الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Département : Génie électrique Et Informatique Industrielle

Mémoire de projet de fin d'études Pour l'obtention du

Diplôme de Master en

Automatique

Spécialité

Automatique et informatique industrielle

Etude comparative entre les protocoles utilisés en smart grid

Réalisé par

Triki Mohammed Hichem **Atba Bilal**

Composition du Jury:

Président	M. A. ZAOUI	Professeur	ENST
Promoteur	M. CHERIFI Tarek	M.C.B	ENST
Examinateur	Mme. OUSAADI Zahira	M.A.A	ENST
Examinateur	Mme.BENDOUDA Djamila	M.C.B	ENST

Année universitaire 2021-2022

REMERCIEMENT

En premier lieu, A Dieu le Miséricordieux qui a guidé nos pas vers un avenir Incha'allah prometteur, où le travail, la persévérance et la quête du savoir seront notre devise, et qui nous a donné la force pour accomplir ce travail.

Nous adressons nos remerciements à nos chers parents, sœurs et frères qu'on aime tant et sans lesquels on ne serait jamais arrivé là où on est

Nous tenons à notifier un remerciement spécial

Pour notre encadrant Mr.CHIRIFI pour sa disponibilité, son aide et pour ces conseils.

Nous exprimons nos profonds remerciements aux membres de jury pour leurs participations dans le jugement de notre travail.

Nous présentons nos chaleureux remerciements à tous nos amis specialement Hadjab Chihab Eddine pour ces services on coté programmation, personnel de le groupement sh-brn

Mr. Fouzi bouhaouch, Mr.Nabil Laib et Mr.ramdane

Qui nous en a compagne dans le monde professionnelle de l'ingénieur

Table de matières

Remerciement ..... **Erreur ! Signet non défini.**

Table de matières 4

I Introduction 1

II Le réseau électrique intelligent (Smart Grid) 1

Définition 1

Intérêt du réseau intelligent 2

PRINCIPE DE FONCTIONNEMENT 3

Home Area Network (HAN) 4

Neighborhood Area Network (NAN) 4

Wide Area Network (WAN) 4

L'Applications de Smart Grid sur le réseau de communication 5

Les exigences de base 6

Formats de données pour l'échange de données 6

Formats d'adresse pour l'échange de données 6

Mappage d'adresses 7

Détection des erreurs de transmission 7

Accusés de réception 7

Direction du flux d'informations 7

Contrôle de séquence 7

Mise en file d'attente 8

Protocoles de routage pour HANs 8

Protocoles de routage pour ZigBee 9

IPv6 comme protocole de routage : 6LowPAN 11

Protocole de routage WirelessHART 12

Protocole de routage Z-Wave 12

Comparaison entre les Protocoles de routage pour HANs 13

Protocoles de routage pour les NAN 13

Reliable Routage dans les NAN sans fill 14

Secure routing pour les NAN sans fill 16

Qos routing 17

Table de Figures

Figure 1 : Domaine d’utilisation des smart grid 2

Figure 2 : Réseau de communication multi-niveau Smart Grid 3

Figure 3 : Réseau de communication Smart Grid à plusieurs niveaux 5

Figure 4 : Classification des protocoles de routage dans SG Communications 8

Figure 5 : topologie de réseaux zigbee 9

Figure 6 : l'attribution d'adresse pour la topologie arborescente 10

Figure 7 : Comparison entre mesh-under and rout-over 11

Figure 8 : routage par graphe 12

Figure 9 : Mécanisme de backtracking et détection de boucle. 15

Figure 10 : exemple de routage hybride 16

Figure 11 : comparaison entre les différents protocoles de routage 18

I Introduction

À l'échelle mondiale, l'adaptation des systèmes électriques est un chantier majeur. L'électrification des territoires ou la modernisation des réseaux électriques existants, les politiques d'efficacité énergétique ou de déploiement des énergies renouvelables, le développement des nouveaux usages de l'électricité ou encore l'introduction du véhicule électrique, sont en effet autant de défis auxquels de nombreux pays ou régions sont confrontés.

Issus de la convergence des technologies des systèmes électriques et des technologies de l'information et de la communication, les systèmes électriques intelligents, ou Smart Grids, jouent un rôle clé dans la réponse à ces enjeux.

Dans ce travail, nous allons d'abord faire le point sur le smart grid en général, ces techniques ainsi que ça utilisation dans l'industrie. Ensuite nous allons fait des point sur les protocoles utilisé dans smart grid Enfin, nous allons faire une comparaison entre ces protocoles.

II Le réseau électrique intelligent (Smart Grid)

Définition

Un réseau électrique intelligent, ou smart grid en anglais, est un réseau de production et de distribution d'électricité décentralisé qui contrôle le flux d'électricité entre fournisseurs et consommateurs selon des technologies de l'information et de la communication(TIC), collectant des informations sur l'état du réseau, ce dernier contribue à équilibrer la production, la distribution, la consommation et l'intégration des énergies renouvelables.

Ce type de réseaux intelligents utilise des techniques informatiques pour optimiser la production, la distribution, la consommation et éventuellement le stockage de l'énergie afin de mieux coordonner l'ensemble des mailles du réseau.

Les smart grids sont les réseaux de distribution du futur qui réuniront les technologies de l'électricité et de l'information. Ils seront capables de :

- Optimiser la production et la distribution,
- Mieux mettre en relation l'offre et la demande entre les producteurs et consommateurs d'électricité.
- Assurer la sécurité de fonctionnement du réseau en présence de production décentralisée intermittente et aléatoire (systèmes solaires.



Figure 1 : Domaine d'utilisation des smart grid

Intérêt du réseau intelligent

L'électricité ne pouvant être stockée facilement, rapidement et économiquement en grandes quantités, les technologies du « réseau intelligent » cherchent à ajuster en temps réel la production et la distribution (offre et demande) de l'électricité en hiérarchisant les besoins de consommation (quantité et localisation) selon leur urgence afin de :

- **Optimiser le rendement des centrales et/ou petites unités de production.**
- **Éviter d'avoir à construire régulièrement de nouvelles lignes.**
- **Minimiser les pertes en ligne.**
- **Optimiser l'insertion de la production décentralisée et diminuer ou éliminer les problèmes induits par l'intermittence de certaines sources (énergies solaire, éolienne, marémotrice et dans une moindre mesure hydroélectrique).**

PRINCIPE DE FONCTIONNEMENT

Les réseaux électriques traditionnels fonctionnent en mode centralisé. Ils sont conçus autour des centres de production afin d'acheminer le flux d'énergie jusqu'aux consommateurs finaux. Ce modèle unidirectionnel est appelé à évoluer vers un modèle multidirectionnel avec l'appui des réseaux intelligents.

