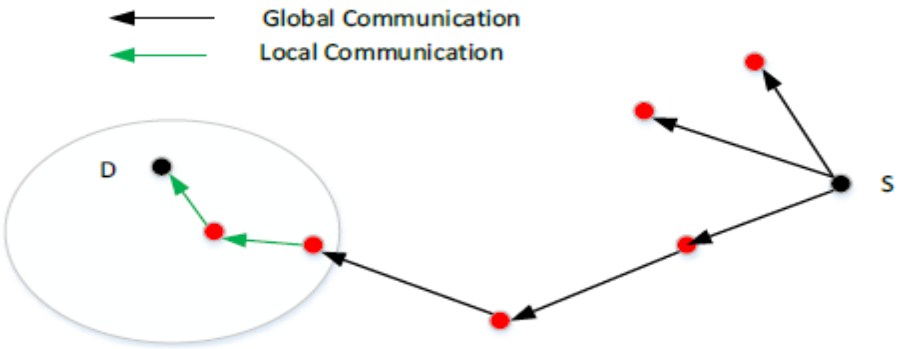


Figure 4. 4. Techniques de transfert de données ‘‘Bubble Rap’’ [9].

Avantages : Taux de livraison meilleur et coût de transmission faible par rapport au protocole de routage épidémique.

Inconvénients : l'identification de la communauté n'est pas facile, l'inondation de la communauté locale par les messages transmis augmente les taux de réplication des messages par rapport aux algorithmes de routage moderne. Si le nœud source résidant dans un réseau dense a un classement local faible, alors le réseau peut devenir encombré de copies de messages indésirables [162].

4.3.4.2. Le protocole de routage HERO (HomE based Relay selectiOn)

Les humains ont tendance à visiter peu d'endroits fréquemment que d'autres et ces endroits sont appelés ''maisons''. Huang et al. ont utilisé cette idée de '' nœud domestique'' dérivée de la cohérence spatiale de la mobilité Humaine dans la sélection de relais à domicile (HomE based Relay selectiOn: HERO) [177]. Ils ont proposé deux algorithmes qui ne nécessitent que des nœuds de saut pour le transfert des messages. Par conséquent, ils n'ont besoin que des données de routage locales et ne nécessitent pas d'information sur le routage global des messages [177].

4.3.4.2.1. Algorithme HERO de base

C'est l'un des algorithmes à copie unique et à saut unique du PSN. Dans le cas où la communication directe entre la source et la destination n'est pas possible, alors un nœud de saut sera sélectionné dans la maison pour jouer le rôle de ''nœud domestique''. Il va mémoriser les données jusqu'à ce qu'une communication directe avec le nœud cible ait lieu.

4.3.4.2.2. Algorithme HERO amélioré

Cet algorithme a été amélioré avec l'idée de la sélection de plusieurs sauts (relais) efficaces en fonction de l'intensité de la visite des zones (ou maison) de nœuds. Ces sauts augmentent éventuellement la probabilité d'atteindre le nœud de destination. Si le contact direct échoue, le nœud source choisira un nœud de saut avec l'intensité de visite la plus élevée (probabilité de visiter ou d'atteindre la destination) pour fonctionner comme un nœud domestique parmi ses nœuds voisins et il lui transféra le message. Ensuite, lui-même va transférer le message vers d'autres nœuds rencontrés s'ils ont comparativement une intensité de visite plus élevée que lui. Ainsi, le nœud nouvellement choisi fonctionnera comme un nœud de saut pour transférer les

messages vers le nœud cible. Ce phénomène de sélection des nœuds relais optimaux continuera jusqu'à ce que tous les messages aient atteint la destination.

Avantages : Aucune information globale n'est conservée. Ici, seuls les nœuds relais sont chargés de la mise à jour des informations ainsi que de la transmission des données, d'où ces deux algorithmes HERO sont caractérisés par une surcharge de communication et une mise en mémoire buffer des informations très faibles. Ils sont relativement stables. En plus, ils ne dépendent d'aucun modèle basé sur la mobilité humaine. Il y a utilisation de la distance jusqu'à la destination comme critères de sélection des nœuds, c'est donc relativement moins compliqué. La résolution du problème associé avec les nœuds de saut qui se transforment en goulots d'étranglement est détournée en essayant de les faire fonctionner en tant que nœuds relais entre différentes communautés. Notons que HERO peut changer d'un système d'algorithme de routage à copie unique à un système d'algorithme de routage à copies multiples à tout moment en fonction de la nécessité de propagation du message [177].

Inconvénients : les algorithmes HERO souffrent d'une phase de démarrage lente à grande échelle des réseaux. Il en résulte une faible propagation des données et conduit finalement à une transmission de données inefficaces [177].

4.3.4.3. Le protocole de routage PNGP (Popular Node Gateway Protocol)

PNGP est une version améliorée du ''Bubble Rap'' [176]. C'est aussi un protocole basé sur la communauté. Le nœud le plus populaire d'une communauté est sélectionné comme passerelle pour cette communauté particulière. Ici, si le nœud de la destination appartient à la même communauté que le nœud source, alors le message sera inondé sans aucun calcul au sein de cette communauté. Dans le cas où le nœud destination n'appartient pas à la communauté du nœud source ; si le nœud source rencontre un nœud qui appartient à la même communauté du nœud de destination, il doit vérifier sa popularité au sein de sa communauté. S'il s'agit du nœud le plus populaire, alors le nœud source inonde les messages vers ce nœud [4].

Avantages : Il surpasse avec succès les performances de son algorithme de base ''Bubble Rap'' [9, 176, 179]. Il présente des performances relativement meilleures qu'Epidémique [9, 168, 169,170], ''First Contact'' [9,155, 160, 161,162] et ''Bubble Rap'' [176] en taux de livraison, et en coût de transmission. Il est de latence moyenne.

Inconvénients : L'Idée d'utiliser le nœud le plus populaire comme passerelle pour fonctionner peut créer un goulot d'étranglement pour l'ensemble du réseau et induit une congestion des trafics dans le réseau, qui finira par réduire les performances globales. Les communautés sont supposées très petites, mais en réalité, les communautés peuvent être assez grandes et multiples, et peuvent même avoir des chevauchements [176].

4.3.5. Catégorie 5: Protocoles de routage basés sur les informations sociales

Les personnes sont dites ‘‘sociales par nature’’. La communauté des chercheurs a utilisé ce concept pour fournir des algorithmes pour la technologie PSN. Les personnes se rencontrent et discutent généralement avec ceux qui ont des intérêts similaires et ils ont l'habitude de visiter fréquemment quelques endroits, ce qui forme progressivement un modèle de mobilité humaine. En utilisant le concept d'information sociale sous les formes de la nature de l'amitié humaine, d'intérêts sociaux et modèles de mobilité humaine, plusieurs plans de diffusion des messages ont été présentés tels que le routage ‘‘Friendship Based Routing’’ [180], ‘‘Social Aware Networking’’ (SANE)) [181, 182], ‘‘Social Circle’’ [183] et ‘‘Chitchat’’ [184].

4.3.5.1. Le protocole de routage ‘‘Friendship Based Routing’’

Pour ce routage, la qualité de l'amitié est utilisée pour évaluer les amis proches (nœuds transmetteurs ou relais) variant dans diverses communautés d'amitié en fonction du temps. Selon Eyuphan B. [180], les amis proches ont certaines caractéristiques comportementales telles les rencontres fréquentes de longue durée et régulières. Pour déterminer la force de l'amitié entre deux nœuds, les métriques ‘‘Social Pressure Metric’’ (SPM) et ‘‘Conditional SPM’’ (CSPM) sont mesurées pour calculer leur pression sociale. L'amitié entre les nœuds varie également de la même manière que les amitiés humaines. Il existe deux types d'amitiés de nœuds : les amis directs et les amis proches indirects.

Amis directs : des connexions directes ou des liens de bonne qualité entre les nœuds sont déterminés à partir de leurs antécédents de contact qui sont utilisés pour identifier l'ami direct. Il aide éventuellement à calculer la SPM.

Les amis proches indirects : les nœuds se contactant fréquemment via leurs amis communs (utilisés comme nœuds de saut) sont dits amis indirects proches. La valeur CSPM est utilisée pour calculer les qualités de lien d'amitié.

*Stratégie de transfert de message : si un nœud P souhaite transférer un message à un nœud ami indirect R et leur ami commun est le nœud Q. Ensuite, pour que le nœud Q agisse en tant que nœud de saut, il doit appartenir à la même communauté d'amitié que le nœud d'objectif R et doit avoir une amitié plus forte avec le nœud R que le nœud P. Sans ces deux conditions, le nœud Q ne peut pas fonctionner comme nœud de transfert [178].

Avantages : Plus performant que PROPHET [172], il a un taux de livraison élevé, un coût moyen de transmission avec une efficacité de l'opération de routage.

Inconvénients : le calcul d'amitié des communautés à chaque période nécessite de l'espace mémoire et du coût. Ainsi, lorsque le nombre de périodes augmente, les besoins en espace mémoire augmentent également [9].

4.3.5.2. Le protocole de routage SANE (Social Aware Networking)

''Social Aware Networking''(SANE) est un protocole de routage basé sur les informations sociales. Il identifie de solides relations sociales entre les différents nœuds (utilisateurs) [181, 182]. Il exploite les caractéristiques des appareils portatifs (tels que le téléphone portable) en négligeant la condition additionnelle de stockage.

Tous les messages qui ont été transférés ont un profile d'intérêt cible (target Interest Profile) ou profile d'opportunité du message (message relevance profile), contenant N ''replicas'' (nombre de copies de message) et le TTL dans leurs entêtes. Deux services de communication, monodiffusion (Unicast) et diffusion par intérêt (Interest-cast) sont fournis dans [181, 182]. En monodiffusion, si les intérêts d'un nœud rencontré sont en grand partie communs avec ceux du nœud cible, il est alors choisi comme un nœud de saut (relai). Ici, le nombre des répliques et la taille de la mémoire buffer sont contrôlés avec une valeur seuil. Si N ''replicas'' augmente à l'infini, il fonctionne comme l'algorithme Epidémique [168] ; ou ''Spray and Wait'' [167,182]. De plus, lorsque la valeur seuil du relais = 0, il fonctionne comme ''Binary Spray and Wait'' [185]. Lorsque la valeur seuil du relais = 1, il fonctionne comme le routage ''Direct Delivery'' [160]. D'autre part, dans ''Interest-cast'', il utilise le profile d'intérêt pour diffuser les informations aux nœuds voisins de même profile d'intérêt.

Avantages: La comparaison avec ‘‘Binary Spray and Wait’’ [185], Epidémique [172] et ‘‘Bubble Rap’’ [176], montre bien que ce protocole améliore effectivement le délai moyen et le coût de transmission.

Inconvénients: En stockant tous les messages répliqués ainsi que la quantité substantielle d'intérêts sociaux, chaque nœud va donc souffrir d’une surexploitation de mémoire.

4.3.5.3. Le protocole de routage ‘‘Social Circle’’

La dynamique utilisant les concepts de modèles sociaux comme des relations sociales, est associée à un protocole de routage basé sur des arbres distribués [183, 186]. Des personnes ont tendance à communiquer avec des amis (personnes avec lesquelles elles partagent une relation solide) fréquemment que d'autres personnes. Les individus communiquent rarement ou jamais avec des personnes inconnues. Les gens ont généralement tendance à visiter fréquemment quelques endroits spécifiques à certaines périodes de la journée ; ce qui montre leurs modèles de mobilité dans le temps. Par exemples, les étudiants suivent des cours à l'université en suivant la même routine chaque semaine; les employés passent un certain temps dans leur bureau…etc. Par conséquent, les cercles humains sociaux ont cette nature interactive, qui est le concept de base du ‘‘social Circle’’. La figure 4.5 montre les modèles de mobilité des nœuds (humains) [183, 186].

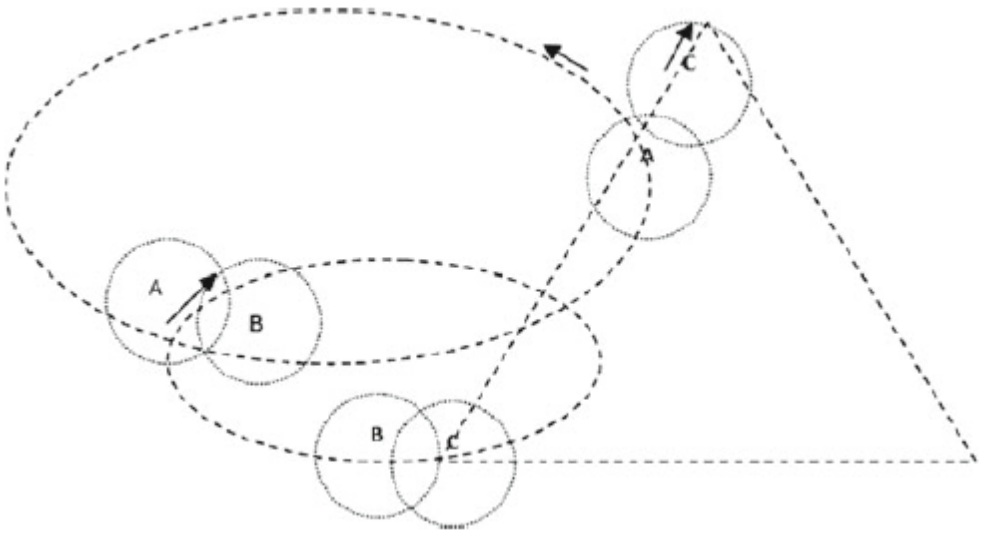


Figure 4. 5. Les modèles de mobilité des nœuds.

Dans ‘‘Social Circle’’, une table communautaire temporelle est maintenue pour garder la trace de la mobilité de l'ensemble du nœud voisin et de leurs horaires tout au long de la semaine; et génère leur réunion par précision. Pour la sélection du nœud de transfert, les concepteurs ont utilisé une liste d'amis et une liste des connaissances. Ces deux listes sont dépendantes l'une de l'autre. La liste d'amis affiche les nœuds ou amis communiquant régulièrement. D'autre part, la liste de connaissances conserve un enregistrement de tous les nœuds voisins du deuxième saut (ont rarement des communications directes). Pour transférer des messages aux communautés voisines ou aux nœuds de destination distants, des nœuds de connaissance sont utilisés. Afin d’accomplir cette tâche, le nœud de plus forte connaissance est sélectionné à l'aide de la table de sociabilité (Sociability Table (ST)). La table ST est formée avec le nombre de connaissances de chaque ami. En cas d'urgence de la livraison d’un message, le nombre de copies du message est modifié. De plus, un nœud ami est choisi de la table de la communauté temporelle pour accélérer le processus de livraison des messages [183, 186].

Mécanisme de routage : Les routages intercommunautaires et intracommunautaires sont utilisés pour la propagation du message. Pour le routage intercommunautaire, si la destination est incluse dans la liste d'amis, et que le message nécessite une livraison rapide, alors le message est directement transféré. Pour le routage intracommunautaire, la destination peut être connue ou inconnue. Si l'objectif est inconnu, alors en utilisant le ST, le message est transmis au plus grand nombre de connaissances avec une optimisation d’atteindre le nœud de destination. De plus, si la destination est connue, alors les nœuds amis correspondants sont inondés avec les répliques de message [183, 186].

Avantages: L'algorithme ‘‘Social Circle’’ a de meilleures performances que PROPHET [172] dans toutes les mesures de performance ; il indique des performances légèrement meilleures que le ‘‘Bubble-Rap’’ [176,187] en taux de livraison, latence, nombre de répliques et les liens d'utilisation. Selon l'urgence de la livraison du message, il peut basculer du protocole de routage à copie unique au protocole de routage à copies multiples [183, 186].

Inconvénients: l'ensemble de données choisi était très petit, il ne peut donc pas garantir son fonctionnement pour les grands réseaux. Le pourcentage de taux d'abandon des messages n'a pas été démontré [183, 186].

4.3.5.4. Le protocole de routage ‘‘ChitChat’’

Pour le ‘‘ChitChat’’ [188], D.McGeehan a essayé d'améliorer le protocole de routage SANE [182] en ajoutant de nouveaux concepts afin de minimiser les défis rencontrés dans le réseau faiblement connecté et améliorer les performances à un niveau visible [184](figure 4.6).

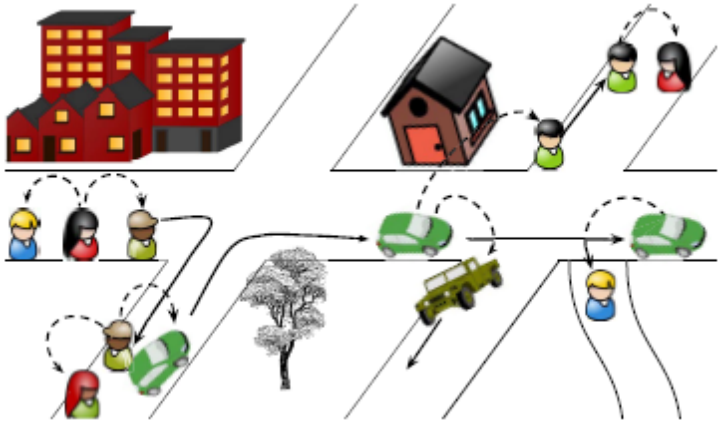


Figure 4. 6. Un exemple de PSN(ChitChat), où les flèches en lignes continues représentent le mouvement des véhicules et les flèches en lignes pointées représentent l’établissement des connexions et l’échange d’information [189].

Un ensemble d'intérêts sociaux (Social Interests : SI) uniques forme un profile social (Social Profile : SP). Pour confirmer les décisions efficaces de transmission de messages, une relation sociale transitoire (Transient Social Relationship : TSR) est utilisée. Ce protocole garde une trace du poids de chaque intérêt social qu'un utilisateur a dans son SP. Le modèle de relation sociale transitoire en temps réel (Real-time Transient Social Relationship : RTSR) aide les nœuds à réussir la transmission des messages ; et met à jour les poids des relations multi-sauts. Le poids de la TSR commence à se dégrader avec l’augmentation du temps de dé-connectivité avec les nœuds d'intérêt similaire. D'autre part, le poids commence à augmenter, si les nœuds restent connectés à un nœud d'intérêt similaire pendant une période plus longue. Dans la phase initiale, si deux nœuds sont présents dans la portée de communication, le modèle RTSR est automatiquement appelé à échanger les TSR ; et il est ajusté et mis à jour comme déjà mentionnée précédemment. Ensuite, l'algorithme achemine les messages vers leurs destinations basées sur l'analyse de l'intérêt des nœuds connectés [24].

Avantages : L’utilisation du modèle RTSR offre une solution indépendante du rang de communication ce qui permet au Chitchat d’être le deuxième protocole avec le plus haut taux

de livraison après Epidémique [159]. De plus, l'efficacité du mécanisme de transfert de messages, permettant la minimisation de la communication en général. Une fois que les nœuds de mêmes intérêts sont rencontrés, les messages sont directement transmis. Ainsi, il n'est pas nécessaire de stocker des données pendant une période plus longue, ce qui aide finalement le ''Chitchat'' à réduire le temps d'utilisation des tampons pour tous les nœuds [159,184].

Inconvenients : les performances de mesure des paramètres de latence et de taux d'abandon pour le ''Chitchat'' n'ont pas été comparées. Les concepteurs ont modifié le Geolife [159,165] simulés par leur algorithme proposé pendant 24 heures seulement. Ainsi, cette simulation ne révèle pas comment cela fonctionnera pour une période plus longue [159].

4.3.6.Catégorie 6: Protocoles de routage basés sur l'efficacité énergétique, ou les points d'accès (Hotspot or Energy Efficiency Based Routing Protocols)

Cette catégorie a été introduite pour lutter contre la rareté des points d'accès Wi-FI (APs). Les protocoles de cette catégorie cherchent toujours à trouver un point d'accès direct ou indirect filaire ou sans fil, en prenant en compte l'efficacité énergétique. ''Energy Efficient Phone to-Phone Communication Method Based on WiFi Hotspot'' (EPCWH) [189] fait partie de cette catégorie.

