

NB-IOT

Narrowband IoT



Realisé par:

- **EL AGAL EL Aydi**
- **OUSTOUH Moussa**

Encadré par:

- **Mr. ERROUTBI Amine**

Table des matières

Table des matières.....	1
Liste des figures	3
Liste des tableaux.....	3
Introduction	4
Qu'est-ce que NB-IoT ?	5
Architecture NB-IoT	6
NB-IoT et Mobilité.....	7
NB-IoT: pile de protocoles	10
Couche physique	10
i. Acquisition et synchronisation de cellules	11
ii. Procédure d'accès aléatoire	12
iii. Estimation de canal et correction d'erreur	12
iv. Interférence dans le même canal	13
Couche de contrôle d'accès aux médias	13
v. Allocation de ressources radio	13
vi. Adaptation des liens	14
vii. Couverture et capacité	14
viii. Gestion de l'énergie et de l'énergie	14
Couches supérieures.....	14
ix. Contrôle et optimisation du plan utilisateur	14
Synthèse:.....	16
Caractéristiques NB-IoT	17
Echange d'un grand volume de données	17
Une latence élevée	17
Utilisation des réseaux mobiles existants.....	18
Les modes de déploiement de NB-IoT	18
Exigences de sécurité de NB-IoT	19
A. Couche de perception.....	20
B. Couche de transmission	21

x. Accès aux terminaux NB-IoT haute capacité.....	21
xi. Environnement réseau ouvert.....	21
C. La couche d'application	22
xii. Identification et traitement de données hétérogènes massives	22
xiii. Intégrité et authentification des données.....	22
xiv. Contrôle d'accès aux données.....	23
NB-IoT et 5G.....	23
Comparaison entre LTE-M et NB-IOT.....	26
Le débit	26
La latence ou temps de réponse.....	26
Support de la mobilité	27
Transfert de données.....	27
NB-IoT et La sécurité.....	28
Méthodes de gestion de la sécurité dans NB-IoT.....	29
Authentification mutuelle.....	29
Les avantages de NB-IoT	30
La faible consommation.....	30
La fiabilité.....	30
Diminution des coûts	30
Une couverture plus adaptée	30
Les inconvénients du protocole Nb-IoT	31
Application.....	31
Implémentation	33
Envoi de données de localisation GPS via GSM à l'aide de Proteus.....	33
Le teste.....	39
Conclusion.....	40
Webographie	41

Liste des figures

FIGURE 1: IOT CONNECTED DEVICES INSTALLED BASE WORLDWIDE 2015-2025	5
FIGURE 2.NB-IOT ARCHITECTURE	6
FIGURE 3.ARCHITECTURE DE RÉSEAU VERS L'INTERFACE AÉRIENNE	7
FIGURE 4.. END-DEVICE ETAT DANS NB-IOT	7
FIGURE 5.CONFIGURATION DE LA CONNEXION	8
FIGURE 6.PROCESSUS DE REPRISE DE CONNEXION	9
FIGURE 7. STRUCTURE DE TRAME DE LIAISON DESCENDANTE NB-IOT	10
FIGURE 8 STRUCTURE DE TRAME DE LIAISON MONTANTE NB-IOT	11
FIGURE 9 REPRÉSENTATION DU CHEMIN DE DONNÉES IP ET NON IP NB-IOT	15
FIGURE 10:PILE DE NB-IOT	16
FIGURE 11:OPERATION MODES OF NB-IOT	17
FIGURE 12:MODES DE DEPLOIEMENT DE NB-IOT	19
FIGURE 13:LA SIMILITUDE ENTRE NB-IOT ET IOT TRADITIONNEL EN TERMES D'EXIGENCES DE SÉCURITÉ.	20
FIGURE 14:COMPARAISON ENTRE LES DIFFERENT LPWA STANDARDS	24
FIGURE 17: LA BIBLIOTHÈQUE ARDUINO	34
FIGURE 15: LA BIBLIOTHÈQUE GSM	34
FIGURE 16: LA BIBLIOTHÈQUE GPS	34
FIGURE 18: SCHÉMA DE LA SIMULATION	34
FIGURE 19:AJOUTER LE FICHIER HEX	35
FIGURE 20:INITIALISATION DE CODE ET SETUP FONCTION	36
FIGURE 21:LOOP FONCTION	37
FIGURE 22:SUITE DE CODE (LOOP FONCTION)	38
FIGURE 23: AJOUTER LE FICHIER .HEX AU SIM	38
FIGURE 24:TEST DE FONCTIONNEMENT DE PROJET	39