SG n'utilisera pas un seul type de réseau de communication. Il n'existe pas de solution unique ou de réseau représentatif pour le SG car chaque service public aura des topographies, des régimes réglementaires et des systèmes de communication hérités différents. SG devrait être un réseau à plusieurs niveaux pris en charge par un maillage hybride de différentes technologies de communication pour fournir un accès efficace et fiable aux composants du réseau dans divers environnements, comme illustré sur la figure. 2. Principalement, il y aura trois composants de ce réseau à plusieurs niveaux qui peuvent déployer une variété de réseaux de communication, y compris câblés et sans fil, sous licence et sans licence, privés et commerciaux, fixes et mobiles, à bande étroite et à large bande. Contrôle de génération (AGC) pour l'estimation d'état, l'analyse des contingences, le flux de puissance optimal, etc.[1]

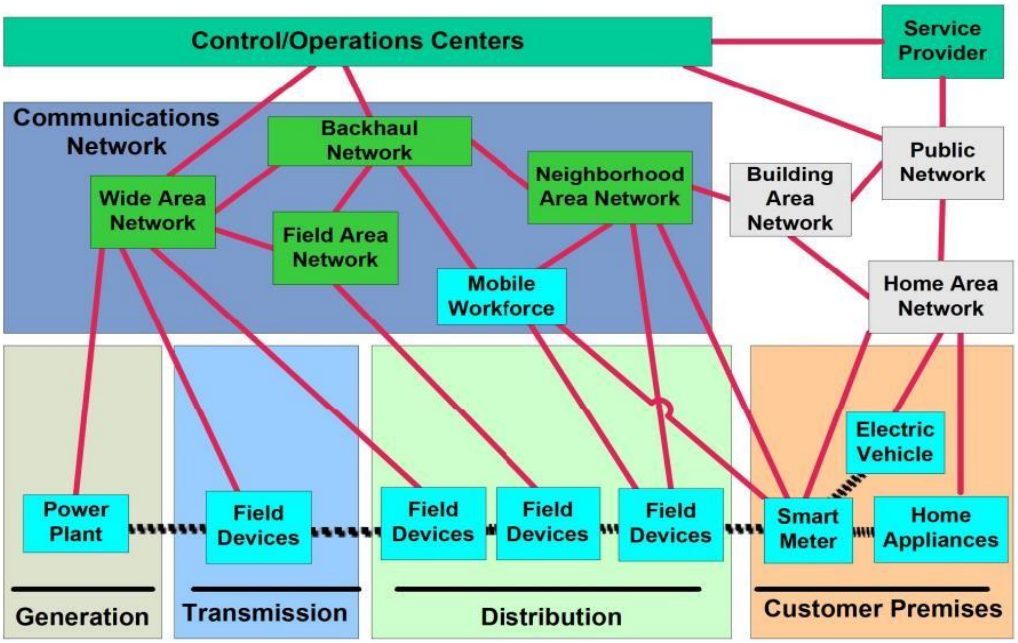


Figure 2 : Réseau de communication multi-niveau Smart Grid

Home Area Network (HAN)

HAN est situé dans le domaine du client et donne accès aux appareils domestiques. Chaque appareil domestique enverra ses lectures de puissance sur ce réseau au compteur domestique ou à la passerelle à l'extérieur de la maison pour l'application AMI. HAN permet également aux réseaux domotiques de surveiller et de contrôler les applications pour le confort de l'utilisateur, la gestion efficace de la maison et la DR application.

Les réseaux domotiques se composent de divers capteurs et actionneurs pour effectuer une variété d'applications, telles que le contrôle de la lumière, la télécommande, l'énergie intelligente, les soins à distance et la sécurité. et la sécurité. Par exemple, l'application de contrôle de la lumière permet de contrôler les lumières à partir de n'importe quel interrupteur ou de les activer par télécommande ou de les allumer/éteindre automatiquement en fonction des informations des capteurs ou Demande DR de la compagnie de services publics. Building/Business Area Network (BAN) est utilisé pour désigner des réseaux similaires lorsqu'ils sont mis en œuvre dans des entreprises, et Industrial Area Network (IAN) lorsqu'il est appliqué à un environnement industriel. [2]

Les communications sans fil dans HAN/BAN/IAN sont préférées aux communications filaires car elles permettent l'ajout et le retrait flexibles d'appareils et réduisent les coûts d'installation.

Neighborhood Area Network (NAN)

NAN connecte les compteurs intelligents aux points d'accès locaux pour les applications AMI. Cela peut être un réseau de compteurs intelligents créant un maillage, ainsi qu'une partie d'un réseau maillé, qui se compose de compteurs intelligents et de certaines passerelles pour relayer les données. La version de ce réseau qui est déployée pour collecter les données des lignes électriques, de la main-d'œuvre mobile, des tours, etc. pour la surveillance du réseau électrique est appelée Field Area Network (FAN). Dans cet article, nous utiliserons les NAN pour désigner les deux types de réseaux. La couverture d'un NAN serait d'environ 1 à 10 miles carrés. Le débit de données serait plus élevé que celui des HAN, environ autour de 10-1000 Kbps. La place des NAN dans le réseau SG Communications est illustrée à la Fig. 2. Les protocoles/normes possibles pour les NAN seraient basés sur des technologies sans fil et câblées.[3]

Wide Area Network (WAN)

Le WAN fournit un lien de communication entre le réseau et les principaux systèmes de services publics. Le WAN comprend deux types de réseaux : Core et Backhaul. Alors que le réseau central est utilisé pour connecter le réseau métropolitain du service public et des sous-stations, le réseau de liaison est utilisé pour connecter le NAN au réseau central. La couverture de ce réseau serait de l'ordre de milliers de kilomètres carrés tandis que les débits de données seraient compris entre 10 et 100 Mbps.

Les technologies sous-jacentes peuvent varier considérablement en fonction de la mise en œuvre. En ce qui concerne les technologies sans fil, des protocoles similaires (par exemple, WiMAX, 3GPP, RF Mesh) mentionnés dans NAN pourraient être utilisés pour un accès étendu dans le réseau de liaison. En fait, le réseau Backhaul peut être considéré comme faisant partie des NAN. Pour les options filaires, DSL ou réseaux optiques passifs (PON) peuvent être utilisés. Metro Ethernet pour le réseau central peut être mis en œuvre avec certaines technologies câblées telles que la commutation Internet Protocol/Multi Protocol Label (IP/MPLS) et la fibre (SONET).

L'Applications de Smart Grid sur le réseau de communication

Il existe de nombreuses applications telles que la réponse à la demande ou la surveillance du réseau qui peuvent utiliser HAN, NAN ou WAN ou une combinaison de ceux-ci, comme illustré à la Fig. 3.le département américain de l'énergie (DOE) détermine que la plupart, sinon la totalité , les applications dans SG peuvent être classées en six catégories fonctionnelles, comme expliqué dans les sous-sections suivantes.[4]

Ces applications doivent avoir une sécurité élevée, une fiabilité élevée et diverses exigences de qualité de service telles que la bande passante et la latence. Bien que certaines de ces exigences puissent être adressées uniquement à la couche de routage des HAN/NAN/WAN, il est fort probable que les approches inter couches améliorent les performances. Dans tous les cas, la conception des protocoles de routage est cruciale pour répondre à la plupart des exigences des applications.