* EPCWH (Energy Efficient Phone to- Phone Communication Method Based on WiFi Hotspot)

Yongjian Y. et ses collaborateurs [189] ont pu trouver un compromis entre la consommation d'énergie limitée des téléphones portables et l'assurance d'une communication efficace entre eux dans les grands réseaux largement dispersés comme le PSN. Leur méthode proposée comprend la commutation entre le mode point d'accès et le mode client qui se fait par l'ordonnancement de ces commutateurs. Les téléphones en mode point d'accès perdent de l'énergie plus rapidement que les téléphones mode client ou du mode récepteur. Aussi les téléphones ont une énergie limitée et une batterie de durée de vie limitée. Les connexions ne peuvent être établies entre deux mobiles que lorsqu'ils sont dans les modes opposés (ex : point d'accés-client). Comme il peut y avoir un ou plusieurs messages dans le réseau, alors, Yongjian Y. et ses collaborateurs ont proposé deux différents schémas de communication [189]:

1. Lorsque le réseau a un seul message, il transfère le message aux téléphones sans la copie du message.

2. Aucun transfert n'est effectué entre deux téléphones ayant le même message unique ou n'ayant aucun message. D'autre part, une approche de commutation uniforme est adoptée, lorsque plusieurs messages existent dans le réseau. Le degré de propagation des messages et l'établissement de la connexion sont décidés en fonction de l'énergie dont dispose chaque appareil [189, 190].

Avantages: Ce protocole cherche à établir un compromis entre la conservation de l'énergie et la propagation des messages.

Inconvénients: Cette méthode propose un modèle de mouvement qui est basé seulement sur le routage Epidémique et le point d'accès de passage aléatoire (Random-way point). Cela ne peut pas assurer son efficacité pour les autres protocoles.

4.4. Les défis face à la technologie PSN

Le PSN peut être défini comme un paradigme de communication qui peut tirer parti de la mobilité humaine et de l'intranet. La réussite de livraison des données devient difficile en absence d'une connexion point à point permanente. Dans cette section, on discutera certains défis sur lesquels l'utilisation de PSN apporte des solutions. Ces défis sont désormais des balises pour les chercheurs qui désirent améliorer PSN [9].

4.4.1. La mobilité

Les PSN sont formés de communautés humaines et on doit donc y inclure la mobilité. Cela signifie que la mobilité des nœuds est un sérieux problème dans le PSN. Dans PSN, il est difficile de construire des chemins de bout en bout pour transmettre le message de la source à la destination, parce que la mobilité de l'utilisateur est indéfinie. En raison de la mobilité des nœuds, il devient imprévisible qu'un nœud rencontre un autre nœud du réseau. C'est pourquoi une connectivité continue de bout en bout est difficilement maintenue. Cela définit que le routage dans un tel réseau est de trouver un chemin temporel entre les sources et la destination [191], mais trouver un cheminement réussi pour les données sans une bonne connaissance de la topologie de réseau dynamique demeure est une tâche difficile [192].

4.4.2. Egoïsme

Comme PSN est formé par des êtres humains qui sont de nature ‘‘égoïste’’. Les humains commandant les appareils qui forment un PSN peuvent transmettre des données pour certaines destinations désirées et non pas pour d’autres. La nature ‘‘stocker-emporte-transfert’’ du PSN nécessite que les nœuds soient prêts à transporter les données des autres, mais la présence de nœuds égoïstes pose un grand défi pour réussir la transmission. Ainsi, des mécanismes sont nécessaires pour encourager les nœuds à transmettre des données et se débarrasser de leurs comportements égoïstes [9].

4.4.3. Transfert des données

Dans le PSN, le transfert de données s'effectue selon une certaine politique, car il prend en charge à la fois ‘‘le réseautage’’ des réseaux intranet et Internet. Dans le cas d'une connectivité locale (intranet), les nœuds transmettent les messages en fonction des connaissances de leur environnement local. Mais acquérir des connaissances précises sur l'ensemble de l'environnement local est un défi majeur, car le PSN est indépendant de toute infrastructure prédéfinie. Comme le PSN dispose de ressources limitées, la disponibilité d’espaces de stockage et d’énergie sont aussi des enjeux majeurs [9].

Dans le PSN, les données sont transmises aux nœuds transporteurs proches de la destination. Mais le principal défi réside dans le développement d'une méthode qui déterminera de manière appropriée un nœud porteur, qui assurera l’opportunité de la bonne transmission d’un message donné à sa destination.

Lorsque la connectivité globale est disponible, un nœud transmet les messages directement à d'autres nœuds appropriés qui sont globalement connectés. Trouver les nœuds qui sont globalement ‘‘connectés fortement’’ demeure un défi dans un réseau dynamique sans infrastructure.

4.4.4. La sécurité

Dans le PSN, le routage s'effectue par la collaboration et la dépendance entre les nœuds. Les nœuds doivent collecter et échanger des messages entre eux. Dans ce cas, les nœuds peuvent être confrontés à différents problèmes de sécurité. Comme les messages sont échangés entre un certain nombre de nœuds, ils peuvent donc être altérés, affectés ou modifiés par un nœud relais malveillant [193]. D'autre part, d'autres problèmes de sécurité peuvent survenir tels que la

redirection, l'écoute clandestine, le refus de service, l'empoisonnement, etc. Ainsi, des mécanismes d'incitation, comme ceux proposés par Marco Z. [194] pour le réseau de capteurs sans fil, devraient également être développés pour sécuriser et protéger la livraison des messages ainsi que pour préserver la confidentialité des utilisateurs dans le PSN.

4.4.5. Évolutivité et Regroupement

La plupart des protocoles de routage du PSN sont plats. Cette approche plate convient aux petits réseaux mais n'est pas évolutive. Dans ce cas, le regroupement (clustering) peut fournir un meilleur résultat qui peut créer des groupes de nœuds mobiles ayant le même modèle de mobilité dans un même groupe. Ainsi, les nœuds appartenant au même groupe peuvent s'entraider pour réduire les frais généraux, rendre le routage évolutif et également partager les ressources. Les approches de regroupement peuvent être utiles pour déployer de grands réseaux en différentes communautés [195]. Afin de découvrir les nœuds qui se chevauchent dans les réseaux complexes, l'approche de regroupement basée sur la mobilité des nœuds et leur compétition les uns avec les autres, en utilisant un mouvement déterministe aléatoire [196], peut être utilisée. Un autre type de technique de regroupement est discuté [197]. Selon Earl O. [197], chaque nœud, au sein d'une communauté, est supposé doté d'une étiquette qui informe les autres nœuds de son étiquette. Il offre une bonne connaissance des communautés pour transmettre les messages de la source à la destination et surtout améliorer considérablement l'efficacité de transfert. L'approche par regroupement est un domaine très important qui ne cesse d'attirer beaucoup de chercheurs. Les futurs travaux sur le PSN se chargeront inévitablement à mieux cerner cette question.

4.4.6. Gestion de l'énergie et du stockage

Les appareils mobiles portés par des êtres humains ont des capacités d'énergie et de stockage très limitées. Pour une transmission de données rapide et fiable, il devient déraisonnable d'utiliser une grande quantité de stockage et d'énergie. Les protocoles de routage PSN existant ne prennent pas en compte la faible consommation d'énergie et le faible espace de stockage dans leurs objectifs de conception. Selon Ratna R. [9], Cette gestion de l'énergie et du stockage peut être une métrique efficace pour évaluer le routage dans le PSN.

4.5. Application de PSN

L'objectif principal du PSN est de maintenir le lien réseau sous des conditions environnementales complexes et exigeantes. Cela inclut son adaptation avec les pannes matérielles ainsi que les pannes logicielles (protocoles). Le PSN qui ne nécessite l'assistance d'aucune infrastructure est applicable dans les régions rurales et en développement pour permettre une communication à faible coût. Les PSN peuvent fournir des communications en place là où la connectivité Internet a été interrompue en raison de défaillances de l'infrastructure.

4.5.1. Communication à distance

Il existe de nombreux projets de communication rurale dans les villages éloignés pour fournir l'accès à Internet. Parmi ces projets, il y a l'utilisation de la transmission asynchrone d'informations pour réduire le coût des communications. Comme exemple, le service de messagerie numérique Wizzy1 qui fournit un accès Internet à certaines écoles de village en Afrique du Sud. Le projet DAKNET [198] s'est concentré sur la fourniture de services Internet à faible coût dans les zones rurales de l'Inde. Il est suggéré l'utilisation des moyens physiques pour transmettre des messages à des zones qui ne sont pas connectées via des réseaux traditionnels, tels que le trafic aérien, routier, ferroutier…etc.

4.5.2. Gestion des catastrophes

Certains modèles sont utilisés pour la sécurité et la communication lors des catastrophes, pour rechercher et secourir les gens. Le modèle de mobilité post-catastrophe [169] inclut au départ l'impact des catastrophes sur le réseau de transport et les modèles de déplacement des personnes et des véhicules de secours.

4.5.3. L'analyse des réseaux sociaux

Le PSN peut être utilisé pour analyser un réseau social. De nombreux domaines de recherche, commençant par l'anthropologie, arrivant au E-commerce et à l'ingénierie, tous ont besoin d'une analyse des réseaux sociaux [199]. Comme PSN travaille avec les personnes, il peut être utilisé pour collecter des données entre les entités sociales, puis les utiliser pour mieux comprendre les implications, les relations et les modèles entre peuples. Ensuite développer de nouvelles applications pour nouveaux usages.

4.5.4. Détection des maladies

De nos jours, l'utilisation du PSN fournit une aide précieuse à la compréhension de la propagation des maladies dans le domaine de l'épidémiologie. PSN aide à suivre les gens collectant des données. Le suivi de la diffusion du VIH (virus de l'immunodéficience humaine), étude réalisée par Hashemian et al. [199], figure parmi les exemples réussis.

4.5.5. Détection de communauté

La détection de communauté est une utilisation très courante du PSN. A partir des données collectées à l'aide du PSN, les communautés ayant une plus grande modularité sont souvent regroupées. Des travaux réalisés sur les communautés sont référenciés par Jian S [163] et Ashish S [200]. Une autre application de la détection de la communauté par le suivi des données à l'aide du PSN pourrait être utilisée pour détecter les mouvements terroristes dans les jungles ou les déserts. Une autre utilisation de la détection communautaire via le PSN pourrait fournir des contrôles d'accès aux réseaux sociaux en détectant les groupes de personnes qui diffusent des ‘‘spams’’ dans les réseaux sociaux, tels que les travaux de Grier et al. [167]. Ainsi, une application de PSN a été très utilisée en Irak en 2014, lorsque le gouvernement irakien a restreint l’accès à Internet [201], permettant de contourner cette restriction de la disponibilité d’accès à un réseau global. Cette technique a été exploité à Hong-Kong, en 2014 toujours, lors des manifestations contre le pouvoir chinois [201], qui contrôle et censure la plupart des communications électroniques. Les protestataires pouvaient ainsi bénéficier d’une meilleure confidentialité de leurs échanges électroniques [201].

4.6. Le modèle de couches adapté au PSN

PSN est une dérivée de DTN [9], alors le modèle de couches adapté au PSN est le même que celui adapté au DTN. Ce modèle est caractérisé par le principe " Store-and-forward ". Pour cela, une nouvelle couche réseau a été mise en place appelée ‘‘la couche Bundle’’(figure 4.7). Elle vient se placer entre la couche application et les couches spécifiques aux réseaux (Transport, Réseau, etc.).

Elle permet donc de s'abstraire des technologies rencontrées sur les différent réseaux du DTN. Une couche intermédiaire, appelée couche de convergence (Convergence Layer), est utilisée pour faire le lien entre la couche Bundle et les couches inférieures [202].

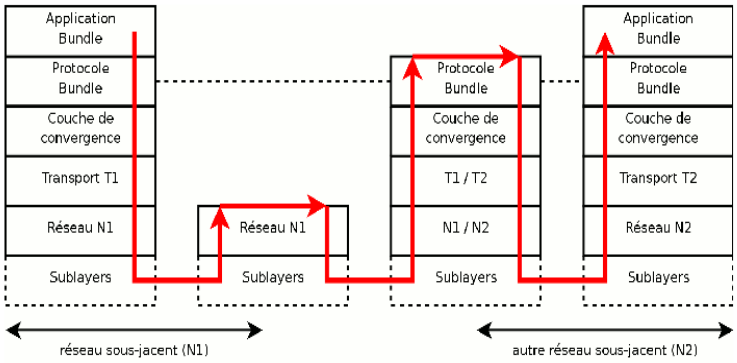


Figure 4. 7. La couche bundle.

Le protocole Bundle est le protocole utilisé dans la couche Bundle. Ce protocole rassemble les données sous forme de message appelés Bundle et se charge de les transmettre [202]. Un exemple d'implémentation du ce protocole sur les Smartphones est détaillé par Lars W. [203].

4.7. Conclusion

Dans ce chapitre, on a présenté et discuté la technologie PSN d'origine dérivée de la technologie DTN. On constatait que PSN est une technologie qui supporte des réseaux hétérogènes. Les algorithmes de routage présents et en cours de développement sont très diversifiés et répondent surtout à des applications dédiées, mais la forte réapparition de PSN est surtout liée à corriger les coupures d'Internet, d'où l'idée d'adapter la technologie PSN pour améliorer la gestion des WSN hétérogènes. L'approche développée dans ce travail reposant sur PSN fera l'objet du prochain chapitre.

Chapitre 05

Chapitre 05 : Le modèle IOT-PSN

5.1. Introduction

L'IOT n'a pas de description universelle. Dans ce chapitre on va définir le modèle IOT-PSN proposé. Ce modèle est décrit par les nœuds (les personnes dotées de leurs téléphones mobiles) qui assurent une meilleure connectivité et une diffusion de l'information grâce à la technologie PSN explicitée dans le chapitre précédent. Le protocole de routage exploité par PSN est le SSEA qui sera défini par la suite. On commence par décrire la topologie de ce modèle, ses différentes composantes, ainsi que les différents scénarios de communication basés sur la coopération des nœuds et leurs degrés de sécurité.

5.2. Description du modèle

5.2.1. Topologie du modèle

Comme première approche, considérons N zones statiques. Chaque zone englobe une communauté. L'extérieur, milieu n'appartenant pas aux zones est défini comme ‘‘EXTERNAL’’, identique au modèle en [204].

On rappelle que chaque nœud peut appartenir à plusieurs communautés. A l'intérieur de la communauté, un nœud est qualifié de membre du réseau local, et les nœuds échangent des messages ‘‘Hello’’ pour assurer leur présence. Quand un nœud arrive dans ‘‘EXTERNAL’’, il est pris comme un membre du réseau social ‘‘ad-hoc’’.

Ensuite, pour chaque nœud, on définit le paramètre *d* comme étant le degré de sécurité qui devrait refléter sur le nombre de communautés auxquelles il appartient. Il est admis qu'en l'absence de connexion Internet, chaque nœud souhaitant désormais communiquer avec sa communauté, envoie des messages via d'autres nœuds. Cette communication est assurée par la technologie PSN (thème déjà détaillé). Alors, il recherche les nœuds avec des valeurs *d* élevées (nœuds qualifiés dignes de confiance) pour sécuriser la transmission. Les différents nœuds coopératifs se trouvant dans la zone ‘‘EXTERNAL’’ forment un réseau IOT reliant les différents réseaux IOT locaux définis à l'intérieur de chaque communauté.

Pour étudier l'efficacité de ce modèle et obtenir des mesures, on a fixé le nombre de communautés. La figure 5.1 montre un exemple de modèle de 5 régions : 4 communautés (communauté 1, 2, 3 et 4) et une région dite ‘‘EXTERNAL’’ qui définit la situation où les nœuds sont en dehors de leurs communautés. A ce stade, chaque communauté a une taille limitée et un nombre de nœuds limité. Les quatre communautés sont délimitées par des cercles, et on a affecté les couleurs rouge, vert, rose et blanc respectivement à la première communauté, la deuxième, la troisième et la quatrième. Lorsque les nœuds sont en ‘‘EXTERNAL’’, la couleur affectée est le jaune. Pour cet exemple, il y a quatre degrés de sécurité *d*: 1, 0,75, 0,5 et 0,25 lorsque le nœud appartient à quatre communautés, trois, deux et une communauté respectivement.

5.2.2. Le degré de sécurité

Pour donner une identité cognitive au nœud, on a défini et introduit le paramètre *d,* degré de sécurité défini comme le montre l'équation (5-1).

$$d = \frac{k}{N} \qquad (5-1)$$

Où *k* est le nombre de communautés auxquelles appartient ce nœud et *N* le nombre total de communautés.

Ainsi, chaque nœud possède un *d* spécifique. Le nœud avec un *d* élevé est un nœud populaire et très sécurisé pour transmettre des informations. D’autres équations peuvent être exploitées pour modéliser selon d’autres spécifications et caractéristiques auxiliaires.

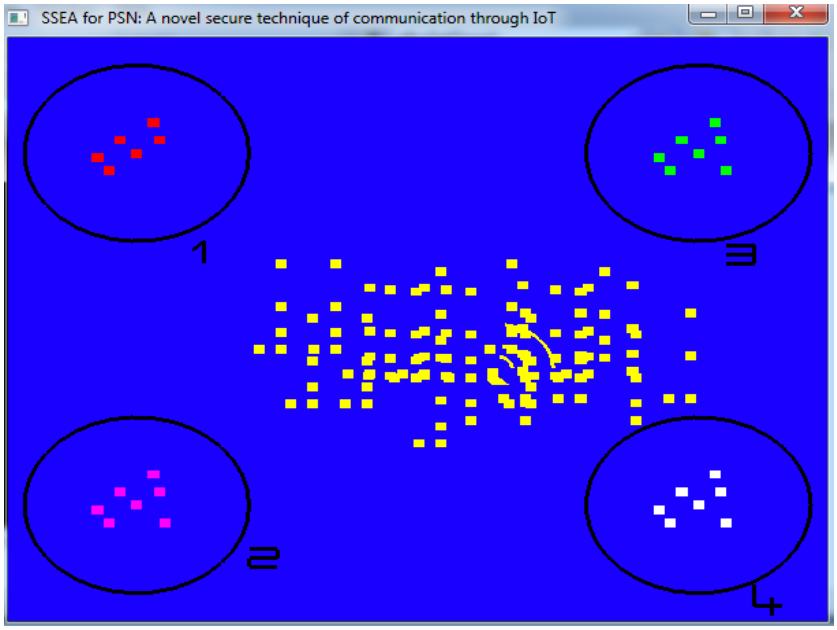


Figure 5. 1. La Topologie du modèle IOT Proposé.

5.2.3 Les scénarios de communication implantés

On a défini un ‘‘member-agent’’ pour le discerner parmi les autres nœuds. Pour expliquer le fonctionnement de notre modèle défini, on a construit deux scénarios:

- ✓ Le premier scénario concerne le déplacement du ‘‘member-agent’’ entre les différentes communautés.
- ✓ Le second concerne la découverte du ‘‘node-agent’’ (nœud susceptible, capable de délivrer l’information à la communauté destination).

L’implantation du modèle et des deux scénarios a été développée en C++ sous l’environnement visuel studio [205, 206] en utilisant la bibliothèque OpenGL (une bibliothèque utilisée dans divers domaines de l'infographie et exploitable sur plusieurs plateformes) [207-211].