Liste des tableaux

TABLE 1: CANAUX ET SIGNAUX	6
TABLE 2.COMPARAISON DE SIGNALISATION ENTRE DIFFÉRENTES MÉTHODES	9

Introduction

Au cours des 20 dernières années, les technologies IoT se sont considérablement développées et ont été intégrées dans divers domaines. À savoir, presque tout peut être connecté via le réseau IoT. L'IoT a considérablement amélioré le traitement des méga données, l'hétérogénéité et les performances. Du point de vue du débit de transmission, les services de communication de l'IoT peuvent être grossièrement classés en deux catégories: les services à haut débit de données (comme le service vidéo) et les services à faible débit de données (comme le service de lecture des compteurs). Selon les statistiques d'ATECH en 2017, les services à faible débit de données représentent plus de 67% du total des services IoT, ce qui indique que les technologies WAN à faible débit de données sont vraiment souhaitables.

Récemment, en raison du développement de l'IoT, les technologies de communication IoT sont devenues matures et répandues. Du point de vue de la distance de transmission, les technologies de communication IoT peuvent être classées en technologies de communication à courte distance et technologies de communication WAN. Les premiers sont représentés par Zigbee, Wi-Fi, Bluetooth, Z-wave et etc. Leur application typique est la maison intelligente. Ces derniers sont souhaités dans les services à faible débit de données comme le stationnement intelligent mentionné ci-dessus, qui est généralement défini par l'industrie comme la technologie LPWAN (Low-Power Wide-Area Network).

L'Internet des objets à bande étroite (NB-IoT) est une technologie LPWA (Low Power Wide Area Wide) proposée par le 3GPP pour la perception et l'acquisition de données destinées aux applications intelligentes à faible débit de données. Les applications typiques sont le comptage intelligent et la surveillance intelligente de l'environnement. Le NB-IoT prend en charge des connexions massives, une consommation d'énergie ultra-faible, une couverture étendue et un déclenchement bidirectionnel entre le plan de signalisation et le plan de données. En outre, il est soutenu par un excellent réseau de communication cellulaire. Par conséquent, NB-IoT est une technologie prometteuse.

Qu'est-ce que NB-IoT ?

Nb-IoT (NB for narrow band) est une technologie cellulaire de type LPWAN (Low Power Wide Area Network). Protocole IP (Internet Protocol), elle permet aux objets de se connecter à internet en se reliant directement aux antennes-relais des opérateurs, évitant ainsi l'installation de passerelles souvent coûteuses pour le client. Le NB-IoT utilise une bande passante vraiment très étroite (narrow band) de 200kHz, une modulation OFDM pour les communications entrantes et SC-FDMA pour les communications sortantes. Du fait de cette bande passante étroite, les débits théoriques envisageables sur ce réseau sont faibles et de l'ordre de 20 à 250 kbit/s en half duplex (émission et réception possibles, mais pas en même temps).

“Le Nb-IoT sera vraiment dédié sur des applications : capteurs, metering – sur des objets fixes. Ce protocole de communication est bas débit, low power et s'appuie sur un réseau d'antennes 4G déjà déployées. Aujourd'hui SIMCom concentre ses développements sur les nouvelles technologies LTE-A/NB-IoT – Cat M et 5G proposant différentes variantes de modules cellulaires basées essentiellement sur des chipset Qualcomm. Nous proposons des modules compacts allant de 24×24, 17×15 ou encore 14×12, intégrant multi technologies Cat M-NB-IoT- Fallback 2G et GNSS, ou encore CatM +Nb-IoT, ou Nb-IoT only (Release 14/NB2) » Magali Ferez (SIMCom).