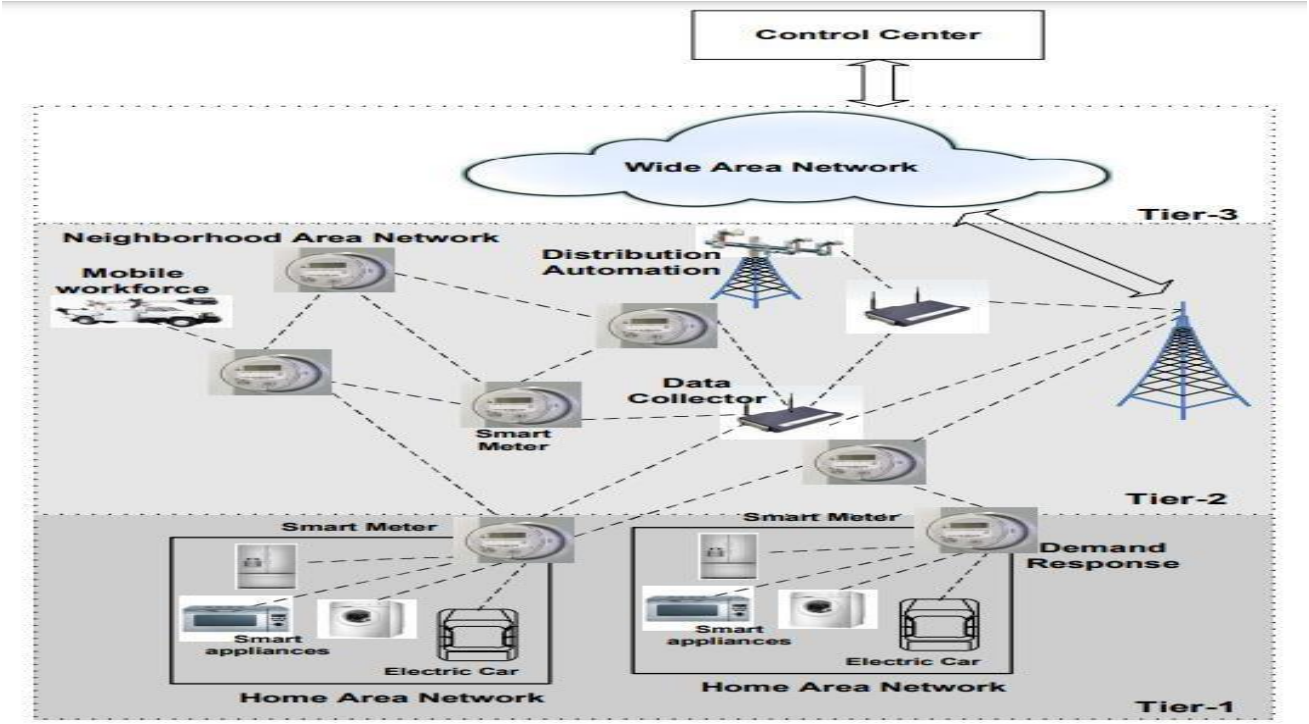


Figure 3 : Réseau de communication Smart Grid à plusieurs niveaux

II Protocol de communication

Un protocole de communication est un système de règles qui permet à deux ou plusieurs entités d'un système de communication de transmettre des informations via n'importe quel type de variation d'une grandeur physique. Le protocole définit les règles, la syntaxe, la sémantique et la synchronisation de la communication et les éventuelles méthodes de récupération d'erreur. Les protocoles peuvent être mis en œuvre par du matériel, des logiciels ou une combinaison des deux. Les protocoles de communication Internet sont publiés par l'Internet Engineering Task Force (IETF). L'IEEE (Institute of Electrical and Electronics Engineers) gère les réseaux filaires et sans fil et l'Organisation internationale de normalisation (ISO) gère d'autres types. L'UIT-T gère les protocoles et les formats de télécommunications pour le réseau téléphonique public commuté (PSTN). Au fur et à mesure que le RTPC et Internet convergent, les normes évoluent également vers la convergence. [5]

Les exigences de base

La transmission de données sur le réseau n'est qu'une partie du problème de protocole. Les données reçues doivent être évaluées dans le contexte de l'évolution du dialogue, le protocole doit donc contenir des règles décrivant le contexte. On dit que ces types de règles expriment la grammaire de la communication. D'autres règles déterminent si les données sont significatives dans le contexte dans lequel l'échange a lieu. On dit que ce type de règle exprime la sémantique de la communication.[6]

Formats de données pour l'échange de données

Des chaînes de bits de messages numériques sont échangées. Les chaînes de bits sont divisées en champs et chaque champ contient des informations relatives au protocole. Conceptuellement, la chaîne de bits est divisée en deux parties appelées l'en-tête et la charge utile. Le message réel est transporté dans la charge utile. La zone d'en-tête contient les champs pertinents pour le fonctionnement du protocole. Les chaînes de bits plus longues que l'unité de transmission maximale (MTU) sont divisées en morceaux de taille appropriée.[7]

Formats d'adresse pour l'échange de données

Les adresses sont utilisées pour identifier à la fois l'expéditeur et le(s) destinataire(s). Les adresses sont transportées dans la zone d'en-tête des chaînes de bits, ce qui permet aux récepteurs de déterminer si les chaînes de bits présentent un intérêt et doivent être traitées ou ignorées. Une connexion entre un émetteur et un récepteur peut être identifiée à l'aide d'une paire d'adresses (adresse de l'émetteur, adresse du récepteur). En général, certaines valeurs d'adresse ont des significations particulières. Une adresse all-1s pourrait être considérée

comme un adressage de toutes les stations du réseau, de sorte que l'envoi à cette adresse entraînerait une diffusion sur le réseau local. Les règles décrivant la signification de la valeur de l'adresse sont appelées collectivement un schéma d'adressage.

Mappage d'adresses

Les protocoles ont parfois besoin de mapper les adresses d'un système sur les adresses d'un autre système. Par exemple pour traduire une adresse IP logique spécifiée par l'application en une adresse MAC Ethernet. C'est ce qu'on appelle le mappage d'adresses.

Détection des erreurs de transmission

La détection des erreurs est nécessaire sur les réseaux où la corruption des données est possible. Dans une approche courante, un CRC de la zone de données est ajouté à la fin des paquets, ce qui permet au récepteur de détecter les différences dues à la corruption. Le récepteur rejette les paquets sur les différences de CRC et s'arrange d'une manière ou d'une autre pour les retransmettre

Accusés de réception

L'accusé de la réception correcte des paquets est nécessaire pour la communication orientée connexion. Les accusés de réception sont envoyés par les récepteurs à leurs expéditeurs respectifs.

Les paquets peuvent être perdus sur le réseau ou être retardés en transit. Pour y faire face, dans certains protocoles, un expéditeur peut attendre un accusé de réception correct de la part du récepteur dans un certain laps de temps. Ainsi, en cas de dépassement de délai, l'expéditeur peut être amené à retransmettre l'information. Dans le cas d'une liaison définitivement rompue, la retransmission n'a aucun effet ; le nombre de retransmissions est donc limité. Le dépassement de la limite de retransmission est considéré comme une erreur.

Direction du flux d'informations

La direction doit être prise en compte si les transmissions ne peuvent se faire que dans une seule direction à la fois comme sur les liaisons semi-duplex ou d'un seul expéditeur à la fois comme sur un support partagé. C'est ce qu'on appelle le contrôle d'accès au support. Des dispositions doivent être prises pour faire face au cas de collision ou de contention lorsque deux parties respectivement transmettent ou souhaitent transmettre simultanément.[8]

Contrôle de séquence

Si de longues chaînes de bits sont divisées en morceaux et envoyées individuellement sur le réseau, les morceaux peuvent se perdre ou être retardés ou, sur certains types de réseaux, prendre des chemins différents vers leur destination. Par conséquent, les morceaux peuvent arriver hors séquence. Les retransmissions peuvent donner lieu à des pièces en double. En marquant les morceaux avec des informations de séquence à l'expéditeur, le

récepteur peut déterminer ce qui a été perdu ou dupliqué, demander les retransmissions nécessaires et réassembler le message original.