5.2.3.1. Le scénario de déplacement entre les communautés

Comme déjà expliqué, notre modèle comporte 4 communautés et un ‘‘EXTERNAL’’, on a considéré que les distances entre les différentes communautés sont fixes. Chaque nœud appartenant à plusieurs communautés mémorise la distance à parcourir et le temps moyen nécessaire pour aboutir à la communauté cible. L’organigramme de figure 5.2 résume le processus de déplacement d’un nœud qualifié comme ‘‘member-agent’’ (avec un degré de sécurité d =1) entre les différentes communautés et appartenant initialement à la communauté 1:

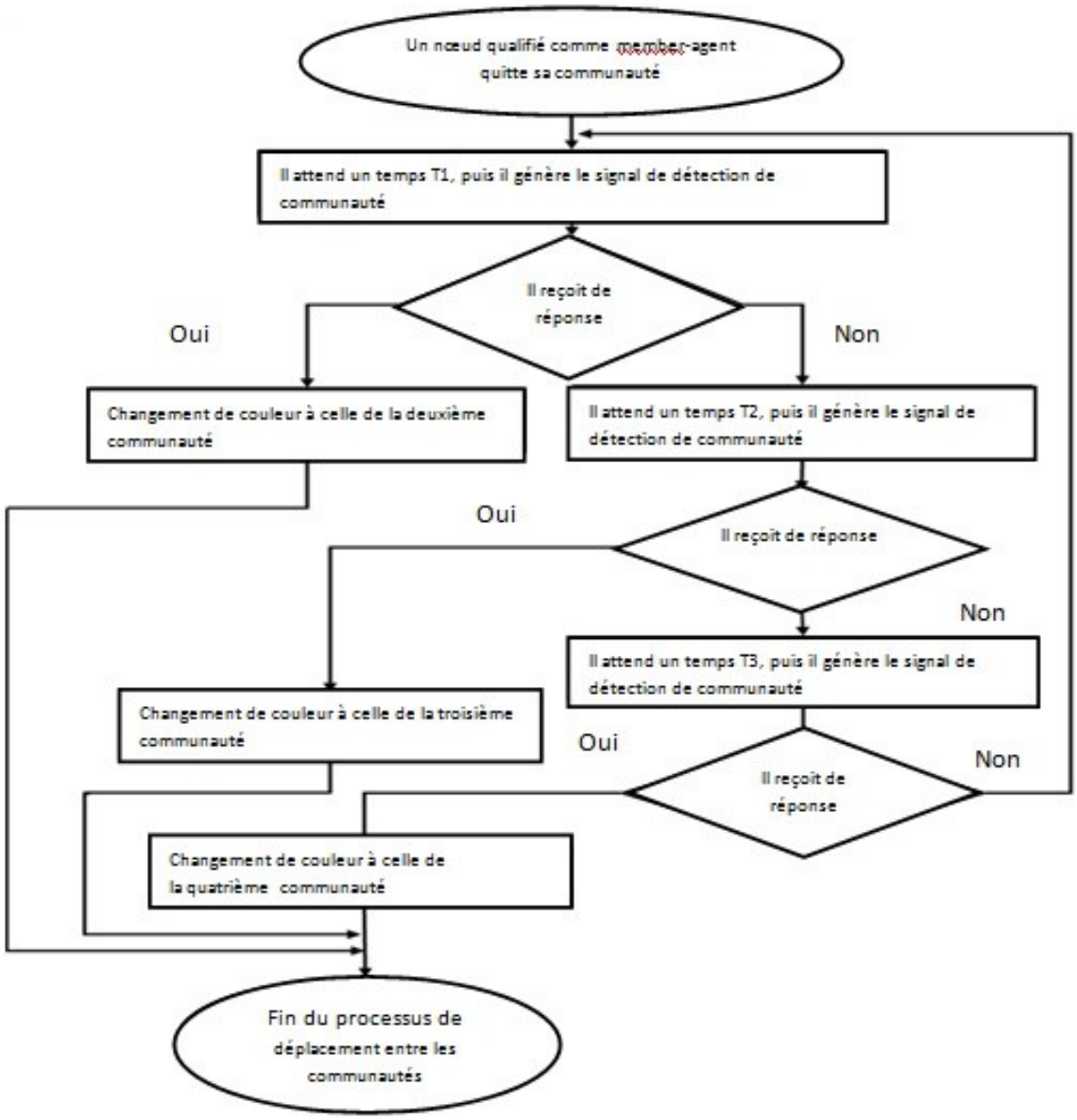


Figure 5. 2. Organigramme du déplacement du ‘‘member-agent’’ entre les communautés.

En quittant sa première communauté, le ‘‘member-agent’’ ne reçoit pas de message hello, donc il suggère qu’il a quitté sa première communauté et qu’il se trouve à la zone dite ‘‘EXTERNAL’’. Alors il change sa couleur au jaune (couleur affectée à cette zone), comme montré sur la figure 5.3. Le nœud est sensé atteindre une autre communauté, alors après un temps T1(le temps moyen nécessaire pour arriver à la deuxième communauté), le ‘‘member-agent’’ envoie un autre message ‘‘hello’’. En recevant une réponse, il confirme son appartenance à la deuxième communauté (la communauté la plus proche) et il change sa couleur à celle de cette dernière

(rose) et ainsi de suite. Si le nœud n'atteint aucune communauté, il refait le processus jusqu'à ce qu'il arrive à une des communautés (figure 5.3).

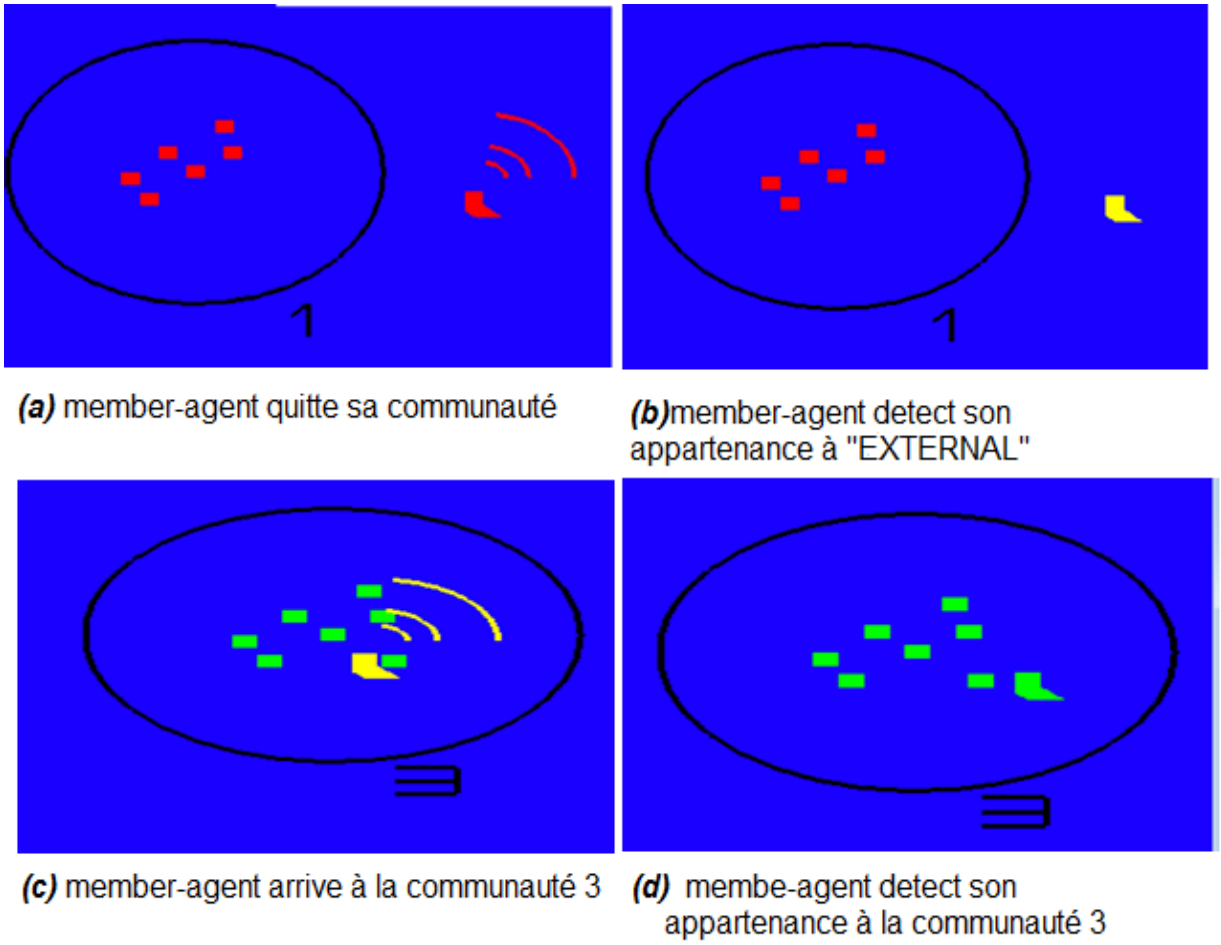


Figure 5. 3. La détection d'appartenance à la communauté 3.

Note: Ce changement de couleurs est à titre démonstratif seulement. Tout un code est exécuté pour mesurer la distance entre les communautés, la vitesse de mouvements des nœuds ainsi que le temps s'écoulant.

5.2.3.2. Le scénario de recherche du ''node-agent''

La procédure effectue les tâches suivantes:

- ✓ Un ''member-agent'' quitte la première communauté et voyage vers une autre.
- ✓ Il envoie un message périodique (message ''hello'') pour vérifier et décider de sa présence au sein de la communauté.

- ✓ En sortant de sa première communauté et avant d'atteindre celle ciblée, le ‘‘member-agent’’ appartient à un média nommé ‘‘EXTERNAL’’.

Une fois dans ‘‘EXTERNAL’’, et lorsqu'une forte congestion apparaît, le ‘‘member-agent’’ sans lien de communication ne peut pas atteindre la communauté ciblée à laquelle il doit délivrer des informations. Ainsi, la technologie PSN devait régir le réseau de communication : le ‘‘member-agent’’ génère un message d'alerte à son environnement pour obtenir d'autres liens ou alternatives qui offriraient une solution. Cette situation demande la coopération des nœuds. Il génère un message d'alerte dans un délai défini et attend une réponse. Ce message comprend un vecteur d'identité comprenant les communautés auxquelles il appartient. Un nœud candidat répondra par un message d'acceptation comprenant son identité. Si plus d'un nœud répond, le ‘‘member-agent’’ calcule leurs degrés de sécurité *d* (reflète la confidentialité d'un message). Il délivre des messages au nœud possédant un *d* le plus élevé afin d’obtenir un lien plus sécurisé. Ainsi, ce nœud se défini comme un ‘‘node-agent’’. Les temporisateurs suivants t_1, $2t_1$, $3t_1$ et $4t_1$ ont été prédéfinis et ajoutés au round pour trouver le ‘‘node-agent’’ avec d=1, 0,75, 0,5 et 0,25 respectivement.

Rappelons aussi que la coopération est un signe d'acceptation ou de refus du transport de messages. Pour modéliser les cas de coopération, on a implémenté un nombre différent de nœuds (considérés comme coopératifs) dans la région définie ‘‘EXTERNAL’’.

L'organigramme de figure 5.4 décrit la procédure de trouver le premier ‘‘node-agent’’. Dans un premier temps, on a considéré que le ‘‘member-agent’’ a quitté la communauté1 pour aller à la communauté 4. Une fois dans ‘‘EXTERNAL’’, une forte congestion apparaît et aucun lien Internet n'est disponible. Dans cette situation, le ‘‘member-agent’’ passe à la technique PSN pour envoyer des informations à la communauté 4. On suggéra que le ‘‘member-agent’’ est entouré de nœuds coopératifs, et chaque nœud coopératif appartient à une communauté (d=0,25) au moins. Quatre situations sont envisagées:

1-Recherche de nœud candidat avec *d*=1

Le ‘‘member-agent’’ envoie un message d'alerte, et lorsqu'il reçoit des réponses, il donne l'information au premier candidat répondant avec d=1. S'il n'y a pas de candidats avec d=1, on passe à la deuxième situation.

2- Recherche de nœud candidat avec *d*=0.75

Le ‘‘member-agent’’ envoie un deuxième message d'alerte, et lorsqu'il reçoit des réponses, il envoie l'information au premier candidat répondant avec *d*=1. S'il n'y a pas de candidats avec *d*=1, il envoie l'information au premier candidat répondant avec *d*=0,75. S'il n'y a pas de candidats avec *d*=0,75, on passe à la troisième situation.

3- Recherche de nœud candidat avec *d*=0.5

Le ‘‘member-agent’’ envoie un troisième message d'alerte, et lorsqu'il reçoit des réponses, il envoie l'information au premier candidat répondant avec *d*=1. S'il n'y a pas de candidats avec *d*=1, il envoie l'information au premier candidat répondant avec *d*=0,75. S'il n'y a pas de candidats avec d=0,75, il envoie l'information au premier candidat répondant avec *d*=0,5. S'il n'y a pas de candidats avec *d*=0. 5, on passe à la quatrième situation.

4- Recherche de nœud candidat avec *d*=0.25

Le ‘‘member-agent’’ envoie un quatrième message d'alerte, et lorsqu'il reçoit des réponses, il envoie les informations au premier candidat répondant avec la valeur *d* la plus élevée.

Si ce premier ‘‘node-agent’’ ne peut pas terminer cette tâche, le processus de la figure 5.4 sera réactivé pour trouver le deuxième ‘‘node-agent’’ et ainsi de suite.

La figure 5.5 montre 3 cas de nombre de ‘‘node-agents’’ : 1, 2 et 3 ‘‘node-agents’’

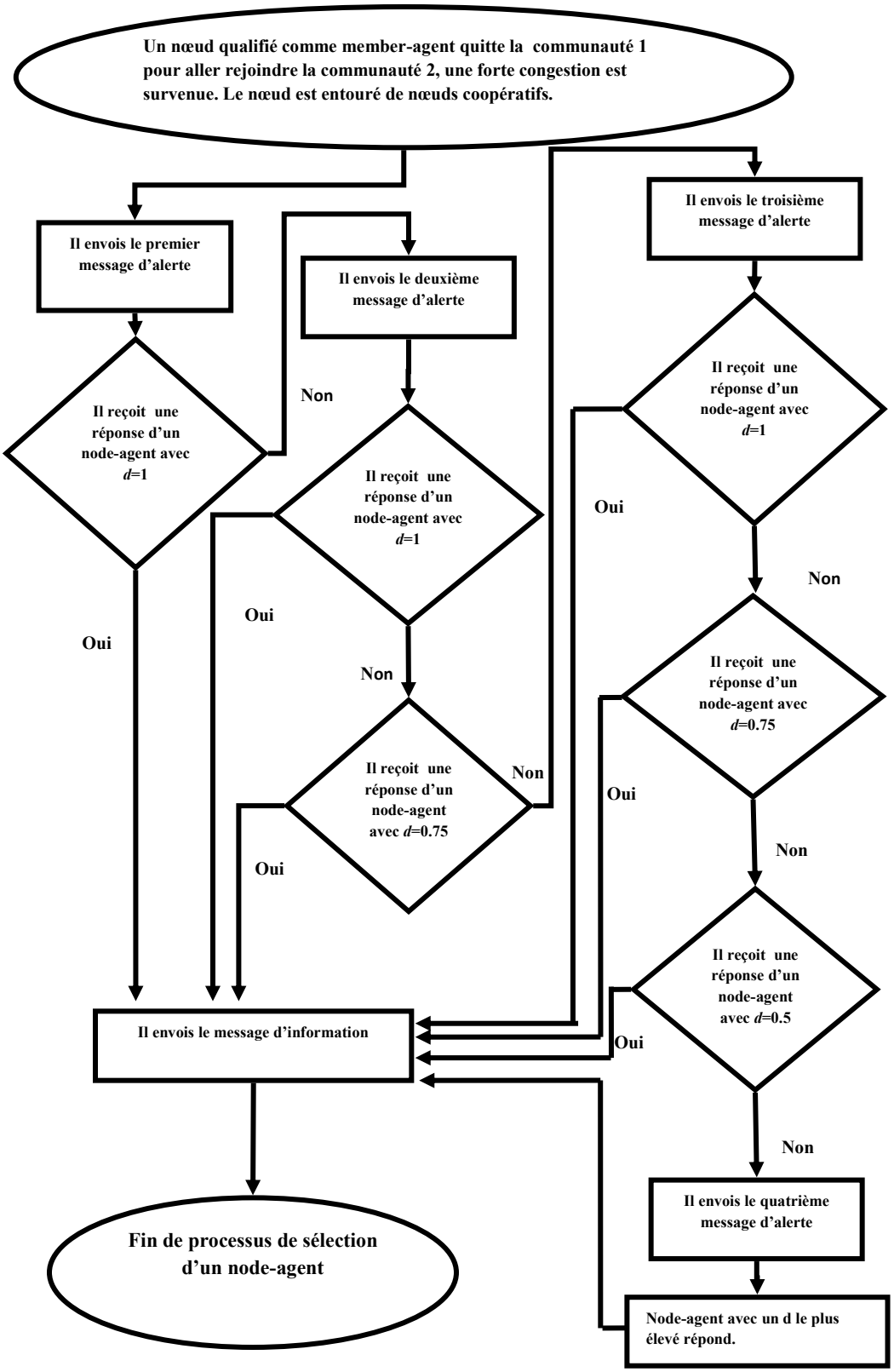


Figure 5. 4. Organigramme de la recherche du ‘‘node-agent’’.

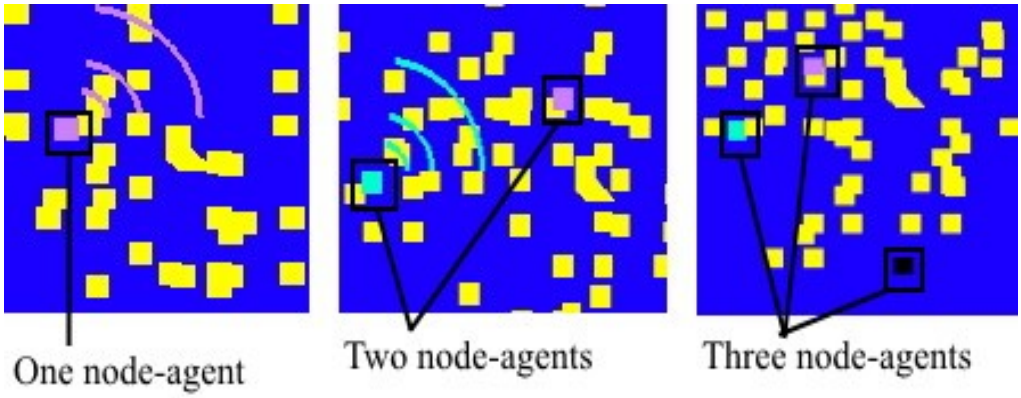


Figure 5. 5. Trois cas de Nombre de ‘‘node-agents’’ différents.

5.3. L’algorithme SSEA

On a déjà défini la technologie PSN ainsi que les différents protocoles de routage utilisés par cette technologie dans le chapitre 3. Dans cette partie, on va tout d'abord, définir l'algorithme d'épidémie simple SEA [9-17] qui représente l’algorithme le plus simple utilisé par le protocole de routage épidémique. Pour une population de taille fixe n, k nœuds sont déjà infectés. L'infection apparaît en rounds. La probabilité qu'un nœud sensible particulier (non infecté) soit ensuite infecté dans un round si k nœuds sont déjà infectés est montrée dans l'équation (5-2).

$$P_{inf}\,(k,n) = \; 1-(1-1/(n-1))^{k} \qquad (5-2)$$

Alors, le nombre attendu de nœuds nouvellement infectés sera $(n-\;k)\big(1-(1-1/(n-1))^{k}\big)$.

La complexité temporelle est de O(log N), également après $log_{0.75}\frac{n}{2}$ intervalles, chaque nœud est infecté [18].

Pour prouver l'efficacité de notre modèle IOT proposé, on a développé le Secure Simple Epidemic Algorithm (SSEA) qui sera explicité ci-dessous.