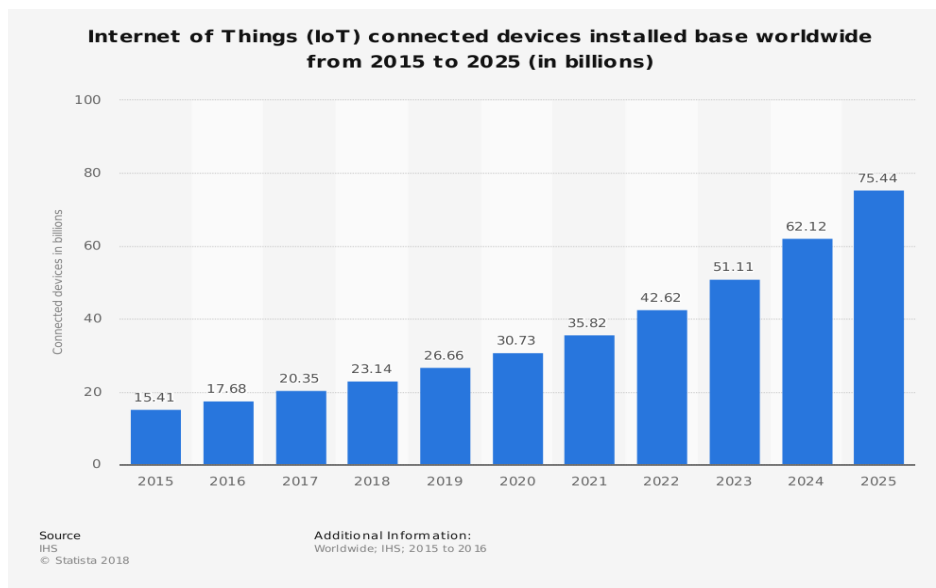


Figure 1: IoT connected devices installed base worldwide 2015-2025

Avec l'avènement de l'IoT, les problématiques liées à l'industrie 4.0 et la prédiction des experts d'avoir plus de 75 Milliards d'objets connectés à l'aide d'un réseau sans fil d'ici 2025, il est nécessaire de créer des technologies adaptées à ces nouveaux besoins. Ce standard permet aux objets connectés de communiquer de gros volumes de données sur de très grandes distances avec une latence très élevée.

Architecture NB-IoT

NB-IoT utilise la même architecture de réseau que dans le réseau LTE mais avec quelques optimisations pour répondre aux besoins des utilisateurs IoT massifs. L'architecture NB-IoT est basée sur l'Evolved Packet System (EPS), comme illustré à la figure 2.

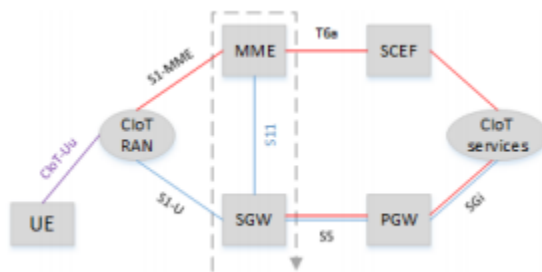


Figure 2. NB-IoT Architecture

	Channel	Usage
UL	Narrowband Physical Uplink Shared Channel (NPUSCH)	Uplink dedicated data
	Narrowband Physical Random Access Channel (NPRACH)	Random access
DL	Narrowband Physical Downlink Control Channel (NPDCCH)	Uplink and downlink scheduling information
	Narrowband Physical Downlink Shared Channel (NPDSCH)	Downlink dedicated and common data
	Narrowband Physical Broadcast Channel (NPBCH)	Master information for system access
	Narrowband Synchronization Signal (NPSS/NSSS)	Time and frequency synchronization

Table 1: CANAUX ET SIGNAUX

Un nouveau nœud a été ajouté à l'architecture, appelé *Service Capability Exposure Function* (SCEF), qui est conçu pour les données de type machine. Deux optimisations sont définies pour Clot dans EPS: l'optimisation Clot EPS du plan de contrôle (lignes rouges) et l'optimisation Clot EPS du plan utilisateur (ligne bleue). Les deux optimisations peuvent être utilisées pour envoyer des données à l'application correspondante. Sur le plan utilisateur, la ligne bleue, les données IP et non IP sont transférées de la même manière que pour le trafic de données conventionnel, c'est-à-dire sur des supports radio via la Serving Gateway (SGW) et la Packet Data Network Gateway (PGW) vers atteindre le serveur d'applications. Avec le plan de commande, les lignes rouges, les communications radio entre l'équipement utilisateur (terminal) et MME sont gérées par le réseau d'accès radio terrestre UMTS évolué (E-UTRAN), qui se compose des stations basées évoluées appelées eNodeB ou eNB (passerelle). Ensuite, les données de liaison montante sont transmises au SGW qui les transmet au PGW. Les données non IP seront envoyées à l'aide de SCEF, qui est le nouveau nœud chargé de fournir les données non IP sur le plan de contrôle et de fournir une interface pour les services réseau (authentification et autorisation, capacités de découverte et d'accès au réseau).