Mise en file d'attente

Les processus de communication ou les machines à état utilisent des files d'attente (ou "tampons"), généralement des files FIFO, pour traiter les messages dans l'ordre d'envoi, et peuvent parfois avoir plusieurs files d'attente avec des priorités différentes

III Les protocoles utilisés dans smart grid

Nous explorerons les technologies de communication Smart Grid standard les plus pertinentes et les protocoles impliqués. Étant donné que le système électrique lui-même est un système des systèmes, chacun ayant ses propres exigences particulières en matière d'environnement et de performances, il n'est pas surprenant qu'une variété de supports et de protocoles de communication différents aient émergé pour prendre en charge ces différents systèmes. [9] Les protocoles utilise dans smart grid sont des protocoles de routage qu'en va l'Explorer

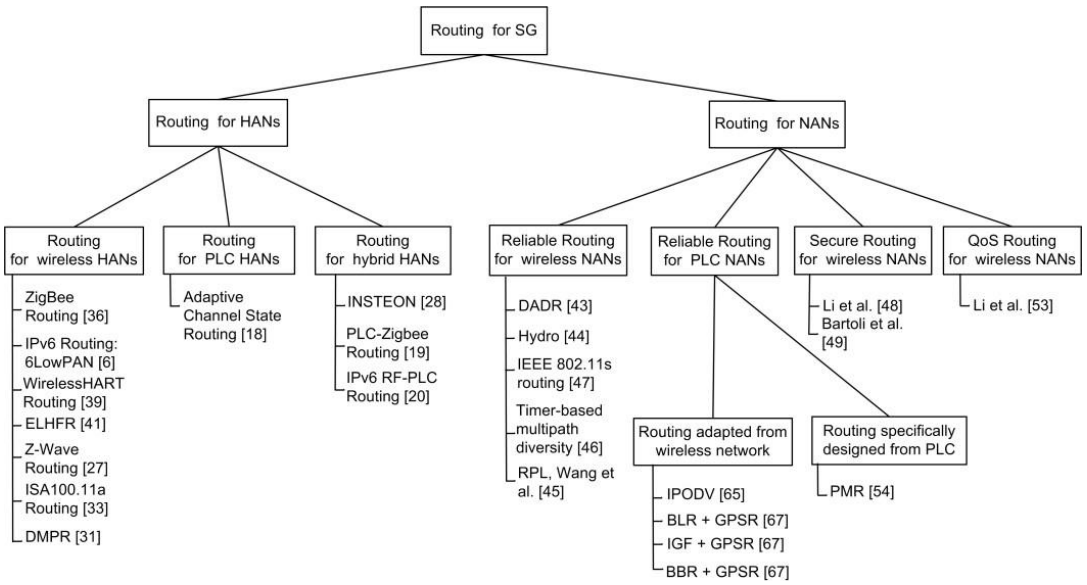


Figure 4 : Classification des protocoles de routage dans SG Communications

Protocoles de routage pour HANs

Plusieurs protocoles ont été recommandés pour les communications HAN. Celles-ci sont principalement basées sur les communications sans fil, dont certaines sont des normes ouvertes. Les normes ouvertes sont principalement basées sur la norme IEEE telle que

ZigBee, WirelessHART et ISA100.11a. Il existe également un certain nombre de protocoles propriétaires tels que Z-Wave , INSTEON et Wavenis.

Récemment, un certain nombre d'études ont ciblé la conception et la mise en œuvre de ces protocoles À la fin, nous fournissons également un résumé comparatif des principaux protocoles ainsi que leurs analyses.

Protocoles de routage pour ZigBee

ZigBee est une norme développée par ZigBee Alliance et recommandée comme choix courant pour les implémentations HAN. ZigBee construit sa couche réseau et sa couche application au-dessus de la norme IEEE. Il dispose de trois types d'appareils : coordinateur ZigBee, routeur et appareil terminal. Alors que le coordinateur et le routeur ZigBee sont tous deux des dispositifs à fonction complète (FFD) IEEE qui ont la capacité d'acheminer des paquets, un dispositif final est un dispositif à fonction réduite (RFD) IEEE qui a une fonction limitée et agit comme un nœud feuille dans le réseau. Comme le montre la Fig. 5, ZigBee prend en charge trois types de topologie de réseau : étoile, arbre et maillage. La topologie en étoile est une topologie à saut unique allant des périphériques finaux à un routeur ou à un coordinateur ZigBee, tandis que la topologie arborescente et maillée prend en charge les communications multi-sauts. Un seul coordinateur ZigBee est autorisé dans une topologie arborescente ou une topologie maillée pour gérer l'ensemble du réseau.[10]

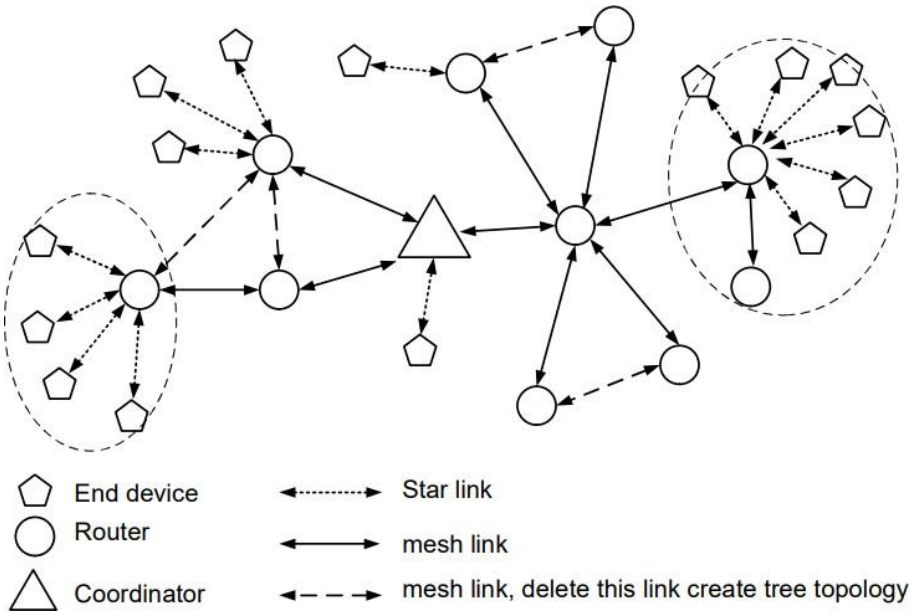


Figure 5 : topologie de réseaux zigbee

Le routage arborescent enraciné au niveau du coordinateur ZigBee est un routage proactif basé sur les relations parent-enfant établies lors de la phase de formation du réseau. Premièrement, le coordinateur ZigBee définit le nombre maximal de routeurs et d'équipements finaux par routeur, ainsi que la profondeur maximale de l'arborescence du réseau. Sur la base de ces trois paramètres, la couche réseau ZigBee effectue une attribution

d'adresse distribuée hiérarchique dans laquelle l'espace d'adressage réseau 16 bits est divisé par le coordinateur ZigBee à ses enfants en utilisant la récurrence suivante :

$$A(d) = \begin{cases} 1 + D_m + R_m & if\ d = L_m - 1 \\ 1 + D_m + R_m \times A(d+1) & if\ 0 \le \mathrm{d} < L_m - 1 \end{cases}$$