5.3.1. Description du SSEA

Notons que le paramètre d doit refléter le nombre de communautés auxquelles appartient un nœud. L'utilité de d apparaitra lorsque les nœuds se trouvent en ‘‘EXTERNAL’’ et sans lien à Internet. Ainsi, chaque nœud est membre du réseau social ‘‘ad-hoc’’ (comme déjà indiqué dans la topologie), et il est supposé coopératif. Pour cette situation, la technologie PSN est choisie pour assurer la communication entre les nœuds. Pour définir SSEA(utilisé dans notre modèle

IOT-PSN), on a pris le SEA auquel est ajouté le degré de sécurité comme condition pour envoyer l'information. L'objectif de cet algorithme est d'infecter uniquement les nœuds avec un degré de sécurité élevé pour sécuriser la communication. Dans cet état, SSEA réduit le nombre de nœuds infectés, donc la consommation d'énergie est ainsi réduite. Le système d'équations (5-3) montre la probabilité qu'un nœud sensible particulier (non infecté) avec une valeur *d* soit ensuite infecté dans un round si *k* nœuds avec une valeur *d* sont déjà infectés.

$$P_{d,inf}(k,n) = \begin{cases} 1-(1-1/(n_d-1))^k, & n_d < n \\ P_{inf}(k,n), & n_d = n \end{cases} \qquad (5-3)$$

L'équation (5-2) est définie par deux valeurs, *n* et *k*, SEA infecte une population entière sans condition ; tandis que les trois valeurs, *n*, *k* et *d*, définissent la probabilité conditionnelle donnée par le système d'équations (5-3). Le degré de sécurité *d* contrôle l'infection dans SSEA. Ce dernier n'affecte que les nœuds souhaités. C'est la première différence entre l'équation (5-2) et le système d'équations (5-3). La seconde est que l'équation (5-2) est définie pour une population globale de *n* nœuds, tandis que le système d'équations (5-3) est défini pour une population de nœuds avec une valeur *d* spécifique. Un cas particulier apparaît lorsque tous les nœuds ont la même valeur *d*, donc le système d'équations (5-3) sera réduit à l'équation (5-2). Concéderons

Pour sélectionner des nœuds avec un degré de sécurité spécifique, le nombre attendu de nœuds nouvellement infectés sera $(n_d - k)\left(1-(1-1/(n_d-1))^k\right)$. A la fin, les n_d nœuds seront infectés avec le même degré de sécurité *d.*

Pour *n* nœuds, et en considérant le coût de communication comme homogène, E_{cost} est le coût énergétique entre deux nœuds. Le coût énergétique du réseau en SEA est nE_{cost}. Dans SSEA, la communication se fait entre n_d nœuds sélectionnés, donc le coût énergétique est $n_d E_{cost}$.

5.3. La simulation du modèle IOT-PSN

Dans cette section, on présentera les différentes mesures effectuées ainsi que la comparaison avec des travaux similaires. Le Matlab est utilisé pour représenter les allures des courbes. On commencera par la comparaison entre SSEA proposé et SEA afin d'éclaircir la nouveauté apportée par SSEA, et on terminera par la comparaison avec les travaux de GOSSIP[18].

5.3.1. Comparaison de SEA avec SSEA

Dans la simulation, on a considéré trois situations afin de pouvoir observer la variation de la réponse du système. La première situation concerne des nœuds de même degré de sécurité. La deuxième situation traite quatre cas pour différents degrés de sécurité et enfin la troisième situation est décrite pour observer l'influence de la variation de t_1. Pour toutes ces situations, la valeur initiale de *k* est 1 (Initialement un seul nœud qui souhaiterait diffuser des informations via des nœuds sécurisés). La simulation est effectuée en ''rounds''.

5.3.1.1 La comparaison pour des nœuds de même degré de sécurité

Pour cette situation, SEA et SSEA sont simulés pour la même population sous Matlab. La situation programmée considère que ''member-agent'' est entouré de nœuds coopératifs de même degré de sécurité *d*. La figure 5.6 représente les nœuds nouvellement infectés. Comme on le voit, tous les graphiques sont très proches et semblent être un seul graphique ; cela est dû au temps de décalage très réduit entre les graphiques. Sur la figure 5.7, Les graphiques sont aussi proches pour le nombre total des nœuds infectés. Pour le coût énergétique de la communication, il est le même pour SEA et SSEA, car le nombre des nœuds est le même.

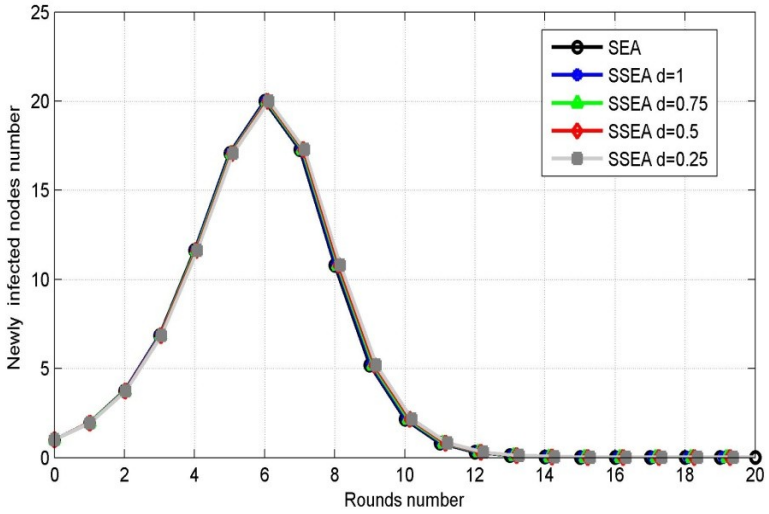


Figure 5. 6. Les Nouveaux nœuds infectés par SSEA pour les différentes valeurs de d pour 100 nœuds.

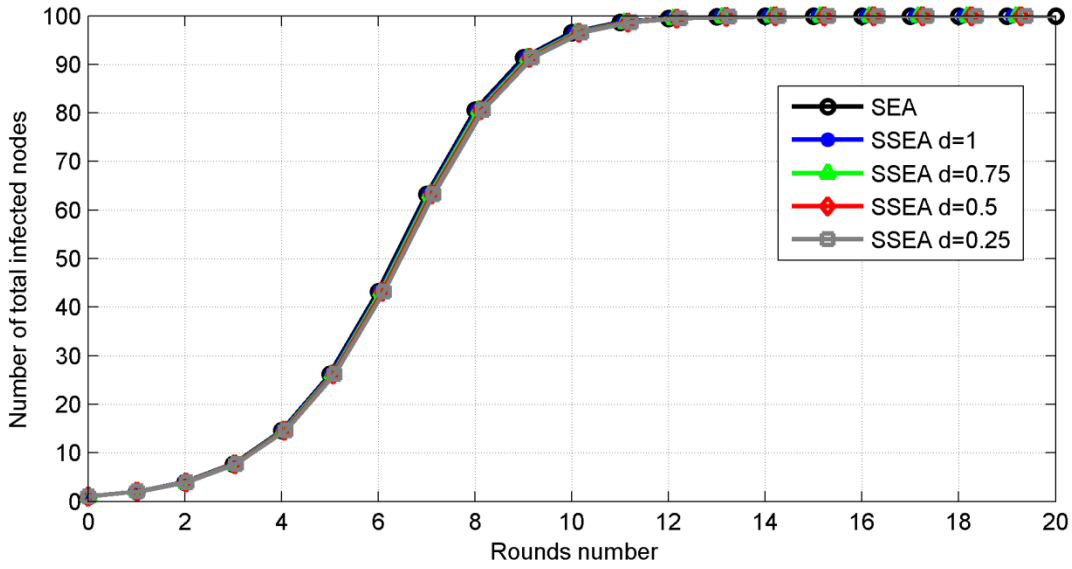


Figure 5. 7. Le nombre total des nœuds infectés par SSEA pour les différentes valeurs de d pour n=100.

5.3.1.2. La comparaison pour des nœuds de différents degrés de sécurité

Dans cette situation, le ‘‘member-agent’’ est entouré de nœuds avec différents degrés de sécurité *d*. Pour chaque degré de sécurité, on a envisagé deux cas différents de nombre de nœuds coopératifs (tableau 5.1):

Tableau 5. 1. Nombre de nœuds coopératifs de différentes valeurs de *d*.

Degré de sécurité	**Nombre de nœuds coopératifs**	
d=1	10	15
d=0,75	18	20
d=0,5	30	34
d=0,25	35	38

Dans tous les cas, le ‘‘member-agent’’ ne communique qu'avec les nœuds coopératifs. La simulation sous Matlab est menée pour deux populations: une population de 100 nœuds et une population de 200 nœuds.

Figure 5.8 ((A)-(B)), figure 5.9 ((A)-(B)) correspondent à une population de 100 nœuds.

Figure 5.10 ((A)-(B)), figure 5.11 ((A)-(B)) correspondent à une population de 200 nœuds.

Comme observé dans tableau 5.2, le temps nécessaire pour infecter une population de 100 nœuds avec SEA est de 14 rounds et pour infecter une population de 200 nœuds, il est de 16 rounds.

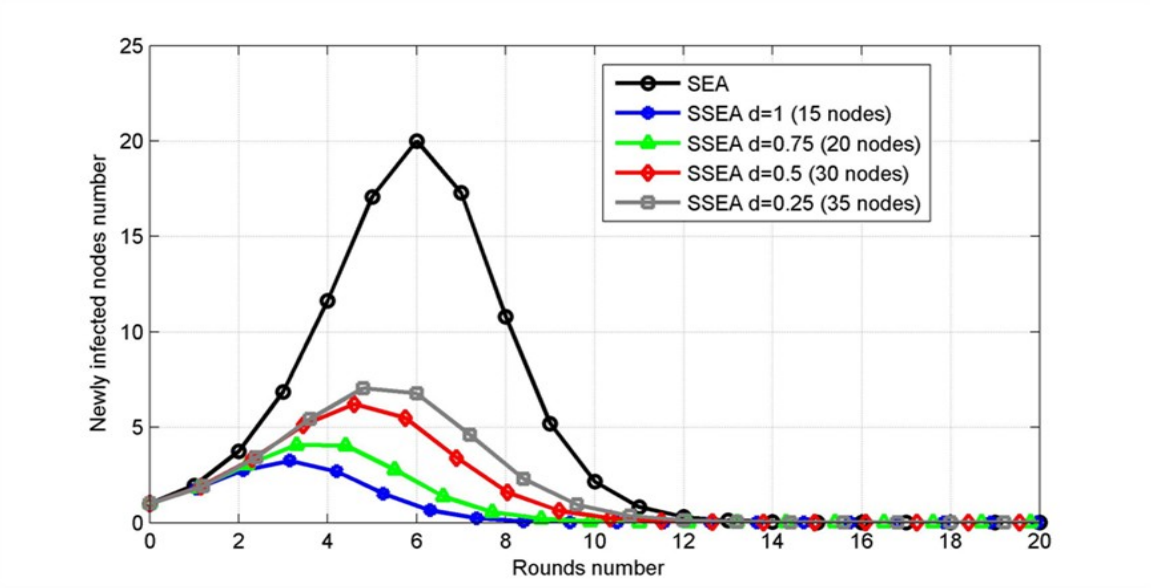
D’après l’observation des figures (figure 5.8 - figure 5.11) et tableau 5.2, le temps nécessaire pour infecter des nœuds avec un degré de sécurité *d*=1 est inférieur aux autres cas de valeurs de *d* (6 rounds pour 10 nœuds et 7 pour 15 nœuds).

Pour *d*= 0,75 : le temps écoulé est de 8 rounds pour 18 nœuds et 9 pour 20 nœuds.

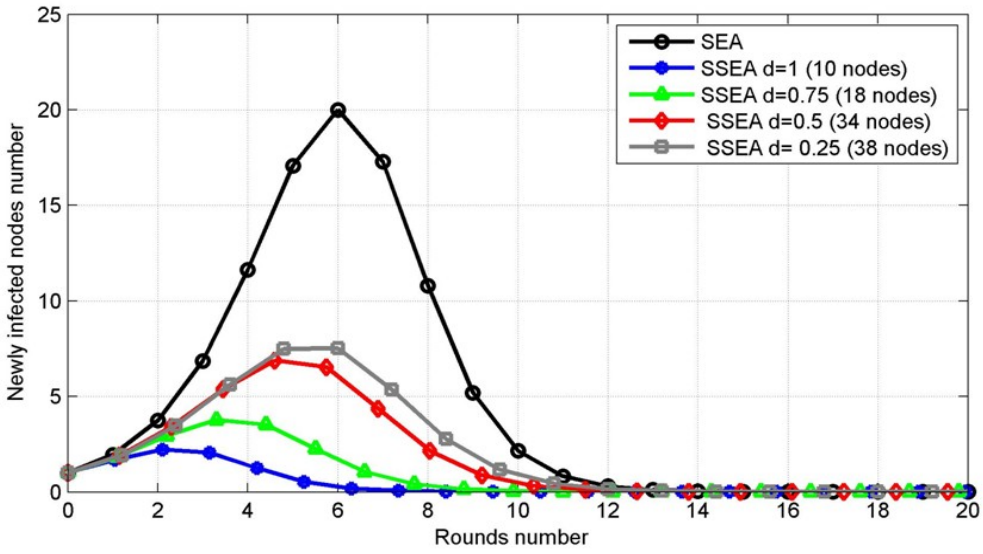
Pour *d*= 0, 5 : le temps écoulé est de 10 rounds pour 30 nœuds et 11 pour 34 nœuds.

Pour *d*= 0,25 : le temps écoulé est de 11 rounds pour 35 nœuds et 12 pour 38 nœuds.

Dans tous les cas (tableau 5.2), le temps le plus court est pour *d* =1, puis pour *d*=0,75, après pour *d*=0,5, et enfin pour *d*=0,25 et le coût énergétique est réduit uniquement aux nœuds sélectionnés. On peut voir que ces mesures et ces résultats répondent aux situations projetées, où on a considéré que les meilleures réponses devront être pour les *d* les plus élevés.

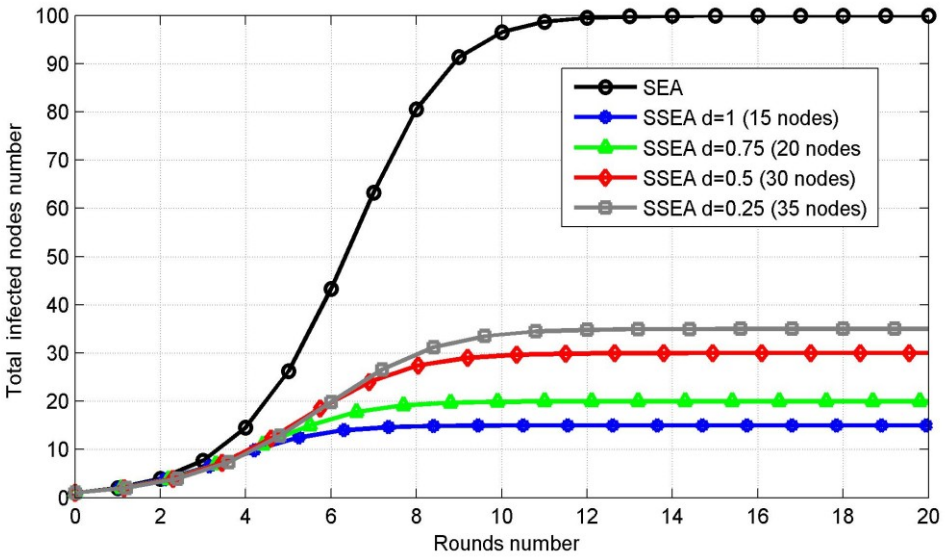


(A)

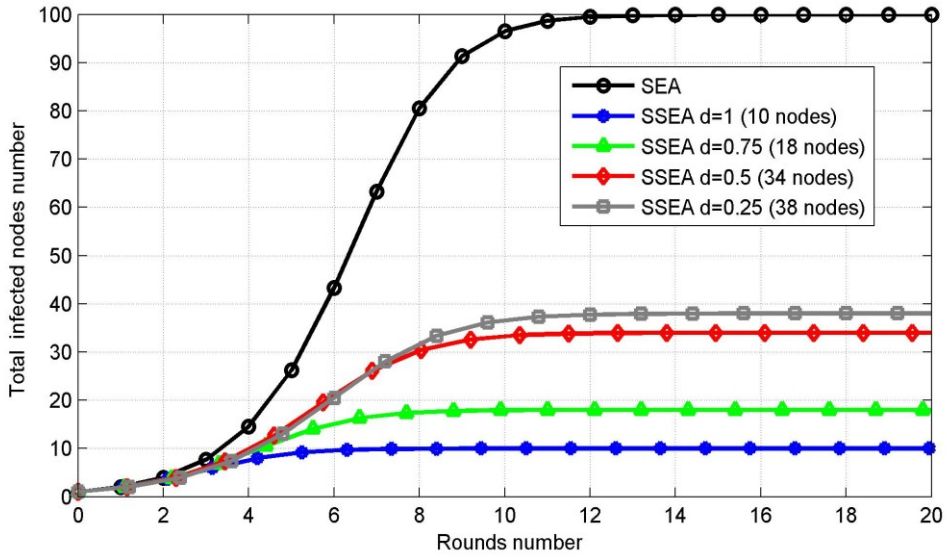


(B)

Figure 5. 8. Les nouveaux nœuds infectés par SSEA pour la sélection de nœuds de valeur d spécifique pour n=100.



(A)



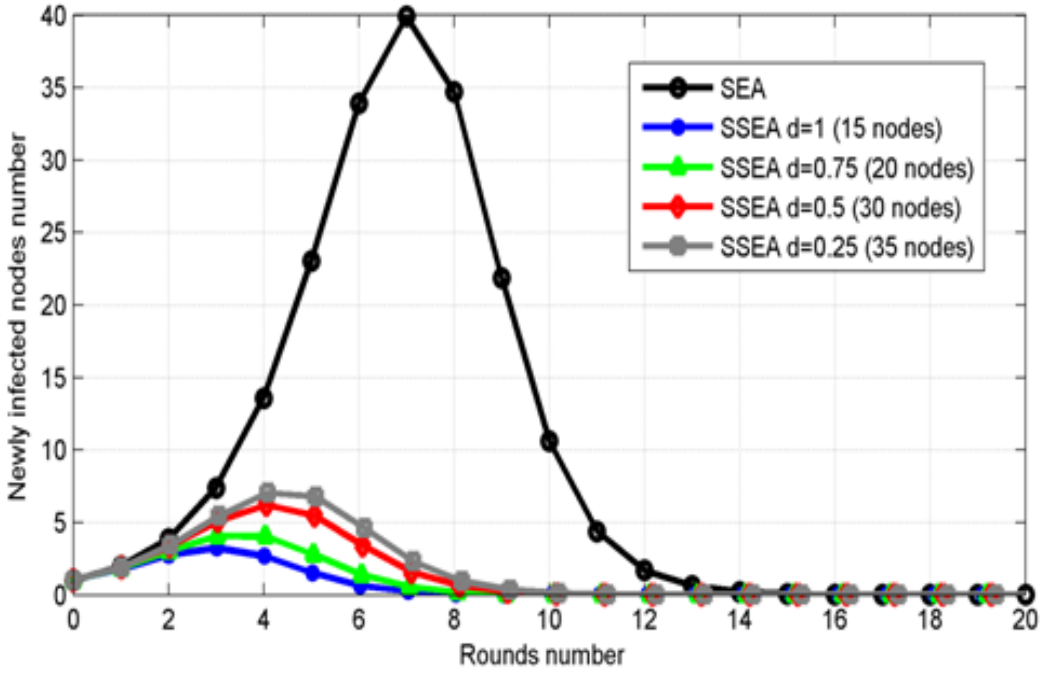
(B)

Figure 5. 9. Le nombre total de nœuds infectés par SSEA pour la sélection de nœuds de valeur d spécifique pour n=100.