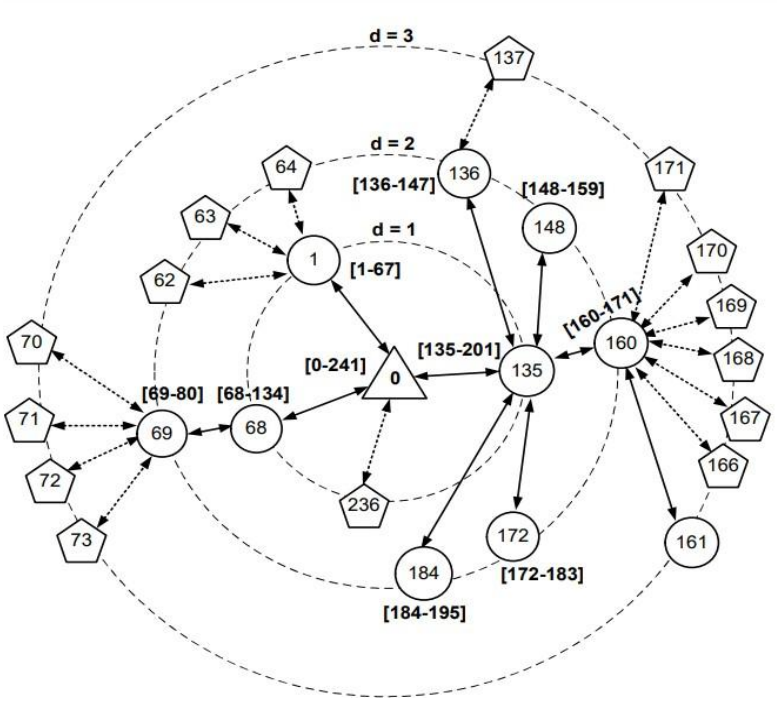
A(d) est le nombre d'adresses allouées à la profondeur d'arbre d.

Rm est le nombre maximum de routeurs connectés à un routeur.

Dm est le nombre maximal d'équipements finaux par routeur.

Lm est la profondeur maximale de l'arborescence du réseau

Le coordinateur et les routeurs prennent toujours la première adresse de l'espace d'adressage tandis que les équipements finaux prennent les dernières adresses Dm de l'espace d'adressage. Par exemple, la Figure 6. Montre l'attribution d'adresse pour la topologie arborescente de la Figure 5



· **Figure 6 :** l'attribution d'adresse pour la topologie arborescente

Lorsqu'un périphérique (soit un routeur, soit un périphérique terminal) rejoint un nœud parent pendant la formation du réseau, le nœud parent fournira une adresse à ce nœud à partir de son pool d'adresses. Étant donné que chaque routeur connaît son espace d'adressage, chaque routeur peut facilement déterminer si la destination appartient à l'un de ses enfants ou non. D'autre part, le routage maillé à la demande est basé sur le mécanisme de découverte de routage de Ad Hoc On Demand Distance Vector (AODV) Les routes sont

établies et stockées dans les tables de routage via les messages Path Request et Path Reply où l'appareil d'origine diffuse Path Request et le l'appareil de destination répond par un message Path Reply. Lorsque le périphérique d'origine est incapable de trouver l'itinéraire vers la destination dans sa table de routage et est également incapable d'initier la découverte d'itinéraire, le routage arborescent est utilisé en dernier recours.

IPv6 comme protocole de routage : 6LowPAN

6LowPAN est un acronyme de IPv6 over Low-power Wireless Personal Area Networks (WPAN). 6LowPAN construit une couche d'adaptation entre la couche MAC et la couche réseau pour permettre la transmission de paquets IPv6 sur IEEE 802.15.4 à travers :fragmentation en raison de la taille différente du paquet IPv6 (1280 octets) et de la taille de trame IEEE 802.15.4 (127 octets) headercompression de 40 octets d'en-tête IPv6 à 2 octets;IPv6 configuration automatique de l'adresse; et découverte de voisins IPv6 pourlowPAN.6LowPAN a deux catégories de routage basées sur quelle couche la décision de routage est effectuée: le maillage sous ou maillage de couche 2 où la décision de routage est prise au niveau de la couche d'adaptation; et le hop de hop de hop de couche 3 où la décision de routage est prise au niveau de la couche réseau.[11] Comme le montre la Figure 7. le routage et le transfert dans le mesh-under sont effectués à la couche de liaison. Un seul saut IP sera constitué de plusieurs couches de liaison houblon.

D'autre part, le routage et le transfert dans le routeover sont effectués au niveau de la couche réseau et de chaque saut de couche de liaison.est un saut IP comme le montre la Figure 6. Par exemple, le protocole de routage pour les réseaux à faible consommation et avec perte (RPL) [qui sera discuté dans la section suivante pour les NAN, est un protocole candidat pour le routage de routage et peut être utilisé dans les réseaux HAN ainsi que NAN.

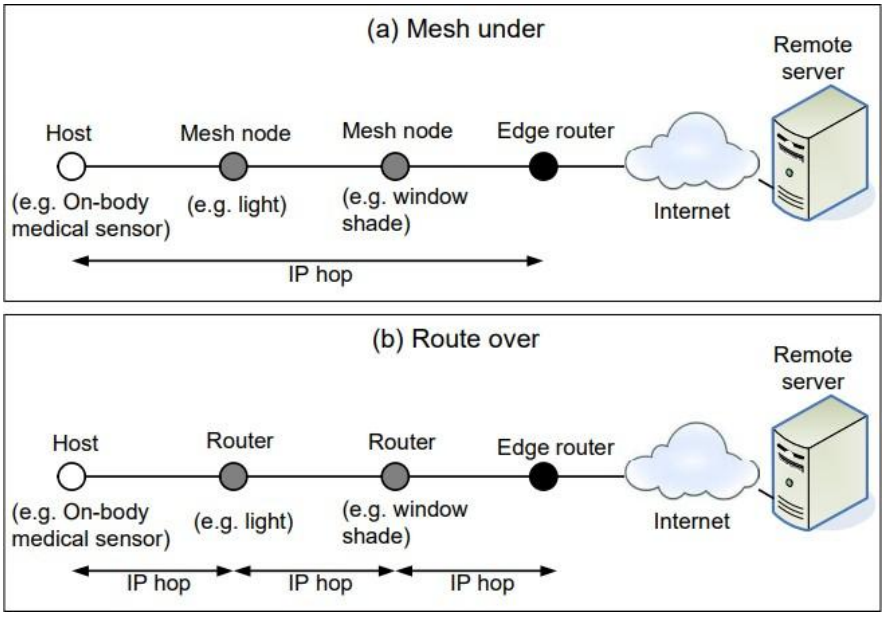


Figure 7 : *Comparison entre mesh-under and rout-over*

Protocole de routage WirelessHART

WirelessHART est une technologie couramment utilisée pour les applications industrielles en temps réel et convient aux applications dans le système d'alimentation électrique, comme dans une sous-station ou une centrale de production. Il s'agit en fait d'un réseau sans fil centralisé qui utilise un gestionnaire de réseau central pour fournir des horaires de routage et de communication statiques. Il utilise le routage graphique pour router les messages et le routage source pour les diagnostics [12]

Réseau. WirelessHART construit sa couche physique sur la base de la norme IEEE 802.15.4-2006 et spécifie les couches liaison de données, réseau, transport et application. Le gestionnaire de réseau dans WirelessHART tient à jour une liste complète de tous les appareils et connaît parfaitement la topologie du réseau. Il obtient ces informations de chaque périphérique réseau en extrayant les tables de voisinage de chaque périphérique réseau. Cette table de voisinage contient une liste de tous les périphériques auxquels un périphérique réseau peut se connecter. Sur la base de ces informations, le gestionnaire de réseau dispose d'un ensemble de routes de graphe non uniques qui peuvent se chevaucher. Chaque itinéraire de graphe est associé à un ID de graphe unique.

La figure 8 montre un exemple d'une topologie de réseau qui a deux ID de graphe : ID de graphe 1 et ID de graphe 2. Le nœud 1 envoie des paquets au nœud 3 en utilisant l'ID de graphe 2, soit via le nœud 2, soit directement au nœud 3. De même, le nœud 1 envoie des paquets au nœud 5 en utilisant le graphe ID 1 qui a plusieurs routes vers le nœud 5

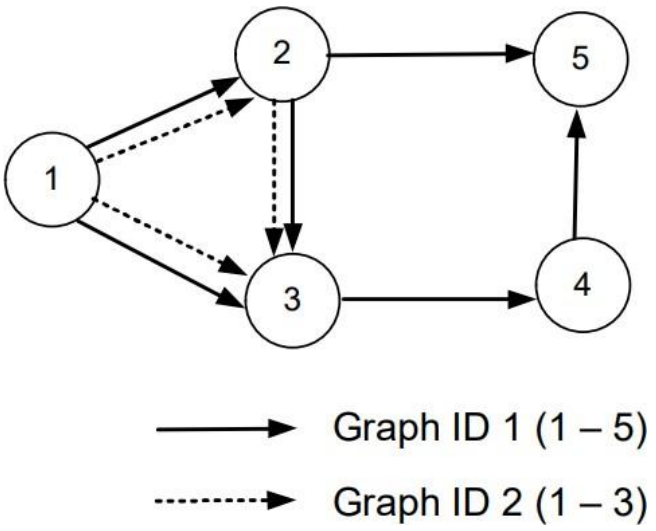


Figure 8 : routage par graphe

Protocole de routage Z-Wave

Z-Wave est une technologie propriétaire développée par ZenSys et destinée au contrôle et à l'automatisation de la maison. Elle se compose d'une pile de protocoles à cinq couches :

physique, MAC, transfert, routage et couche d'application. Z-Wave a deux types d'appareils de base : Contrôleur et Esclave. Le dispositif contrôleur peut émettre des commandes de contrôle tandis que l'esclave est un dispositif final qui exécute les commandes du contrôleur. Les contrôleurs sont davantage différenciés en fonction de leurs fonctions dans le réseau. Un contrôleur principal est le seul contrôleur du réseau maillé Z-Wave qui a la capacité d'inclure ou d'exclure des appareils dans le réseau et, par conséquent, il a le dernière topologie de réseau dans sa table de routage.

Z-Wave utilise un mécanisme de routage source au niveau de la couche de routage. Le contrôleur qui initie le message stocke un itinéraire complet de jusqu'à quatre sauts vers la destination dans la trame. Chaque nœud intermédiaire transmet le message selon cette route. Dans le cas d'un contrôleur portable, il essaiera d'atteindre la destination directement d'abord (c'est-à-dire sans routage) avant d'essayer de déterminer sa position et de trouver un nœud pouvant être utilisé comme point de départ pour répéter une trame. Sur la base de ce nœud de départ, il calcule le l'itinéraire le plus court vers la destination et place un itinéraire complet dans le cadre.[13]

Comparaison entre les Protocoles de routage pour HANs

En tableau 1 nous fournissons un résumé des protocoles de routage pour HAN en spécifiant les protocoles MAC et de couche d'adaptation associés. En particulier, le protocole MAC sous-jacent utilisé affecte la conception, le coût et les performances des protocoles de routage.

Routing Protocol	*Data Link*	*Adaptation Layer*	*Network Layer*
ZigBee	CSMA/CA	n/a	Tree routing, on-demand mesh routing, source routing
6LowPAN **- Mesh Under** **- Route Over**	 CSMA/CA CSMA/CA	 layer 2 mesh routing n/a	 n/a RPL routing
Wireless-HART	TDMA	n/a	graph and source routing
ISA100.11a	TDMA, CSMA/CA, graph routing and source routing	n/a	backbone routing
Z-Wave	CSMA/CA	n/a	Source routing
INSTEON	TDMA	n/a	Simulcast

Tableau 1 : Résumé des protocoles de routage pour les HAN

En a constaté pendant les caractéristiques citées avant que le zigbee est le meilleur protocole par ce qu'il fonctionné avec le routage arborescent qui donne un adressage fiable et rapide.

Protocoles de routage pour les NAN

De nombreuses applications de Smart Grid utilisent NAN. En particulier, les applications AMI ont jusqu'à présent reçu le plus d'attention de la part de la communauté des chercheurs. Dans de telles applications, les protocoles de routage se concentrent sur la transmission des données du niveau du point d'accès au niveau de distribution de liaison,

Cependant, selon la communication sous-jacente utilisée, les défis de routage peuvent différer.

Nous classons les protocoles de routage basés sur WMN en 3 catégories basées sur les exigences de SG : Routage Reliable, Routage secured et Protocoles de routage QoS.

Reliable Routage dans les NAN sans fill

Des ruptures de route fréquentes se produisent dans un réseau maillé sans fil en raison des effets d'évanouissement et des interférences de signal qui rendent la qualité des liaisons sans fil instable et variable dans le temps. Cela est particulièrement vrai pour les applications SG qui sont déployées dans des environnements difficiles. [14]

Pour résoudre ce problème et améliorer la fiabilité, trois approches ont été proposées pour Smart Grid :

- Utiliser plusieurs chemins
- Fournir un mécanisme de réparation de chemin rapide et efficace tout en minimisant la surcharge de contrôle
- la modification du calcul des paramètres de coût et l'utilisation d'un algorithme de prévention des fluctuations d'itinéraire.

Notez que ces techniques ont déjà été utilisées dans plusieurs réseaux tels que les réseaux de capteurs sans fil (WSN) et maintenant leur applicabilité à un réseau SG à grande échelle.

Backtracking

Cette approche offre plusieurs avantages dans les environnements sans fil peu fiables. Il s'adapte rapidement à la topologie qui change fréquemment en utilisant un autre itinéraire tout en transportant les informations sur la liaison défaillante dans le paquet de données. Donc les itinéraires sont mis à jour dynamiquement avec une faible surcharge de contrôle.

De plus, étant donné que les taux d'erreur binaire des liaisons dépendent de la taille du paquet, il fournit une topologie plus fiable par rapport à l'approche traditionnelle de découverte de route dans laquelle le paquet de contrôle est plus petit que le paquet de données. Cela évite également la divergence de fiabilité de la liaison car il n'y a pas de décalage horaire entre la découverte d'itinéraire et le transfert de données comme dans le routage traditionnel. Le routage traditionnel typique comporte deux étapes indépendantes :

- la découverte et la maintenance des itinéraires
- le transfert des données.