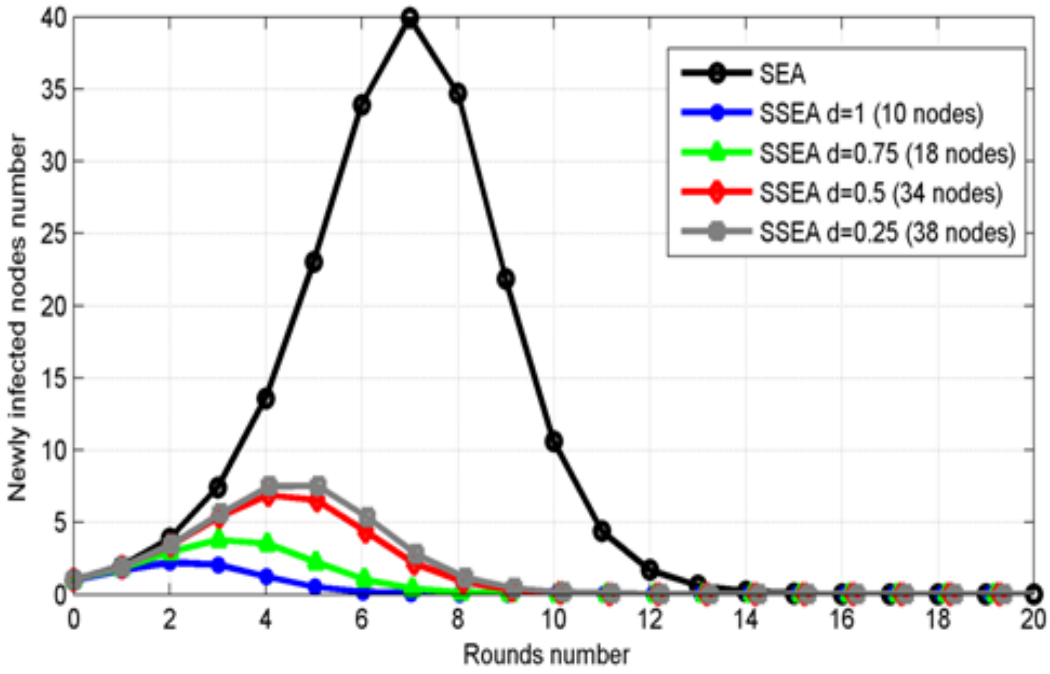
Tableau 5. 2. Performance selon la variation du nombre total de nœuds par SSEA.

		Temps en Rounds	**Le coût énergétique**
Nombre Total de nœuds ***d***	100 **nœuds** (sans considération de *d*)	14	$100E_{cost}$
	200 **nœuds** (sans considération de *d*)	16	$200E_{cost}$
1	10 nœuds	6	$10E_{cost}$
	15 nœuds	7	$15E_{cost}$
0.75	18 nœuds	8	$18E_{cost}$
	20 nœuds	9	$20E_{cost}$
0.5	30 nœuds	10	$30E_{cost}$
	34 nœuds	11	$34E_{cost}$
0.25	35 nœuds	11	$35E_{cost}$
	38 nœuds	12	$34E_{cost}$

Le temps nécessaire pour infecter 100 nœuds en SEA est estimé à 14 rounds et le coût énergétique est de $100E_{cost}$ (figure 5.8, tableau 5.2). Pour infecter 200 nœuds il est estimé à 16 rounds et le coût énergétique est de $200E_{cost}$ (figure 5.10, tableau 5.2). Rappelons que la communication est basée sur la technologie PSN et quelque soit le nombre total de population la performance du système dépend seulement de nœuds coopératifs. Alors Pour ces deux cas différents de population, on peut voir que pour des mêmes cas de coopération, les résultats pour SSEA sont les mêmes. On peut prendre comme exemple le cas de coopération de 10 nœuds avec un degré de sécurité de *d*=1. Pour ce cas le temps d'infection est de 6 rounds, et le coût énergétique n'est que de $10E_{cost}$.

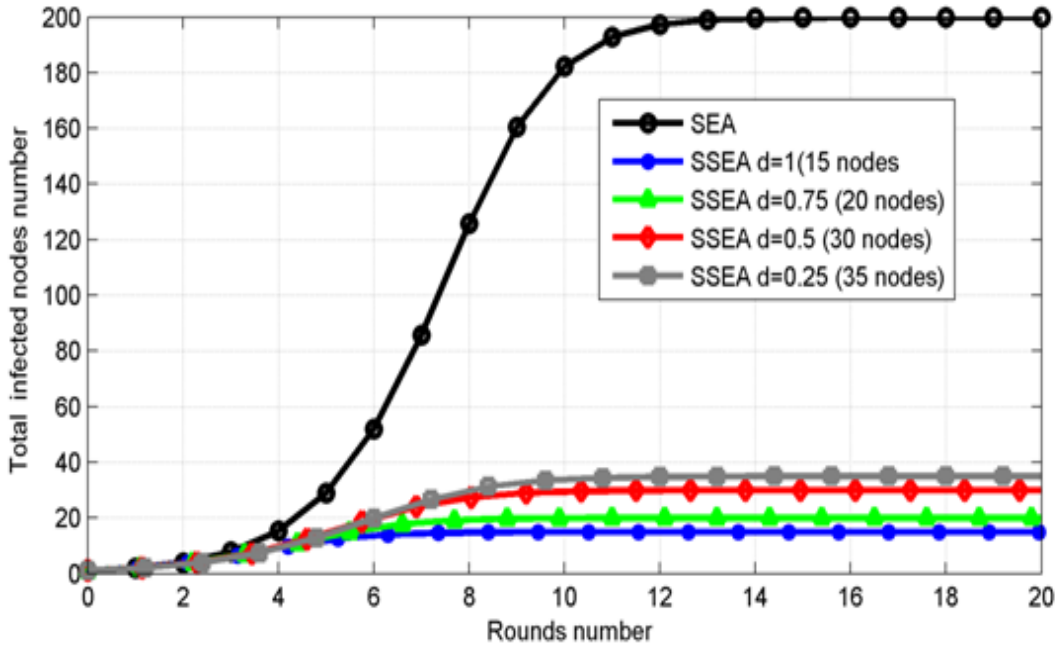


(A)

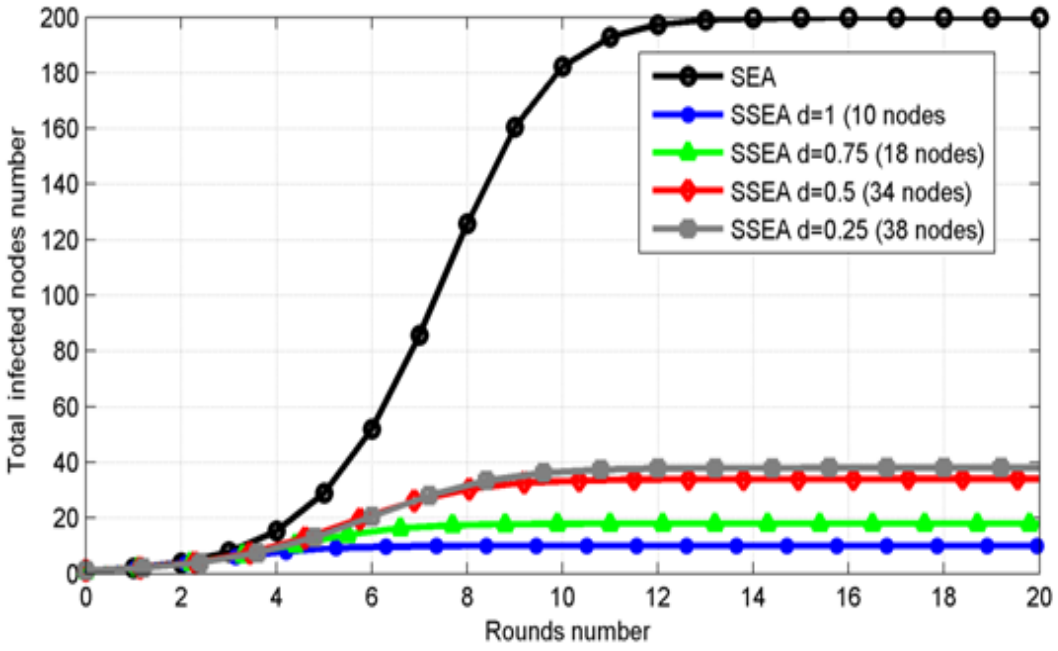


(B)

Figure 5. 10. Les nouveaux nœuds infectés par SSEA pour la sélection de nœuds de valeur d spécifique pour n=200.



(A)



(B)

Figure 5. 11. Le nombre total de nœuds infectés par SSEA pour la sélection de nœuds de valeur d spécifique pour n=200.

5.3.1.3. Influence de t_1 sur le temps d'infection

Plus le nombre de population est élevé et plus le temps d'infection par SEA est élevé, comme observé sur tableau 5.3, figure 5.12 et figure 5.13. Sur une population de 200 nœuds le temps d'infection est de 16 ''rounds'' et pour une population de 800 nœuds il n'est que de 21 ''rounds''.

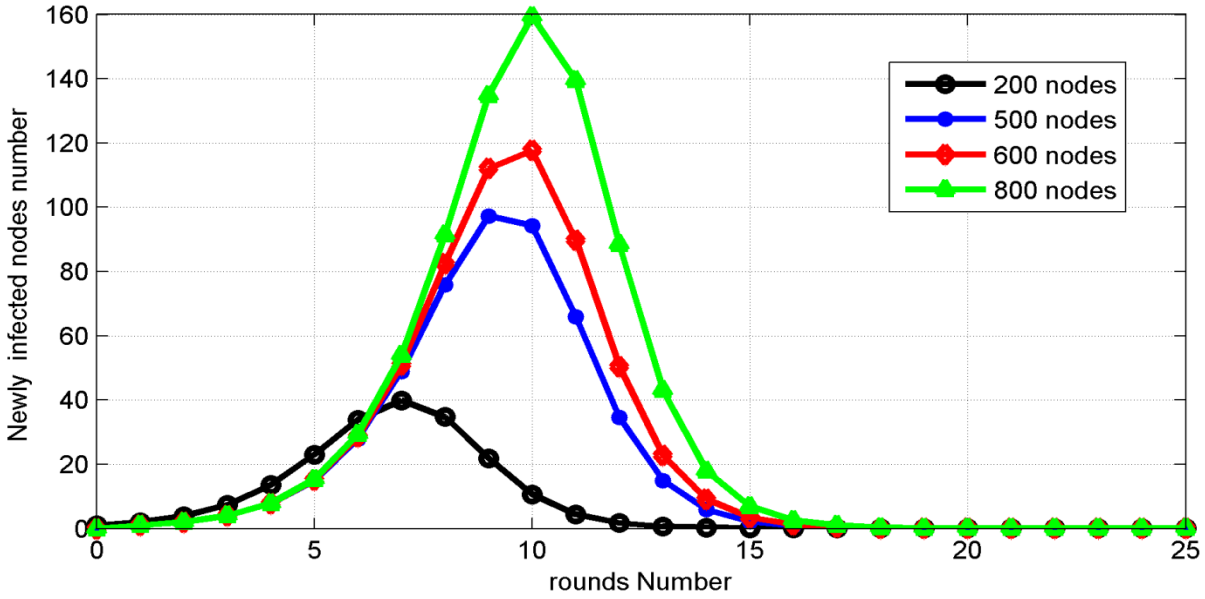


Figure 5. 12. Les nouveaux nœuds infectés par SEA pour différentes valeurs de n.

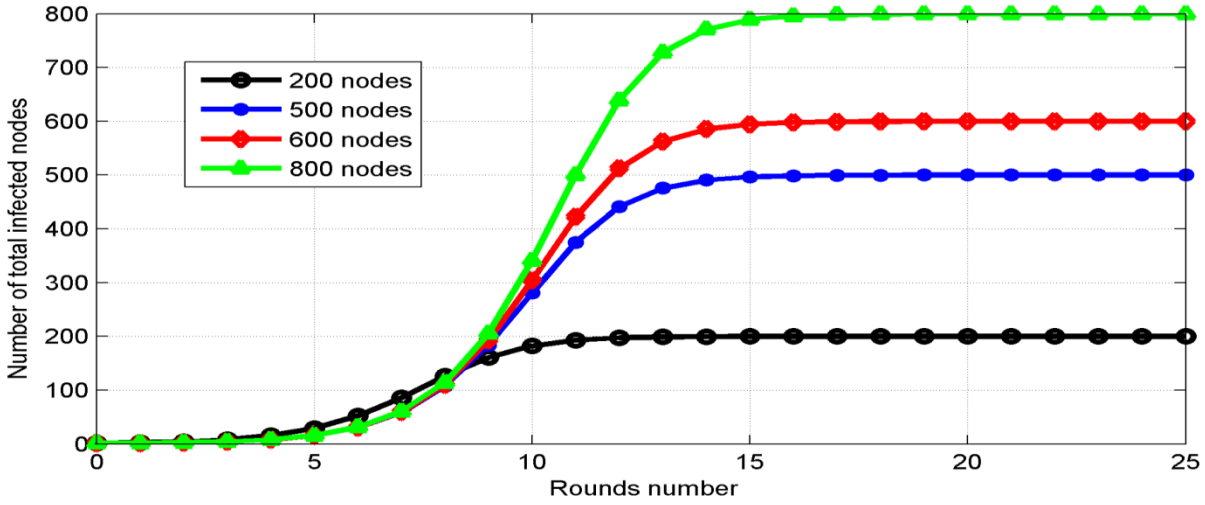


Figure 5. 13. Le nombre total de nœuds infectés par SEA pour différentes valeurs de n.

Tableau 5. 3. Performance selon la variation du nombre total de nœuds par SEA

Nombre De nœuds	Temps en Rounds	Coût énergétique
200	16	$200E_{cost}$
500	19	$500E_{cost}$
600	20	$600E_{cost}$
800	21	$800E_{cost}$

Comme déjà défini, t_1 caractérise le choix d'un ''node-agent'' avec un degré de sécurité d=1 parmi les nœuds répondant par l'acceptante de candidature. Si le nœud répondant a un degré de sécurité différent de 1, 0.75 par exemple, le ''member-agent'' doit relancer un nouveau message d'alerte afin de pouvoir communiquer avec des nœuds de degré de sécurité plus élevés. Alors $2t_1$ sera ajouté au round et l'information sera envoyée au candidat de d=0.75 ou 1. Ce processus se reconduit pour une troisième fois ($3t_1$ sera ajouté au round) si d< 0.75 et l'information est envoyée au candidat de d=0.5 ou supérieur. Si cette condition n'est pas satisfaite, un nouveau message d'alerte est alors envoyé pour la quatrième fois ($4t_1$ qui sera ajouté au round) et l'information sera alors envoyée au candidat ayant la valeur de d la plus élevée.

La stratégie d'application de SSEA dépend du nombre de nœuds coopératifs. L'infection est en ''round'', et plus le nombre de nœuds est élevé et plus le nombre de ''rounds'' augmente. Comme la complexité temporelle est de O(log N), alors n nœuds seront infectés après $log_{0.75}\frac{n}{2}$ ''rounds''.

D'après le tableau 5.3, 200 nœuds seront infectés par SEA après 16 ''rounds'', 500 nœuds après 19 ''rounds'', 600 après 20 intervalles et enfin 800 nœuds après 21 ''rounds''. Comme on a déjà expliqué, le temps d'infection pour SSEA dépend du degré de sécurité (tableau 5.4).

Tableau 5. 4. Variation de ‘‘rounds’’ d’infection selon *d* et t_1

Degré de sécurité *d*	1	0.75	0.5	0.25
‘‘round’’ d’infection	$1+t_1$	$1+2t_1$	$1+3t_1$	$1+4t_1$

Le tableau 5.5 montre le décalage de temps d’infection de SSEA par rapport à SEA pour le même nombre de nœuds.

Tableau 5. 5. Décalage de temps d’infection de SSEA par rapport à SEA

Nombre total de noeuds	***d=1***	***d=0.75***	***d=0.5***	***d=0.25***
200	$16+16t_1$	$16+32t_1$	$16+48t_1$	$16+64t_1$
500	$19+19t_1$	$19+38t_1$	$19+57t_1$	$19+76t_1$
600	$20+20t_1$	$20+40t_1$	$20+60t_1$	$20+80t_1$
800	$21+21t_1$	$21+42t_1$	$21+63t_1$	$21+84t_1$

Les tableaux suivants montrent la variation de temps d’infection pour différentes valeurs de t_1:

Tableau 5. 6. Décalage de temps d’infection de SSEA par rapport à SEA pour t_1=1/200(round)

t_1=1/200(round)				
Nombre total de nœuds	***d=1***	***d=0.75***	***d=0.5***	***d=0.25***
200	16.08	16.16	16.24	16.32
500	19.095	19.19	19.285	19.38
600	20.1	20.2	20.3	20.4
800	21.105	21.21	21.315	21.42

Tableau 5. 7. Décalage de temps d'infection de SSEA par rapport à SEA pour t_I=1/100(round)

t_I=1/100 (round)				
Nombre total de nœuds	***d=1***	***d=0.75***	***d=0.5***	***d=0.25***
200	16.16	16.32	16.48	16.64
500	19.19	19.38	19.57	19.76
600	20.2	20.4	20.60	20.80
800	21.21	21.42	21.63	21.84

Tableau 5. 8. Décalage de temps d'infection de SSEA par rapport à SEA pour t_I=1/50(round)

t_I=1/50(round)				
Nombre total de nœuds	***d=1***	***d=0.75***	***d=0.5***	***d=0.25***
200	16.32	16.64	16.96	17.28
500	19.38	19.76	20.14	20.52
600	20.40	21.2	21.20	21.6
800	21.46	21.84	22 .26	22.68

Tableau 5. 9. Décalage de temps d'infection de SSEA par rapport à SEA pour t_I=1/20(round)

t_I=1/20(round)				
Nombre total de nœuds	***d=1***	***d=0.75***	***d=0.5***	***d=0.25***
200	16.8	17.6	18.4	19.2
500	19.95	20.9	22.85	22.8
600	21	22	23	24
800	22.05	23.1	23.15	25.2

Tableau 5. 10. Décalage de temps d'infection de SSEA par rapport à SEA pour *t1*=1/10(round)

t_I=1/10(round)				
Nombre total de nœuds	***d=1***	***d=0.75***	***d=0.5***	***d=0.25***
200	17.6	19.2	20.8	22.4
500	21.9	22.8	24.7	26.6
600	22	24	26	28
800	23.1	25.2	27.3	29.3

D'après les tableaux tableau 5.6-5.10, on peut voir que pour tableau 5.6 et tableau5.7 le décalage dans le temps est légèrement remarquable (t_I=1/100(round), t_I=1/200(round)). Plus la valeur de t_I est élevée et plus le décalage est remarquable. Comme on peut le voir sur tableau 5.10, pour un t_I=1/10(round), il est de plus de 2 ''rounds'' pour les populations supérieures à 500 nœuds. Mais cela n'influe pas sur la performance du modèle proposé, puisque l'objectif est toujours de communiquer avec les nœuds coopératifs les plus sécurisés. Le seul critère qui reste est de choisir un t_I réduit afin d'accélérer la communication.

5.3.2. La Comparaison de SSEA avec GOSSIP [18]

Comme défini dans notre modèle IOT, le nœud diffuse des informations uniquement vers les nœuds avec un degré de sécurité élevé. Pour donner une comparaison entre SSEA et GOSSIP [18] (tableau 5.10), on a tout d'abord comparé GOSSIP [18] avec SEA (tableau 5.11), ensuite avec SSEA afin de pouvoir observer l'amélioration apportée par SSEA.

Pour Gossip[18] la propagation de l'information peut se faire à un nombre de voisins limité pour une itération, et que la propagation de l'information se continue de la même manière jusqu'à l'infection totale de la population de n nœuds. Il a étudié la variation de temps (calculé en rounds) et le nombre de messages répliqués pour différentes nombre de nœuds.

D'après le tableau 5.11, la complexité temporelle est de O(log *N*) [18], également après $log_{0.75}\frac{n}{2}$ intervalle, chaque nœud est infecté.

Alors, pour la comparaison on a gardé le nombre de nœuds donné par le tableau 5.11. Pour chaque cas, on a calculé le nombre de ''rounds'' nécessaires pour diffuser l'information par SSEA pour différentes valeurs de degrés de sécurité (tableau 5.13, tableau 5.14, tableau 5.15, tableau 5.16).

En observant le tableau 5.12, on peut voir que GOSSIP [18] est plus performant que SEA. Pour une population par exemple de 257 nœuds le nombre de ''rounds'' est de 17 pour SEA alors qu'il est de 15 pour GOSSIP [18].

Tableau 5. 11. Performance de GOSSIP[18]

Nombre total de nœuds *N*	Temps en Rounds
65	11
129	13
257	15
513	16

Passons maintenant à la comparaison de SSEA avec GOSSIP [18]. Pour chaque valeur de *d*, on a envisagé trois taux du nombre total de nœuds N considérés dans GOSSIP [18] : 1/8, 1/4 et 1/3.

On peut observer dans le tableau 5.13 pour *d*=1, que le meilleur moment est pour le taux 1/8 de la population globale, et plus le taux est élevé, le plus le nombre de tours converge vers celui de GOSSIP[18].

Tableau 5. 12. Comparaison SEA et GOSSIP[18]

Nombre total de nœuds *N*	Temps en Rounds GOSSIP [18]	Temps en Rounds SEA
65	11	12
129	13	15
257	15	17
513	16	19

Dans le tableau 5.14 pour *d*=0,75, on peut voir aussi que le nombre de ‘‘rounds’’ converge vers GOSSIP[18] pour les taux élevés de la population globale.

Dans tableau 5.15 pour *d*=0,5, et tableau 5.16 pour *d*=0,25, on peut remarquer que le nombre de ‘‘rounds’’ converge aussi vers GOSSIP [18] pour les taux élevés de la population.

Pour les différents états de valeurs de degrés de sécurité *d*, le meilleur moment est pour *d* = 1. Dans tous les cas, le nombre de ‘‘rounds’’ pour SSEA est inférieur à celui de GOSSIP[18].

Ainsi, comme le prouve la comparaison avec SEA, et la comparaison avec GOSSIP [18], SSEA, réduit la consommation d'énergie aux nœuds sélectionnés, et réduit le temps d’infection des nœuds(figure 5.14).

Tableau 5. 13. Comparaison de SSEA (*d* =1) et GOSSIP [18]

Nombre total de nœuds *N*	**Temps en Rounds [18]**	**Temps en Rounds (SSEA) *d* =1**		
		$\frac{N}{8}$	$\frac{N}{4}$	$\frac{N}{3}$
65	11	5	8	9
129	13	8	10	11
257	15	10	12	13
513	16	12	15	16

Tableau 5. 14. Comparaison de SSEA (*d* =0.75) et GOSSIP [18]

Nombre total de nodes *N*	**Temps en Rounds [18]**	**Temps en Rounds (SSEA) *d* =0.75**		
		$\frac{N}{8}$	$\frac{N}{4}$	$\frac{N}{3}$
65	11	5	8	9
129	13	8	10	11
257	15	10	12	13
513	16	12	15	16

Tableau 5. 15. Comparaison de SSEA (*d* =0.5) et GOSSIP [18]

Nombre total de nœuds *N*	**Temps en Rounds [18]**	**Temps en Rounds (SSEA) *d* =0. 5**		
		$\frac{N}{8}$	$\frac{N}{4}$	$\frac{N}{3}$
65	11	5	8	9
129	13	8	10	11
257	15	10	13	14
513	16	13	15	16

Tableau 5. 16. Comparaison de SSEA (*d* =0.25) et GOSSIP [18]

Nombre total de nœuds *N*	**Temps en Rounds [18]**	**Temps en Rounds (SSEA) *d* =0.25**		
		$\frac{N}{8}$	$\frac{N}{4}$	$\frac{N}{3}$
65	11	5	8	9
129	13	8	10	11
257	15	10	13	14
513	16	13	15	16

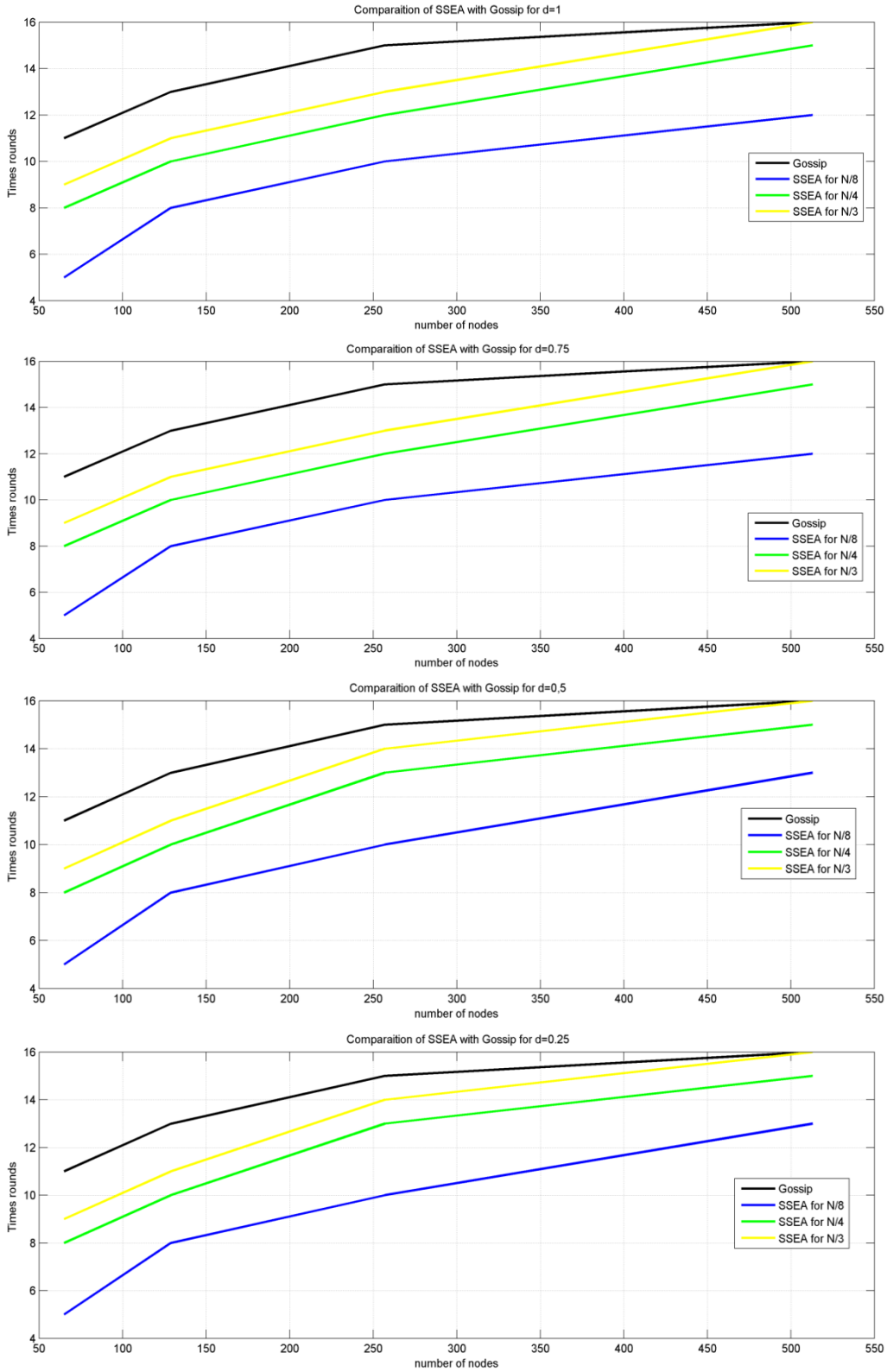


Figure 5. 14. Comparaison de SSEA et Gossip[18].

Enfin, on peut confirmer que SSEA est bénéfique en termes de réduction de temps et de consommation d'énergie, donc le coût de la communication est ainsi réduit.

En final, on s'est limité aux simulations produites dans cette thèse, mais avec d'autres simulations, d'autres fonctions et des changements des paramètres, le modèle pourrait fournir de nouveaux avantages et ainsi des perspectives sont donc lancées.

5.4. Conclusion

Dans ce chapitre, on a pu donner une brève description de notre modèle proposé constitué de 4 communautés et un ''EXTERNAL'', dont l'échange d'information est basé sur l'algorithme SSEA (utilisé par la technologie PSN) dans la zone ''EXTERNAL''. Deux scénarios ont été considérés : le déplacement entre les communautés et la recherche du ''member-agent'' lors d'une forte congestion empêchant ainsi le ''node-agent'' d'atteindre sa communauté cible. La recherche du ''member-agent'' est selon une condition de sécurité définie par le paramètre *d* définissant le nombre de communautés auxquelles le ''member-agent'' appartient. On a aussi introduit le SSEA adopté par la technologie PSN utilisée pour l'échange d'information.

Cette technique de communication peut aussi servir de moyen de liaison entre les nœuds des WSN et les stations de bases lors de coupures de l'Internet.

Une simulation de l'algorithme SSEA est effectuée. Dans une première étape, on a commencé par une comparaison entre le SEA et le SSEA pour une totale population de même degré de sécurité. Pour ce cas, la différence est remarquable par un décalage dans le temps du au temps défini t_1 qui caractérise la valeur du degré de sécurité. La deuxième situation caractérise la communication entre seulement les nœuds coopératifs, où on a considéré plusieurs cas avec des degrés de sécurité différents et des taux de coopération différents. Le temps d'infection est remarquablement réduit pour les degrés de sécurité élevés. On a pu voir aussi que, dans tous les cas, le coût énergétique est réduit aux nœuds sélectionnés. Pour la troisième situation, on a étudié l'influence de la valeur de t_1 sur la réponse du système ; où on a remarqué que la seule influence est la latence dans le temps qui peut être bornée par le choix d'une valeur réduite de t_1. Une deuxième comparaison de SSEA avec Gossip[18] a été effectuée, où on a considéré plusieurs cas de coopération en disposant de valeurs fournies par GOSSIP[18]. L'ensemble des mesures effectuées a montré que SSEA est effectivement bien meilleur que GOSSIP[18]. Enfin on peut

affirmer qu'à travers les résultats de comparaison obtenus, l'initiative et le recours au développement de SSEA sont amplement justifiés vu la preuve d'efficacité démontrée.

Conclusion Générale

Cette recherche a introduit un nouveau modèle IOT. Il s'agit d'un réseau de capteurs sans fil (WSN) particulier. Dans ce modèle, les nœuds (personnes dotées de leurs Smartphones) voyagent entre un ensemble de communautés et un ‘‘EXTERNAL’’. Cette définition prouve sa valeur lorsque les nœuds sont déconnectés. Alors, ils utilisent la technique PSN pour échanger l’information. La coopération des nœuds voisins est le facteur clé pour établir le lien. La popularité et la réputation des nœuds mesurent la confidentialité des messages. Cette technique de communication est définie par le degré de sécurité *d*, qui reflète le nombre de communautés auxquelles appartient le nœud. Pour ce modèle, la communication est suggérée confidentielle grâce à SSEA défini qui ne permet la communication qu’avec des nœuds de valeurs de *d* élevées. Afin de simuler cet algorithme, on s’est limité à quatre communautés, c’est à dire quatre valeurs de *d* : 1,0.75, 0.5, 0.25. Une étude comparative avec les travaux GOSSIP [18] a permet de confirmer l’efficacité du modèle IOT-PSN.

Comme toutes les méthodes de communication, cette méthode présente aussi certains inconvénients. Le premier est la rupture d'un lien lorsque les nœuds sont absents [8, 17]. Etant donné que la méthode se concentre sur les zones à forte congestion, ce problème est désormais éliminé. L’autre facteur est le temps d’attente de réponse pouvant être qualifié de durée longue en raison de l'absence de coopération des nœuds, et sous autres contraintes, expliqué par la non disponibilité des nœuds ou leur disponibilité avec une batterie faible ou une charge faible. Cette situation produit un problème qui n'est pas permanent ; car par essence le nœud est en permanence à la recherche de nœuds coopératifs. Ainsi il y a un retard de communication mais pas son extinction. La réduction de la sécurité des communications peut se produire lorsque tous les nœuds ont des degrés de sécurité faibles.

D'autre part, cette méthode offre un avantage de valeur qui se traduit par le pouvoir de fonctionner sans structure spécifique et sans technologie spécifique [9]. Lorsqu'aucune connexion Internet n'est disponible, cette méthode basée sur l'identification cognitive est excellente pour obtenir un lien entre les nœuds [9, 13]. Grâce à la sélection d'un nombre réduit de nœuds avec des degrés de sécurité élevés, cette méthode offre un faible coût de

communication avec des liens plus sécurisés. Toutes les technologies de mise en réseau peuvent être utilisées [13-15] : Wifi, Bluetooth, Ultrasons.....

Comme l'objectif principal du PSN est de maintenir le lien réseau sous des conditions environnementales complexes incluant ainsi son adaptation avec les pannes matérielles ainsi que les pannes logicielles (protocoles) ; cette méthode peut servir comme liaison de secours pour les réseaux WSN lors des ruptures de lien avec la station de base.

Ainsi, on estime que dans le futur, lorsque tous les réseaux sans fil se réuniront pour assurer des liaisons permanentes, les méthodes basées sur le PSN seraient positionnées en leader et entreront en concurrence directe avec le réseau Internet.

Bibliographie

[1].Challal Y., ‘‘Systèmes Intelligents pour le Transport ; Réseaux de Capteurs Sans Fils’’, Version 1 SIT60, 2008.

[2].Karen R., Scott E., Lyman C., “The internet of things: an overview”, Reston, VA 20190 USA, 2015.

[3].Crabtree A., Tolmie P., “A Day in the Life of Things in the Home”, CSCW '16, 1736-1748, 2016, DOI: 10.1145/2818048.2819954.

[4].Cinta C., Daniel C., Gonçalves J., Kuniwake J., “Pratical Introduction to Internet of Things: Practice using Arduino and Node.js”, the 22nd Brazilian Symposium on, 17-18, 2016, DOI:10.1145/2976796.2988224.

[5].Stout W., Urias V., “Challenges to securing the Internet of Things”, ICCST, 1-8, 2016, DOI: 10.1109/CCST.2016.7815675.

[6].Ruiz M., Álvarez E., Serrano A., García E., “The Convergence between Wireless Sensor Networks and the Internet of Things, Challenges and Perspectives: a Survey”, IEEE Latin America Transactions, 14, 10, 4249-4254, 2016, DOI: 10.1109/TLA.2016.7786301.

[7].Lingel J., “The Poetics of Socio-Technical Space: Using Craft to Reflect on the Internet of Things”, the 2016 CHI Conference, 815-826, 2016, DOI:10.1145/2858036.2858399.

[8].Djibrilla I., ‘‘Réseaux de collecte de données pour les zones blanches étendues’’, Thèse de doctorat de l’Université Paris-Saclay, Paris, France, 2019.

[9].Sarkar R., Rasul K., Chakrabarty A., “Survey on Routing in Pocket Switched Network, Wireless Sensor Network”, **7,** 9, 113-128, 2015, DOI: 10.4236/wsn.2015.79010.

[10].Papaj J., Dobos L., Palitefka R., “Candidate node selection based on trust for cognitive communication of mobile terminals in hybrid MANET-DTN”, CogInfoCom, 61-66, 11/2014, DOI: 10.1109/CogInfoCom.2014.7020415.

[11].Priyantha N., “The Cricket Indoor Location System”, PhD Thesis, University of Cambrige, Boston, MIT, USA, 2005.

[12].Priyantha N., Chakraborty A., Balakrishnan H., “The Cricket Location-Support System”, the 6th annual international conference, 32-43, 2000, DOI: 10.1145/345910.345917.

[13].Amah T., Kamat M., Abu Bakar K., Moreira W., Oliveira-Jr A., Batista M., “Spatial Locality in Pocket Switched Networks”, WoWMoM, 1-5, 2016, DOI: 10.1109/WoWMoM.2016.7523583.

[14].Bromberg Y., Grace P., Réveillère L., “Starlink: runtime interoperability between heterogeneous middleware protocols”, ICDCS, 446-455, 2011, DOI:10.1109/ICDCS.2011.65.

[15].Emruli B., “Ubiquitous Cognitive Computing: A Vector Symbolic Approach”, PhD Thesis, Luleå University of Technology, Luleå, Sweden, 2014.

[16].Mohamed T., ‘‘Sécurisation de l’Internet des objets’’, Réseaux et télécommunications [cs.NI], Université Paris-Saclay, Paris, France, 2018.

[17].Genç Z., Özkasap Ö., “Peer-to-Peer Epidemic Algorithms for Reliable Multicasting in Ad Hoc Networks”, International Journal of Electronics and Communication Engineering, 1, 3, 575-579, 2007, DOI: 10.5281/ZENODO.1069985.

[18].Yang R., Analysing the efficiency and robustness of gossip in different propagation processes with simulations, Journal of Physics: Conference Series, 1486, 3, 032001, 04/2020, DOI: 10.1088/1742-6596/1486/3/032001.

[19].Kevin A. , “That ‘Internet of Things’ Thing”, Report; Part2, RFiD Journal, 2010.

[20].Dirk H., Evangelos P., “Society: Build digital democracy”, Nature Journal, 527, 7576, 33-34, 11/2015, 10.1038/527033a.

[21].Nicolas G., ‘‘Architectures protocolaires interopérables pour le réseau de collecte de l’Internet’’, Thèse de doctorat, Réseaux et télécommunications [cs.NI], Université Toulouse le Mirail, Toulouse II, France, 2020.

[22].Jean-Pierre H., ‘‘L’Internet des objets Deux technologies clés: les réseaux de communication et les protocoles’’, REE, 4, 2016.

[23].Guillaume G., ‘‘Approche de gestion orientée service pour l’Internet des objets (IoT) considérant la Qualité de Service (QoS)’’, Thèse de doctorat, Réseaux et télécommunications [cs.NI], INSA de Toulouse, Toulouse, France, 2018.

[24].Hend B., ‘‘les fondamentaux d’IOT’’, PRIDA Track 1 (T1), 8/2020.

[25]. ‘‘Présentation générale de l'Internet des objets’’, UIT-T, Y.2060, 2012.

[26].Imad S., ‘‘internet des objets (IOT) Concept, Enjeux, Défis et Perspectives eISTE Openscience, 2018.

[27].Harald S., Patrick G., Peter F., Sylvie W., “Vision and challenges for Realising the Internet of Things”, CERP-IoT, 3/ 2010.

[28].OASIS “Advancing open standards for the information society”, URL https://www.oasis-open.org/, visité le 31/08/2022.

[29].Frederic L., ‘‘Internet des Objets centré service autocontrôlé’’, Thèse de Doctorat, Autre [cs.OH], Conservatoire national des arts et métiers - CNAM, France, 2019.

[30].Alexis B., Benoît P., Guillaume A., ‘‘Synthèse sur les protocoles de communication pour l’Internet des objets de l’industrie 4.0’’, [Rapport Technique] LS2N, Université de Nantes, Nantes, France, 2019.

[31].Klaus F., “RFiD handbook fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication”, third edition, 3rd edition John Wiley & Sons, Ltd, 2010.

[32].Landt J., “The history of RFID”, IEEE Potentials, 24, 4, 8-11, 2005, DOI: 10.1109/MP.2005.1549751.