Un autre avantage est qu'au lieu de lancer une nouvelle découverte d'itinéraire lorsque tous les sauts suivants possibles échouent, il ramène le paquet à son expéditeur précédent afin que l'expéditeur précédent puisse essayer un autre itinéraire. Comme la figure 9 nous montre.

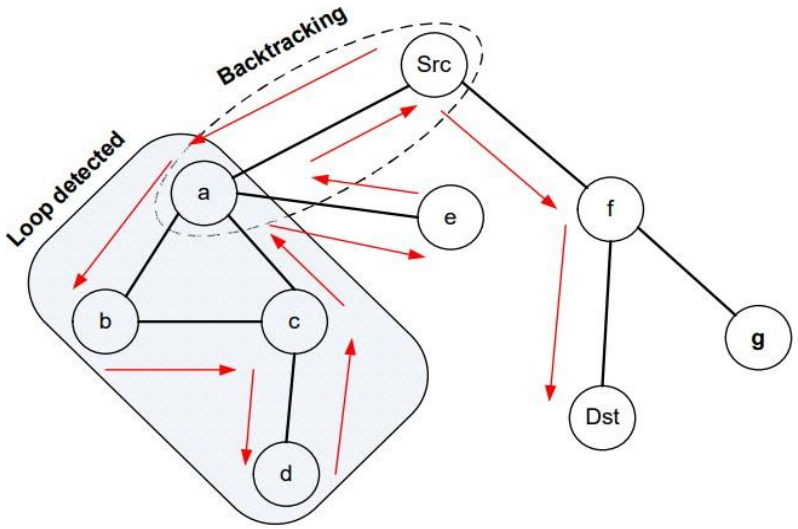


Figure 9 : Mécanisme de backtracking et détection de boucle.

Protocole de routage hybride

Le protocole de routage hybride (Hydro) est un protocole de routage à état de liens pour les réseaux à faible puissance et avec perte. Il utilise un algorithme distribué pour la formation de graphes acycliques dirigés (DAG) qui fournit plusieurs chemins vers un routeur frontalier. Pour fournir une route par défaut fiable à un routeur frontière, chaque nœud construit sa table de routage par défaut en ajoutant ses nœuds voisins vers un routeur frontière. Ensuite, chaque nœud maintiendra des statistiques sur le taux de réussite des paquets de couche liaison des nœuds dans sa table de routage par défaut. Les entrées de la table de routage par défaut sont classées en fonction de cette estimation de liaison basée sur les données.[15]

Basé sur la base de données d'état des liens, le routeur de bordure optimise un routage point à point actif entre les nœuds, puis utilise un message d'installation d'itinéraire pour mettre à jour la table de flux d'un nœud. Ceci Le message d'installation de route se compose de la correspondance de flux et du chemin de flux. La correspondance de flux est le critère utilisé pour déterminer si un paquet donné correspond à une entrée de table de flux alors que le chemin de flux est complet chemin d'accès à un nœud de destination. Ainsi, chaque nœud prend l'ordre d'actions suivant pour transférer un paquet vers une destination. Tout d'abord, il utilise le routage source si le paquet a des informations de routage source dans son en-tête et transfère le paquet au nœud suivant dans la séquence. Ensuite, routage source point à point basé sur sa table de flux si la destination se trouve dans la table de flux. Enfin, il utilise la

route par défaut pour transférer le paquet vers un routeur de frontière qu'il utilise le routage triangulaire.

Par exemple, la communication entre le nœud 7 et le nœud 4 de la Fig. 10 utilise le routage triangulaire. Le nœud 7 envoie le message au routeur de bordure en utilisant son itinéraire par défaut, puis le routeur de bordure utilise le routage source pour l'envoyer au nœud 4.

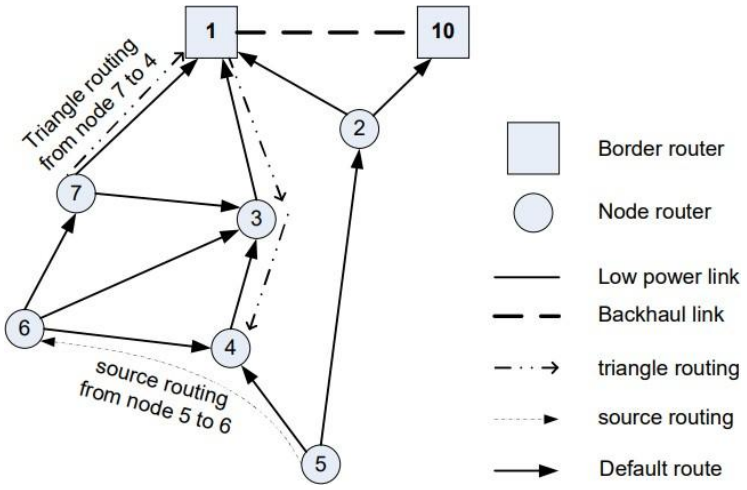


Figure 10 : exemple de routage hybride

Secure routing pour les NAN sans fill

La sécurité doit couvrir tous les aspects de SG, y compris les protocoles de routage et les données transitant par le réseau. Bien que certains articles traitent de la sécurité et de la confidentialité des données pour SG, comme indiqué dans, il n'existe aucun travail spécifique sur la sécurité de routage pour le SG. Cependant, étant donné que la plupart des protocoles de routage proposés pour les NAN sont basés sur WMN, il existe de nombreux travaux pour la sécurité dans WMN qui peuvent convenir à SG avec quelques adaptations. [16]

Ainsi, dans cette sous-section, nous examinerons ces deux catégories séparément. Dans cette section, nous concentrons notre discussion sur les menaces de sécurité sur le routage qui peuvent survenir au niveau des couches réseau et liaison de données. La couche de liaison est également prise en compte car de nombreux protocoles de routage suivent une approche intercouche où les informations de la couche de liaison sont utilisées pour les décisions de routage. Étant donné que les stratégies de routage WMN suivent deux étapes majeures de découverte de route et de maintenance de route, des attaques similaires sur le routage MANET/WSN peuvent également se produire à différentes phases du routage WMN, comme résumé dans le tableau 2, et celles-ci peuvent provenir d'attaquants internes ou externes. Étant donné que la plupart des protocoles de routage proposés pour les NAN

discutés dans le document sont basés sur HWMP de la norme IEEE 802.11s, nous discutons spécifiquement des attaques de sécurité et du routage sécurisé sous HWMP.

Phase de routage	Attaque de sécurité
Découverte d'itinéraire	Attaque par débordement de la table de routage, Positionnement du cache de routage, attaque inondation Boucle de routage, Routage modification des messages.
Entretien des itinéraires	broadcasting false control message
Attaques avancées/sophistiquées	Attaque de trou de ver, attaque de trou noir gouffre, attaque byzantine, attaque précipitée, La consommation de ressources attaque, emplacement PHEV attaque de divulgation.