[33].Wolfgang I., Michael H., “Weaknesses of the ISO/IEC 14443 protocol Regarding Relay attacks”, RFID-TA, 335-342, 2011, doi: 10.1109/RFID-TA.2011.6068658.

[34].Thomas S., Heydt B., Daniel V., Kevin F., et al., “Vulnerabilities in first-generation RFID-enabled credit cards”, FC’07, 2-14, 2007.

[35].Klaus F., “Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities”, In 5th European Workshop on RFID Systems and Technologies, 1-31, 2009.

[36].Luca M., Luigi P., Antonio V., “Evolution of wireless sensor networks towards the Internet of Things: A survey”, SoftCOM, 1-6, 2011 .

[37].Carles G., Josep P., “Wireless home automation networks: A survey of architectures and technologies”, IEEE Commun Mag. 48, 6, 92-101, 2010, DOI: 10.1109/MCOM.2010.5473869.

[38].IEEE STANDARDS ASSOCIATION, “IEEE standard for local and metropolitan area networks”, Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks, IEEE Computer Society, 2012, ISBN: 978-0-7381-7259-0. URL:http://ieeexplore.ieee.org/servlet/opac?punumber=6190696.

[39].IEEE STANDARDS ASSOCIATION, (2013) “IEEE standard for local and metropolitan area networks. Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)”, Amendment 5: Physical layer specifications for low energy, critical infrastructure monitoring networks, IEEE Computer Society, 2013, ISBN: 978-0-7381-8446-3. URL:http://ieeexplore.ieee.org/servlet/opac?punumber=6581826.

[40].Anis K., Mario A, Eduardo T., “GTS allocation analysis in IEEE 802.15.4 for real-time wireless sensor networks”, In the Proceedings of the 20th IEEE International Parallel Distributed Processing Symposium, 8, 2006, DOI: 10.1109/IPDPS.2006.1639415 .

[41].De D., Giuseppe A., Seghitti A., Anastasi G., “From IEEE 802.15. 4 to IEEE 802.15. 4e: A step towards the internet of things”, In Advances onto the Internet of Things. Springer International Publishing, 260, 135-152, 2014, DOI: 10.1007/978-3-319-03992-3_10.

[42].Nacer K., Mohamed R., Driss B., Michael G., “Wireless Sensor Network for Internet of Things”, ISSNIP, 1-6, 2014.

[43].Montenegro G., Kushalnagar N., Hui J., Culler D., “Transmission of IPv6 Packets over IEEE 802.15.4 Networks”. RFC 4944. Internet Requests for Comments. RFC Editor, Network Working Group, 2007.

[44]. Wei L., Xiaoling Z., Yang X., Fuqiang W., et al., “Survey and experiments of WIA-PA specification of industrial wireless network”, Wirel. Commun. Mob. Comput., 11, 8, 1197-1212, 8/2011, DOI:10.1002/wcm.976, URL:https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.976, visité le 30/05/2022.

[45].Stig P., Simon C., “WirelessHART Versus ISA100.11a : The Format War Hits the Factory Floor”, IEEE Ind. Electron. Mag., 5, 4, 23-34, 12/2011 DOI: 10.1109/MIE.2011.943023, URL: http://ieeexplore.ieee.org/document/6102417/.

[46]. Kim A., Frederik H., Stig P., Paula D., “When HART goes wireless : Understanding and implementing the WirelessHART standard”, ETFA. 899-907, 2008, DOI: 10.1109/ ETFA.2008.4638503.

[47].Baker N., “ZigBee and Bluetooth strengths and weaknesses for industrial applications”, Computing Control Engineering Journal, 16, 2, 20-25. 4/2005, DOI: 10.1049/cce:20050204.

[48].Mirko F.,Claudio P., Maurizio A.,Claudio B., “On the performance of ZigBee Pro and ZigBee IP in IEEE 802.15.4 networks”, IEEE 9th International Conference WiMob, 83-88, 2013, DOI: 10 . 1109 / WiMOB. 2013. 6673344.

[49].Carsten B., Angelo P., Zach S., “CoAP : An Application Protocol for Billions of Tiny Internet Nodes”, IEEE Internet computing, 16, 2, 62-67, 3/2012, DOI: 10.1109/MIC.2012.29.

[50].Mario C., Giovanni P., Timothy T., Ozan K., “Bluetooth 5 : A Concrete Step Forward toward the IoT”, IEEE Commun. Mag, 56, 7, 125-131, 7/2018, DOI: 10.1109/MCOM.2018.1700053.

[51].Carles G., Joaquim O., Josep P., “Overview and Evaluation of Bluetooth Low Energy : An Emerging Low-Power Wireless Technology”, Sensors Journal, 12, 9, 11734-11753, 8/2012, DOI: 10 . 3390 / s120911734.

[52].Wim D., “IEEE 802.11 Wireless Method and Physical Specification: 802.11 MAC Requirements and Comparison Criteria”, Power 5.10, 1993.

[53].IEEE Computer Society et LAN/MAN Standards Committee, “Information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 11, wireless LAN medium access control (MAC) and physical layer (PHY) specifications”, OCLC : 38598622. New York, N.Y: Institute of Electrical and Electronics Engineers, 1997, ISBN : 978-1-55937-935-9.

[54].IEEE Computer Society, “Supplement to IEEE standard for Information technology– telecommunications and information exchange between systems– local and metropolitan area networks – specific requirements : part 11 : wireless LAN medium access control (MAC) and physical layer (PHY) specifications : High-speed physical layer in the 5 GHz band”, OCLC: 50293188. New York, N.Y., USA: Institute of Electrical and Electronics Engineers, 1999 ISBN : 978-0-7381-1809-3. URL: http://ieeexplore.ieee.org/lpdocs/epic03/standards.htm.

[55].IEEE Computer Society, “IEEE Standard for Information technology–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements”, IEEE Std 802.11e-2005, 11/2005, DOI: 10.1109/IEEESTD.2005.97890.

[56].Yujun C., Dong Y. et Huachun Z., “Det-WiFi : A Multihop TDMA MAC Implementation for Industrial Deterministic Applications Based on Commodity 802.11 Hardware”, Wireless Communications and Mobile Computing, 1-10, 2017.

[57].Boris B., “IEEE 802.11ax : High-efficiency WLANS”, IEEE Wireless Communications 23, 1, 38-46, 2016, DOI: 10.1109/MWC.2016. 7422404.

[58].Adriana B., Ryan E., Edward W., Peter E., et al., “IEEE 802.11 af: a standard for TV white space spectrum sharing”, IEEE Commun. Mag., 51, 10, 92-100, 2013 DOI: 10.1109/MCOM.2013.6619571.

[59].Demian L., Roman M., “Comparison of 802.11 af and 802.22 standards–physical layer and cognitive functionality”, Elektro Revue, 3, 2, 12-18, 6/2012, ISSN: 1213-1539.

[60].Adame T., Albert B., Boris B., Jaume B., et al., “IEEE 802.11 AH : the WiFi approach for M2M communications”, IEEE Wireless Communications, 21, 6, 144-152, 2014, DOI: 10.1109/MWC.2014.7000982.

[61].Khorov E., Lyakhov A., Krotov A., Guschin A. “A survey on IEEE 802.11ah : An enabling networking technology for smart cities Computer Communications”, Computer Communications, 58, 53-69, 3/2015, DOI: 10.1016/j.comcom.2014.08.008.

[62].3GPP, URL : http://www.3gpp.org/, visité le 20/06/2022.

[63].Zayas A. D., Merino P., “The 3gpp NB-IoT system architecture for the Internet of Things”, ICC Workshops, 277–282, 05/2017, DOI: 10.1109/ICCW.2017.7962670.

[64].Hoglund A., Lin X., Liberg O., Behravan A., et al., « Overview of 3gpp Release 14 Enhanced NB-IoT”, IEEE Network, 31, 6, 16–22, 11/2017, DOI:10.1109/MNET.2017.1700082.

[65].Ratasuk R., Vejlgaard B., Mangalvedhe N., Ghosh A., “NB-IoT system for M2m communication”, WCNC, 1–5, 4/ 2016 DOI: 10.1109/WCNC.2016.7564708.

[66].Éclairage intelligent Philips Hue, URL : https://www2.meethue.com/fr-fr/decouvrir-hue, visité le 24/04/2022.

[67].Good Night Lamp, URL: http://goodnightlamp.com/, visité le 24/04/2022.

[68].Google Home., URL :https://store.google.com/product/google_home, visité le 24/04/2022

[69].Nest. Thermostats Nest, URL : https://nest.com/fr/thermostats/, visité le 16/04/2022.

[70].Lockitron. Lockitron,, URL : https://lockitron.com/, visité le 25/05/2022

[71].Tado. Tado, 2018. URL : https://www.tado.com/fr, visité le 25/05/2022.

[72].Insight Robotics, Forestry-Focused Risk Management, URL: https://www.insightrobotics.com/en/, visité le 31/08/2022.

[73].Hikob. Systèmes d’acquisition de données stationnaires par Hikob, URL : https://www.hikob.com/instant/, visité le 18/05/2022.

[74].All Traffic Solutions IoT Solutions for Smart Parking &Transportation Mgmt., URL : http://www.alltrafficsolutions.com/, visité le 20/05/2022.

[75].Cantaloupe Systems, URL : https://www. cantaloupesys.com/, visité le 20/05/2022.

[76].SenseAware, URL : https://www.senseaware.com/ , visité le 20/05/ 2022.

[77].Alexander S., 2016, "The Internet of Things: Business Applications, Technology Acceptance, and Future Prospects", Doctoral Thesis, Julius Maximilian University of Würzburg,Germany, https://opus.bibliothek.uni-wuerzburg.de/frontdoor/index/index/year/2016/docId/13160.

[78]. Rong X.,Yingxin Z., Xiao H., Fan Z., et al., "A Hybrid Task Crash Recovery Solution for Edge Computing in IoT-Based Manufacturing", IEEE Access, 9, 10220-106231, 2021, DOI: 10.1109/ACCESS.2021.3068471.

[79].Zhida G., Zhirong Z., Weidong L., "Establishment of Intelligent Identification Management Platform in Railway Logistics System by Means of the Internetof Things", Procedia Engineering, 29, 726–730, 2012. DOI :10.1016/j.proeng.2012.01.031.

[80].Pierre-Luc L., '' Les drones et l'imagerie satellitaire en agriculture'', 7e Colloque céréales à paille et canola, 9/1/2019,

[81].Bumblebee Project Home / Blog, URL: http://niksargent.com/bumblebee/, visité le 30/08/2022.

[82].HydroPoint. Irrigation Systems, Water Conservation & Leak Detection, 2022. URL:https://www.hydropoint.com/, visité le 31/05/2022.

[83].Ji-chun Z., Jun-feng Z., Yu F., Jian-xin G. "The study and application of the IOT technology in agriculture". 2010 3rd International Conference on Computer Science and Information Technology, 2, 462–465, 7/2010, DOI: 10.1109/ICCSIT.2010.5565120.

[84].Streetline, URL: https://www.streetline.com/, visité le 01/09/2022.

[85].Livehoods, URL: http://livehoods.org/, visité le 1/9/2022.

[86].BigBelly Solar: Transforming Trash Collection Operations,URL: https://www.telit.com/resources/case-studies/bigbelly-solar/, visité le 20/06/2022.

[87].Bhaumik C., Ghose A., Jha A., Sharma M., et al. "Road condition monitoring and alert application: Using in-vehicle smartphone as internet-connected sensor". In 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (Percom Workshops), 00, 489–491, 03/2012, DOI: 10.1109/PerComW.2012.6197543.

[88].Michael B., Rodger L., “IoT interoperability: A hub-based approach”, 79–84. IEEE, October 2014. ISBN 978-1-4799-5154-3. DOI: 10.1109/IOT.2014.7030119. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7030119.

[89].Foschini L., Taleb T., Corradi A., Bottazzi D., “M2M-based metropolitan platform for IMS-enabled road traffic management in IoT”, IEEE Commun. Mag., 49, 11, 50–57, 11/2011. DOI: 10.1109/MCOM.2011.6069709.

[90].Sanchez L., Muñoz L., Galache J., Sotres P., et al., “SmartSantander: IoT experimentation over a smart city testbed”, Computer Networks, 61, 217–238, 03/2014, DOI:10.1016/j.bjp.2013.12.020.

[91].Elmangoush A., Coskun H., Wahle S., Magedanz T., “Design aspects for a reference M2M communication platform for Smart Cities”, 2013 9th International Conference on Innovations in Information Technology (IIT), 204–209, 03/2013, DOI: 10.1109/Innovations.2013.6544419.

[92].Marah R., El Hibaoui A., “Algorithms for Smart Grid management”, Sustainable Cities and Society, 38, 627–635, 04/2018, DOI:10.1016/j.scs.2018.01.041.

[93].Nazmus S., Khandakar A., Mark A., Manoj D., “Software defined neighborhood area network for smart grid applications”, Future Generation Computer Systems, 79, 500–513, 02/2018, DOI:10.1016/j.future.2017.09.064.

[94].Echelon - Street Lighting, URL: https://www.Echelon.com/, visité le 01/09/2022.

[95].Wattics, URL: https://www.wattics.com/, visité le 01/09/2022.

[96].AirCasting, URL: http://aircasting.org/, visité le 01/09/2022.

[97].Air Quality Egg. Air Quality Egg - Science is Collaboration, URL : https: //airqualityegg.com/, visité le 01/09/2022.

[98].Netamo. Capteur de qualité de l’air intérieur - Healthy Home Coach, URL: https://www.netatmo.com//en-us/security, visité le 01/09/2022.

[99].Zang J., Qi A., “The application of Internet Of Things (IOT) in emergency management system in China”. 2010 IEEE International Conference on Technologies for Homeland Security (HST), 139–142, 11/ 2010. DOI: 10.1109/THS.2010.5655073.

[100].Gachet D., de Buenaga M., Aparicio F., Padrón V., “Integrating Internet of Things and Cloud Computing for Health Services Provisioning: The Virtual Cloud Carer Project”. 2012

Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 918–921, 07/2012, Doi:10.1109/IMIS.2012.25.

[101].Mu-Hsing K., "Opportunities and Challenges of Cloud Computing to Improve Health Care Services", J Med Internet Res, 13, 3, e67, 21/09/2011, DOI: 10.2196/jmir.1867.

[102].Lei Y., Yang L., XiaoJuan Z., "Smart Hospital based on Internet of Things", Journal of Networks, 7, 10, 1654-1661, 10/2012, DOI: 10.4304/jnw.7.10.

[103].Doukas C., Maglogiannis I., "Bringing IoT and Cloud Computing towards Pervasive Healthcare". 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 922–926, 07/2012, DOI: 10.1109/IMIS. 2012.26.

[104].BIOPAC, System France, URL:https://www.biopac.com/product-category/ research/ telemetry-and-data-logging/bioharness/, visité le 20/04/2022.

[105].Lechal Wearble Tech & GPS Navigation Device, URL: http://www.lechal.com, visité le 21/04/2022

[106].Mimo, URL: https://babyjourney.net/, visité le 01/09/2022.

[107].UCIC, URL: http://www.ucic.io/, visité le 30/08/2022.

[108].Electricfoxy Pulse, URL: http://www.electricfoxy.com/pulse/, visité le 20/05/2022.

[109].Yanzi, URL: https://www.yanzi.se/, visité le 20/05/2022.

[110]. en-Gauge Life Safety Monitoring, URL: http://www.engaugeinc.net,visité le 21/05/2022.

[111].Google Glass, URL: https://x.company/glass/. Visité le 25/06/2022.

[112].Smart Structures, URL: http://www.smart-structures-inc.com, visité le 01/06/2022.

[113].Paul M., "Real World Data ANN-based Analysis for Smart Cities", URL: http://www.motionloft.com.

[114].Sun E., Zhang X., Li Z., "The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in Mines", Safety Science, 50,4, 811–815, 04/2012, DOI:10.1016/j.ssci.2011.08.028.

[115].White D., Esswein S., Hallstrom J., Ali F., et al., "The Intelligent River©: Implementation of Sensor Web Enablement technologies across three tiers of system architecture : Fabric, middleware, and application", 2010 International Symposium on Collaborative Technologies and Systems, 340–348, 05/2010, DOI: 10.1109/CTS.2010.5478493.

[116].Sachit B., Giovanni P., Paul P., Fausto D., et al., "Influance of robotic shoal size, configuration, and activity on zebrafish behavior in free-swimming environment", ScienceDirect, 275,269-280, 2014.

[117].Tinka A., Rafiee M., Bayen A., "Floating Sensor Networks for River Studies", IEEE Systems Journal, 7, 1, 36–49, 03/2013. DOI: 10.1109/JSYST.2012.2204914.

[118].Hossam M., "Concepts, Applications, Experimentation and Analysis of Wireless Sensor Networks", second Edition, Springer, 2016.

[119].Arampatzis T., Lygeros J., Manesis S., "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks", IEEE International Symposium on Mediterranean Conference on Control and Automation, 719-724, 06/2005.

[120].Lyes K., Nadjib B., "Revisiting Directed Diffusion In The Era Of IoT-WSNs: Power Control For Adaptation to High Density", 8th International Conference On Information, Intelligent Systems and Applications(IISA), 2017.

[121]. Thierry A., ''Des réseaux de capteurs sans fil à l'intelligence ambiante dans le suivi envirennemantal. Synthèse de travaux. Modélisation et simulation'', Thèse d'Habilitation, Université de Corse Pasquale Paoli, Corse, 2019.

[122].Amit R., Randeep S., Abhishilpa N., "Wireless sensor networks-Challenges and Possibilities", International Journal of Computer Applications,140,2,0975-8887, 04/2016.

[123].Jennifer Y., Biswanath M., Dipack G., "Wireless sensor network survey", Computer Networks, 52,12, 2292–2330, 08/2008, DOI: 10.1016/j.comnet.2008.04.002.

[124].Lan F., Weillian S., Yogesh S., Erdal C., "A survey on sensor networks", IEEE Commun Mag 40, 8,102–114, 08/2002.

[125].Kostas B., Dimitris A., "Signal processing & communication challenges in sensor networks", First Greek SP Jam, IEEE Signal Process Society,17/10/2009.

[126].Akyildiz I., Stuntebeck E., "Wireless underground sensor networks: research challenges", AdHoc Networks, 4, 6, 669–686, 11/2006.

[127].Li M, Liu Y, "Underground structure monitoring with wireless sensor networks", IPSN'07, 69-78, 04/2007.

[128].Akyildiz I., Pompili D., Melodia T., "Challenges for efficient communication in underwater acoustic sensor networks", ACM SIGBED Review, 1, 2, 3-8, 07/2004.

[129].Heidemann J., Li Y., Syed A., Wills J., Ye W., “Underwater sensor networking: research challenges and potential applications”, IEEE wireless communications and networking conference (WCNC), 228-235, 2006.

[130].Rawat P., Singh K., Chaouchi H., Bonnin J., “Wireless Sensor Networks: a survey on recent development and potential synergies”, J Supercomput, 68, 1, 1-48, 04/2014, DOI: 10.1007/s11227-013-1021-9.

[131].Benoit A., ‘‘Algorithmique des réseaux et des télécoms’’, Notes de cours (ENS Lyon, M1), Chapitre3: Réseaux sans fil, 2006.

[132].XIANGYANG L., “Wireless Ad Hoc and Sensor Networks Theory and Applications’’, Cambridge University Press, 2008.

[133].LEHSAINI M., ‘‘Diffusion et couverture basées sur le clustering dans les réseaux de capteurs : application à la domotique’’, Thèse de Doctorat En Informatique, Université de Franche-Comté U.F.R Sciences et Techniques, France, 2009.

[134].Global Inventures/Zigbee. Zigbee alliance, URL: http//www.zigbee.org, visité le 05/09/2022.

[135].Adame T., Bel A.,Boris B., Jaume B., et al. , “IEEE 802.11AH : the WiFi approach for M2M communications” , IEEE Wireless Communications, 21, 6, 144-152, 12/2014, DOI: 10.1109/MWC.2014.7000982.

[136].Evgeny K., Andrey L., Alexander K., Andrey Guschin, “A survey on IEEE 802.11ah: An enabling networking technology for smart cities”, Computer Communications, 58, 53-69, 01/03/ 2015, DOI: 10.1016/j.comcom.2014.08.008.

[137].ANT technology, URL:http://www.thisisant.com/technology, visité le 15/04/2022.

[138].Dugas C., “Coronis Systems, Wavenis ULP long range wireless platforms, sensing, and M2M monitoring solutions”, M2M Workshop ETSI, Sophia Antipolis, 04/06/2008-05/06/2008.

[139].EnOcean, Url:http://www.enocean.com/en/enocean-wireless-standard/, visité le 20/04/2022.

[140].Jin C., “Data Aggregation in Wireless Sensor Networks”, Doctoral Thesis of philosophy, Networking and Internet Architecture, [cs.NI], INSA Lyon, France, 2016.

[141].Sami_Mnasri, Thierry V., Nasri N., ‘‘Contribution au déploiement optimisé des réseaux de capteurs sans fil’’, Journées Nationales des communications Terrestres (JNCT), Toulouse-Blagnac, ISBN :978-3-8417-3468-6, 22/052014-23/05/2022.

[142].Claude C., ‘‘La Sécurité des Capteurs et Réseaux de Capteurs’’, PLANETE INRIA, 06/2008, URL: https://team.inria.fr/privatics/claude-castelluccia/.

[143].Ali J., ‘‘Le Clustering basé sur la Classification Spectrale pour l'Optimisation d’Energie dans les Réseaux de Capteurs Sans Fil Homogènes’’, Thèse de doctorat, université MOHAMMED V, Faculté des Sciences, Rabat, Maroc, 2015.

[144].El Hanafi T., ‘‘Cryptographie à base de courbes elliptiques pour la sécurisation des traitements et des échanges d’informations dans les RCSF’’, Thèse de doctorat, université Paris 8, Paris, France, 2020.

[145].Mandicou B., Olivier F., Ibrahima N., Florent N., ‘‘Routage et agrégation de données dans les réseaux de capteurs sans fil structurés en clusters auto-stabilisants’’, Special issue CARI’14, ARIMA Journal, 21, 85-107, 2015.

[146].Samira C., ‘‘ Tolérance aux pannes dans un réseau de capteurs sans fil multi-canal’’, Informatique et language [cs.CL], Thèse de Doctorat, Université de Paris-Est, Université de Manouba (Tunisie), 2016.

[147].Diery N., ‘‘Optimisation de la durée de vie dans les réseaux de capteurs sans fil sous contraintes de couverture et de connectivité réseau. Réseaux et télécommunications [cs.NI], Thèse de Doctorat, Université de Haute Alsace – Mulhouse, Université Cheikh Anta Diop (Dakar), 2016.

[148].Mehdi B., ‘‘Protocoles de communication et optimisation de l’énergie dans les réseaux de capteurs sans fil, Réseaux et télécommunications [cs.NI], Thèse de Doctorat, Université du Maine, France, 2016.

[149].Karla B., ‘‘ Optimisation des communications dans les réseaux de capteurs hétérogènes’’, Thèse de Doctorat en Informatique, Université BOURGOGNE FRANCHE-COMTE, France,2018.

[150].Deni Y., Satria M., Anazida Z., Dewi N., “Performance Comparison of Baseline Routing Protocols In Pocket Switched Network”, Jurnal Teknologi, 72,1,1-6, 2016.

[151].Fall K., “A Delay-Tolerant Network Architecture for Challenged Internets”, *SIGCOMM*’03, 27-34, 25/08/2003-29/08/2003.

[152].Dong W., Li C., Miao Z., "Joint Link State and Forwarding Quality: A Novel Geographic Opportunistic Routing in VANETs", The International Conference on Computer, Information and Telecommunication Systems (CTIS), 1-5, 07/2016.

[153].Minea M., Claudia S., Stăncel I., Viviana L., "Combined Opportunistic Vehicular/Cellular Networking for Cooperative Driving Assistance in Highway Scenarios", The International Conference on Applied and Theoretical Electricity (ICATE), 1-6, 2016.

[154].Seguí J., Jennings E., "Delay Tolerant Networking – Bundle Protocol Simulation", The 2nd IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT'06), 235-240, 2006.

[155].Raveneau P., Rivano H., "Tests Scenario on DTN for IoT. III Urbanet collaboration", [Technical Report] RT-0465, Inria-Research Centre, Grenoble, Rhone-Alpes, France, 2015.

[156].Stusek M., Masek P., Kovac D., Ometov A., et al., "Remote Management of Intelligent Devices: Using TR-069 Protocol in IoT", The 39th IEEE International Conference on Telecommunications and Signal Processing (TSP), 74-78, 2016.

[157].Simatic J., Cherkaoui A., Bastos RP., Fesquet L., "New Asynchronous Protocols for Enhancing Area and Throughput in Bundled-Data Pipelines", The 39th IEEE International Conference on Telecommunications and Signal Processing (TSP) 1-6, 2016.

[158].Burleigh S., "Delay-Tolerant Electronic Commerce", The IEEE International Conference on Wireless Communications and Signal Processing (STP), 1-4, 2015.

[159]. Bijan B., Satchidanand D., Bijaya K., Ajit K., et al., "Computational Intelligence in Sensor Networks", Volume 776, Springer, 2019.

[160].Gamit V., Patel M., "Evaluation of DTN routing protocols", IJERST, 3, 2, 588-592, 02/2014.

[161].Jain S., Fall K., Patra R., "Routing in a delay tolerant network". SIGCOMM'4, 145–158, 08/2004.

[162]. Amah, T.E., Kamat M., Moreira W., Bakar K., et al., "Towards next generation routing protocols for pocket switched networks", J. Network Computer Appl., 70, 51-88, 2016.

[163].Shen J., Moh S., Chung I., "Routing protocols in delay tolerant networks: A comparative survey", The 23rd International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2008), 6–9, 2008.

[164].Alessandro M., Giacomo M., Paolo S., Julinda S., “Social-Aware Stateless Routing in Pocket Switched Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2, 1, 252-261, 01/2015

[165].Keränen A., Ott J., Kärkkäinen T., “The ONE Simulator for DTN Protocol Evaluation”, The 2nd International Conference on Simulation Tools and Techniques (ICST), SIMUTools, 02/03/2009-06/03/2009, DOI: 10.1145/1537614.1537683.

[166].Mehta N., Shah M., “Human-mobility-based spray and wait: Efficient routing protocol for pocket switched networks” Int. J. Future Generation Commun. Networking, 9, 1, 11–22, 2016.

[167].Spyropoulos T., Psounis K., Raghavendra C., “Spray and wait: an efficient routing scheme for intermittently connected mobile networks”, The 2005 ACM SIGCOMM workshop on Delay-tolerant networking, 252–259, 2005.

[168].Vahdat A., Becker D., “Epidemic routing for partially-connected ad hoc networks”. Tech. rep., Duke Univ., Duhram, NC, England, 2000, URL: http://issg.cs.duke.edu/epidemic/epidemic.pdf.

[169].Rasul K., Makaroff D., Stanley K.G., “Hybrid community-based forwarding: A complete energy efficient algorithm for pocket switched networks”, The 40th IEEE Local Computer Networks Conference Workshops (LCN Workshops), 760–768, 2015.

[170].Zhang X., Neglia G., Kurose J., Towsley D., “Performance modeling of epidemic routing”, Computer Networks, 51, 10, 2867–2891, 2007.

[171].Kumari S., Yadav P., Yadav M., “Review of efficient routing in delay tolerant network”, ijecs, 4, 12, 15165-15171, 12/2015.

[172].Lindgren A., Doria A., Schelén O., “Probabilistic routing in intermittently connected networks”. ACM SIGMOBILE Mobile Computing Commun. Rev., 7, 3, 19–20, 2003.

[173].Zhang F., Joe I., Gao D., LiuY., “An efficient multiple-copy routing in intermittently connected mobile networks”, Int. J. Future Generation Commun. Networking, 9, 5, 207–218, 2016.

[174].Huang T., Lee C., Chen L., “Prophet+: An adaptive prophet-based routing protocol for opportunistic network”, The 24th IEEE International Conference on Advanced Information Networking and Applications, 112–119, 04/ 2010.

[175].Uddin M., Ahmadi H., Abdelzaher T., Kravets R., "Intercontact routing for energy constrained disaster response networks", IEEE Trans. Mobile Computing, 12,10, 1986–1998, 2013.

[176].Hui P., Crowcroft J., Yoneki E., "Bubble Rap: social-based forwarding in delay-tolerant networks", IEEE Trans. on Mobile Computing, 10, 11, 1576–1589, 2011.

[177].Huang J., Cheng X., Bi J., Chen B., "Wireless relay selection in pocket switched networks based on spatial regularity of human mobility", Sensors 16, 1, 94, 18/01/2016, DOI: 10.3390/s16010094.

[178].Barua R., Shadman S., Chakrabarty A., "Pngp: A social relationship based routing algorithm for pocket switched network", The 19th International Conference on Computer and Information Technology (ICCIT), 25–30, 12/2016.

[179].Bayir M., Demirbas M., "On the fly learning of mobility profiles for routing in pocket switched networks", Ad Hoc Networks, 16, 13–27, 2014.

[180].Bulut E., Szymanski B., "Friendship based routing in delay tolerant mobile social networks", The IEEE Global Telecommunications Conference (GLOBECOM 2010), 1–5, 2010.

[181].Mei A., Morabito G., Santi P., Stefa J., " Show me your friends and I'll tell you what you like". Extremecom 2010 Dharamsala, India, 2010.

[182].Mei A., Morabito G., Santi P., Stefa J., "Social-aware stateless forwarding in pocket switched networks", The 30th IEEE International Conference on Computer Communications (IEEE Infocom 2011), 251–255, 2011.

[183].Fida M., Ali M., Adnan A., "Socialcircle: A message forwarding technique for pocket switched networks" The 6th IEEE International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1–7, 2015.

[184].McGeehan D., Lin D., Madria, S., "Chitchat: An effective message delivery method in sparse pocket-switched networks", The 36th IEEE International Conference on Distributed Computing Systems (ICDCS), 457–466, 2016.

[185].Zheng Y., Li Q., Chen Y., Xie X., Ma W., "Understanding mobility based on GPS data", The 10th International Conference on Ubiquitous Computing (UbiComp '08), 312–321, 2008.

[186]. Fida M., Ali M., "Community-based heuristic routing protocol for disrupted social network", The 11th IEEE Malaysia International Conference on Communications (MICC), 222–227, 26/11/2013-28/11/2013.

[187].Hui P., Crowcroft J., Yoneki E., "Bubble Rap: Social-Based Forwarding in Delay Tolerant Networks", MobiHoc'08, 241-250, 26/05/ 2008-28/05/2008.

[188].Douglas J., "Towards efficacy and efficiency in sparse delay tolerant networks", Doctoral thesis of philosophy, Computer Science, MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY, Colombia, 2020.

[189].Wang E., Yang Y., Wu J., "Energy efficient phone-to-phone communication based on wifi hotspot in psn", The 24th International Conference on Computer Communication and Networks (ICCCN), 1-8, 2015.

[190].Wang E., Yang Y., Wu J., Liu W., "Phone-to-phone communication utilizing wifi hotspot in energy-constrained pocket switched networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, 65, 10, 8578-8590 10/ 2016.

[191].Nguyen A., Senac P., Diaz M., "Understanding and Modeling the Small-World Phenomenon in Dynamic Networks", MSWiM'12, 377-384, 21/10/2012-25/10/2012.

[192].Nguyen A., Senac P., Diaz M., "How disorder impacts routing in human-centric disruption tolerant networks", The ACM SIGCOMM workshop on Future human centric multimedia networking, 47–52, 2013.

[193].Ochiai H., Esaki H., Ishizuka H., Kawakami Y., "A field experience on dtn-based sensor data gathering in agricultural scenarios", IEEE Sensors, 955–958, 11/ 2010.

[194].Ntareme H., Zennaro M., Pehrson B., "Delay tolerant network on smartphones: Applications for communication challenged areas", The 3rd Extreme Conference on Communication (ExtremeCom'11), 14, 1–14, 26/09/2011-30/09/2011.

[195].Pathan A., Lee H., Hong C., "Security in wireless sensor networks: issues and challenges", The 8th International Conference Advanced Communication Technology (ICACT), 2, 1043 - 1048, 20/02/2006-22/02/2006.

[196].Pfleeger C., Pfleeger S., Margulies J., "Security in computing", Prentice Hall, Fifth edition, 2015.

[197].Pietiläinen A., Oliver E., LeBrun J., Varghese G., et al., “Mobiclique: middleware for mobile social networking”, The 2nd ACM workshop on Online social networks (WOSN’09), 49–54, 17/08/2009.

[198].Rasul K., Nuerie N., Pathan A., “An enhanced tree-based key management scheme for secure communication in wireless sensor network”, The 12th IEEE International Conference on High Performance Computing and Communications (HPCC 2010), 671–676, 09/2010, DOI: 10.1109/HPCC.2010.14.

[199].Prescott G., Smith S., Moe K., “Information system technology challenges for nasas earth science enterprise”, IEEE 2001 International Geoscience and Remote Sensing Symposium (Cat. No.01CH37217), 1, 484-486, 2001.

[200].Sharma A., Navda V., Ramjee R., Padmanabhan V., et al, “Cool-tether: Energy efficient on-the-fly wifi hot-spots using mobile phones”, The 5th International Conference on Emerging Networking Experiments and Technologies (CoNEXT’09), 109–120, 01/12/2009-04/12/2009.

[201]. Maül C., ‘‘Détection de communautés orientée Sommet pour des réseaux mobiles opportunistes sociaux’’, Thèse de Doctorat, Informatique, Université Pierre et Marie Curie, Paris, France, 2017.

[202]. Scott K., Burleigh S., “bundle protocol specification”, Memo, RFC: 5050, NASA Jet Propulsion Laboratory ,11/2007.

[203]. Morgenroth J., Schildt S., Wolf L., “A bundle protocol implementation for android devices” Thee 18th annual international conference on Mobile computing and networking [Mobicom'12], 443-446, 08/2012, DOI: 10.1145/2348543.2348606.

[204]. Khouni S., Chemali H., “SSEA for PSN: A novel Secure technique of communication through IOT devices”, Sigma J Eng Nat Sci, 40, 2, 300-309, 06/2022, DOI: 10.14744/sigma.2022.00034.

[205]. “Setting up Visual Studio 2010 for your first OpenGl Project”, URL: http://gamedev.dlivingstone.com/.

[206]. Shreiner D.,“Opengl programming-guide: the official guide to learning OpenGl, versions 3.0 and 3.1”, Seventh Edition, Addison-Wesley, 2010.

[207].Movania M., “OpenGL Development Cookbook”, PACKT PUBLISHING, 2013.

[208].Hill F., “ computer graphics using openGl hill book”, excerpt For ECE660 Fall 1999, 3rd edition.pdf (pdf), 2007. URL:https://scholar.cu.edu.eg/eldeib/files/computer_graphics_using_opengl_by_f_s_hill-jr_and_stephen_m__3rd_edition-2007.pdf.

[209]. Joey D., “ Learn OpenGl; An offline transcript of learnopengl.com”, ME :), 3rd printing, LEARNOPENGL.COM, 2017, URL:https://learnopengl.com/book/learnopengl_book.pdf.

[210]. إياد هلالي ، ”دليل المبرمج إلى OpenGl“ ،البراق للطباعة و النشر و التوزيع، الطبعة الأولى 2004-1425.

[211].OpenGl Architecture Review Board, “OpenGL Reference Manual; The official reference document for OpenGl”, Addition-Wesley, ISBN 0−201−63276−4, 1993.

ملخص: الخوارزمية الوبائية البسيطة (SEA) هي بروتوكول اجتماعي يستخدم في تقنية شبكة تبديل الجيب (PSN). يصيب SEA جميع المستخدمين. لقد حددنا خوارزمية آمنة وبسيطة (SSEA) لـ PSN حيث تتحكم درجة الأمان في حركة الانتقال. SSEA لا تصيب كل المستخدمين. نظرًا لأن إنترنت الأشياء (IOT) ليس له تعريف محدد، فقد اقترحنا نموذجًا جديدًا لـ IOT. في هذا الأخير ، تضمن PSN التي تستخدم SSEA المطور تبادل المعلومات. لفهم أفضل ، حددنا نموذجًا صغيرًا بأربعة مجتمعات ونموذج'' خارجي''. العقد التي تنتقل بين المجتمعات لها درجات أمان مختلفة. تعكس درجة الأمان عدد المجتمعات التي تنتمي إليها العقدة وتحدد حالة أمان SSEA. يعتمد تبادل المعلومات على العقد المتعاونة. تقديم المساعدة والخدمات الإضافية في الزمان والمكان تحدد هذا التعاون. في أفضل الأحوال ، تصيب SSEA العقد ذات درجات الأمان العالية وتقلل من تكلفة اتصالات الشبكة. يمكن استخدام هذا النموذج كحل استعجالي لربط WSN بمحطاتها الأساسية.

كلمات مفتاحية: شبكة التأخير المسموح ، شبكة تبديل الجيب، شبكة الأدهك، الوبائية، إنترنت الأشياء، شبكة الاستشعار اللاسلكية

Résumé: Simple Epidemic Algorithm (SEA) est l'un des protocoles sociaux utilisés dans la technologie Pocket Switched Network (PSN). SEA infecte une population entière. On a défini un algorithme d'épidémie simple sécurisé (Secure Simple Epidemic Algorithm (SSEA)) pour le PSN où une condition de sécurité contrôle le trafic et que SSEA n'infecte pas une population entière. Vu que l'Internet des objets (IOT) n'ayant pas de définition spécifique, on a proposé un nouveau modèle d'IOT. Dans ce dernier, le PSN qui utilise le SSEA développé garantit l'échange d'informations. Pour mieux comprendre, on a défini un petit modèle avec quatre communautés et un ''EXTERNAL''. Les nœuds voyageant entre les communautés ont des degrés de sécurité différents. Le degré de sécurité reflète le nombre de communautés auxquelles appartient le nœud et produit la condition de sécurité de SSEA. L'échange d'informations repose sur les nœuds coopératifs. La fourniture d'aide et de services supplémentaires dans le temps et dans l'espace identifie la coopération. Dans le meilleur des cas, SSEA infecte les nœuds avec des degrés de sécurité élevés et réduit le coût de communication réseau. Ce modèle peut servir comme une solution secours pour relier les WSN avec leurs stations de base.

Mots clés: Internet des Objets, Réseaux de Capteurs sans Fil, Réseau commuté de poche, Réseau tolérant aux retards, Epidémique, Ad-hoc network.

Abstract: Simple Epidemic Algorithm (SEA) is a social protocol used in the Pocket Switched Network (PSN) technology. SEA, generally, infects an entire population. We have defined a Secure Simple Epidemic Algorithm (SSEA) for PSN where a security condition controls the traffic and the SSEA doesn't infect a global population. As the Internet Of Things (IOT) has no specific definition, we have proposed a new model of IOT. In this latter, PSN using the developed SSEA guarantees the exchange of information. For simplicity, a small model comprising four communities and an ''EXTERNAL'' is defined. Nodes traveling between communities have different security degrees. The security degree reflects the number of communities to which a node belongs and provides security condition for SSEA. The exchange of information relies strongly on cooperative nodes. Supplying help and extra services in time and space identify cooperation. In the best case, SSEA infects nodes with high security degrees and reduces the network communication cost. This model can be used as a backup solution to link WSN to corresponding base stations.

Keywords: Internet Of Things, Wireless Sensor Network, Pocket Switched Network, Delay Tolerant Network, Epidemic, Ad-hoc network.