Tableau 2 : Résumée des Attaques sur les phases routages

Qos routing

L'approvisionnement QooS dans WMN a commencé à recevoir l'attention de la communauté des chercheurs récemment et initialement certains travaux ont été effectués avec l'hypothèse d'un seul canal. Les extensions QoS de base vers 802.11 ont également été développées sous802.11e au moyen de Hybrid Controlled Channel Access et EDCA (Enhanced Distributed Channel Access), mais uniquement destiné à la couche MAC. Un framework pour fournir IEEE 802.11e [17]

Basé sur différents types de données critiques dans le temps peuvent être hiérarchisés différemment en fonction des applications. Par conséquent, la hiérarchisation basée sur les applications et les flux peut mieux répondre aux exigences de SG, tout comme IntServ. À cette fin, il ne suffira pas de proposer des approches de routage QoS côté HAN, NAN ou WAN. Une compréhension globale de la QoS des passerelles au niveau des différents composants du réseau peut être nécessaire. La mise en œuvre de la hiérarchisation des messages doit être basée sur le nombre de 23 niveaux de priorité, l'allocation des ressources à chaque niveau, le mappage de priorité à chaque classe de communication, la transition de priorité entre les différents réseaux, les critères de contrôle d'admission en cas de congestion dans le réseau et les dynamiques d'ajustements de contrôle.

IV Comparaison finale entre les protocoles

Routing Protocol	*Reliable*	*Secure*	*QoS*	*Point-to-point routing*	*One-to-many routing*	*Many-to-one routing*	*Multi-path*	*Low Latency*	*Scalable*	*Energy Efficient*	*Load Balancing*	*Application*
DADR	✓				✓	✓	✓		✓			wireless AMI
Hydro	✓			✓	✓	✓	✓		✓		✓	wireless AMI
Timer based multipath diversity routing	✓				✓	✓	✓				✓	wireless AMI
Jung et al.	✓			✓		✓	✓					wireless AMI, status management and monitoring
Wang et al.	✓				✓	✓		✓	✓			wireless AMI
Li et al.		✓			✓	✓			✓			wireless AMI
Bartoli et al.	✓	✓				✓				✓		wireless AMI
Li et al.			✓	✓					✓			DR
PMR	✓				✓		✓					AMI-PLC

Figure 11 : comparaison entre les différents protocoles de routage

V Conclusion

Il existe un intérêt croissant pour le développement de protocoles de routage pour satisfaire les exigences des applications SG. Cependant, le développement de protocoles de routage pour SG est encore à ses balbutiements étant donné qu'il reste encore beaucoup de défis à relever. Dans cet article, nous avons résumé et classé ces protocoles de routage sous trois composants de réseau SG, à savoir les HAN, les NAN et les WAN. Pour les deux premiers, nous avons présenté une classification de routage en utilisant le support de communication sous-jacent et plusieurs mesures clés telles que la fiabilité, la sécurité et la qualité de service. Nous avons également identifié les avantages et les inconvénients de ces protocoles pour souligner la nécessité de poursuivre les recherches. De plus, nous avons décrit et discuté plusieurs problèmes majeurs liés au routage, tels que la qualité de service, la sécurité, les tests et la multidiffusion qui doivent être résolus dans les futurs protocoles de routage.

Page référence

[1]: A. Ghassemi, S. Bavarian, L. Lampe, Cognitive radio for smart grid communications, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 297 –302

[2] : V. Aravinthan, V. Namboodiri, S. Sunku, W. Jewell, Wireless ami application and security for controlled home area networks, in: Power and Energy Society General Meeting, 2011 IEEE, pp. 1 –8 [4]: Daniels, W.Salter, "WHAT IS SCADA?" International Conference on Accelerator and Large Experimental Physics Control Systems, 1999, Italy, pp. 5.

[3]: C. Gomez, J. Paradells, Wireless home automation networks: A survey of architectures and technologies, Communications Magazine, IEEE 48 (2010) 92 –101.

[4]: D. of Energy, Communications requirements of smart grid technologies, 2010.

[5]: *https://en.wikipedia.org/wiki/Communication_protocol*

[6]: *Marsden 1986, Chapter 3 - Fundamental protocol concepts and problem areas, p. 26-42, explains much of the following.*

[7]: *Comer 2000, Sect. 7.7.4 - Datagram Size, Network MTU, and Fragmentation, p. 104, Explains fragmentation and the effect on the header of the fragments.*

[8]: *Marsden 1986, Section 3.7 - Flow control, p. 36-38.*

[9]: *D. Dzung, I. Berganza, A. Sendin, Evolution of powerline communications for smart distribution: From ripple control to ofdm, in: Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on, pp. 474 –478*

[10]: *B. Akyol, H. Kirkham, S. Clements, M. Hadley, A survey of wireless communications for the electric power system, Prepared for the U.S. Department of Energy, 2010.*

[11]: *T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, K. Struik, J. Vasseur, Rpl: Ipv6 routing protocol for low power and lossy networks, 2011.*

[12]: *ang, Y. Xu, M. Gidlund, Coexistence of ieee802.15.4 based networks: A survey, in: IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society, pp. 2107 –2113.*

[13] :*G. Mikhail, Catching the z-wave, Electronic Engineering Times India (2006) 1–5.*

[14] J.-S. Jung, K.-W. Lim, J.-B. Kim, Y.-B. Ko, Y. Kim, S.-Y. Lee, Improving ieee 802.11s wireless mesh networks for reliable routing in the smart grid infrastructure, in: Communications Workshops (ICC), 2011 IEEE International Conference on, pp. 1 –5.

[15] P. Darbee, Insteon:the details (2005)

[16] F. Li, B. Luo, P. Liu, Secure information aggregation for smart grids using homomorphic encryption, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 327 – 332.

[17] *H. Jiang, W. Zhuang, X. Shen, A. Abdrabou, P. Wang, Differentiated services for wireless mesh backbone, Communications Magazine, IEEE 44 (2006) 113 – 119.* [18] *"FOUNDATION Specification System Architecture" (FF 581) Revision FS 1.1, The Fieldbus Foundation, 2000.*

Résume

Avec les récentes initiatives visant à mettre à niveau le réseau électrique existant vers le Smart Grid (SG), il y a eu un intérêt significatif pour la conception et le développement d'une infrastructure de communication efficace pour connecter les différents composants du SG. En plus des réseaux et protocoles sous-jacents actuellement utilisés, de nouvelles approches câblées/sans fil sont en cours de déploiement pour différents composants/applications du SG.

Mots-clés : Réseau intelligent, Réseau de communication, Routage, HANs, NANs, WANs

Abstract

With the recent initiatives to upgrade the existing power grid to the Smart Grid (SG), there has been a significant interest in the design and development of an efficient communications infrastructure for connecting different components of the SG. In addition to the currently used underlying networks and protocols, new wired/wireless approaches are being planned for deployment for different components/applications of the SG.

Keywords: Smart Grid, Communications Network, Routing, HANs, NANs, WANs

ملخص

مع المبادرات الأخيرة لترقية شبكة الطاقة الحالية إلى الشبكة الذكية كان هناك اهتمام كبير بتصميم وتطوير بنية تحتية لاتصالات فعالة لربط المكونات المختلفة للشبكة الذكية. بالإضافة إلى الشبكات والبروتوكولات الأساسية المستخدمة حاليا في التخطيط لنهج السلكية و اللاسلكية جديدة المتوقع نشرها لتطبيقات مختلفة من الشبكة الذكية

كلمات مفتاحية :الشبكة الذكية,شبكة الاتصالات,التوجيهHANs, NANs, WANs