Dans l'architecture du réseau d'accès. Le GW est connecté au MME et au S-GW à l'aide de l'interface S1 comme le montre la figure 3. Les GW sont connectés avec l'interface X2 bien qu'il n'y ait pas de transfert, cette interface permet une connexion rapide qui reprend lorsque ED passe d'IDLE STATE à RCC CONNEXION.

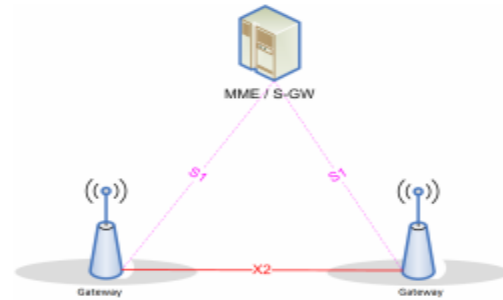


Figure 3. Architecture de réseau vers l'interface aérienne

NB-IoT et Mobilité

La gestion de la mobilité dans les réseaux IP consiste à fournir une connectivité transparente pendant le transfert IP (transfert doux ou dur), tandis que la mobilité dans l'IoT se réfère à assurer la livraison d'informations à la demande et pendant le mouvement.

Dans NB-IoT, un ED se connecte à un seul GW pour communiquer avec, c'est-à-dire que chaque ED est associé à un GateWay. Pendant le mouvement, cet ED peut changer son emplacement plusieurs fois et, chaque fois que la connexion est perdue, il recherchera un GW approprié pour se connecter. Lorsque ED dispose de données à transmettre (liaison montante), il recherche une cellule sur une fréquence appropriée, lit les informations SIB et démarre la procédure d'accès aléatoire.

1) Accès aux cellules: cette étape est répétée chaque fois qu'un ED perd la connexion avec le GW. Dans NB-IoT, un ED a deux états comme indiqué sur la figure 4, RRC IDLE (état de veille) et RRC CONNECTED (état de connexion). Le transfert a été supprimé car cette norme a été conçue pour être simple en réduisant la complexité des fonctions LTE. La communication est considérée comme courte, avec des messages peu fréquents entre l'ED et le GW, et un GW peut servir cela. L'ED recherche un GW sur une fréquence appropriée. Ensuite, la configuration de la connexion commence comme indiqué sur la figure 5. Pendant la configuration de la connexion, l'ED obtient d'abord l'ID de cellule physique à bande étroite (NCellID) du canal NSSS diffusé par le GW. Deuxièmement, l'ED decode NCellID pour obtenir le NB-MIB, qui comprend la taille SIB1-NB, le nombre de répétitions, la planification foSIB1 (accès et sélection de cellule) et sa position de départ. Troisièmement, l'ED decode SIB1-NB pour

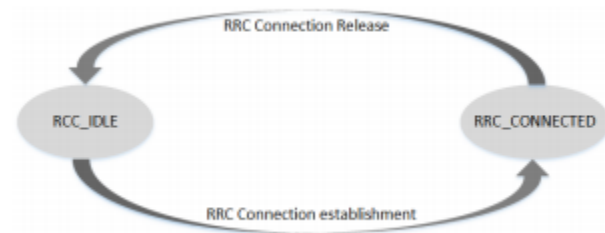


Figure 4.. End-device etat dans NB-IoT

obtenir les informations sur les paramètres d'accès aux cellules: PLMNID, code TA, identité et état des cellules et informations sur la sélection des cellules comme le niveau minimum du récepteur. Quatrièmement, l'ED decode NB-SIB2, qui lui fournit les informations de configuration sur les canaux logiques et physiques courants. La plupart des informations dans SIB2 sont la configuration du canal d'accès aléatoire (RACH) qui est requise pour la synchronisation de liaison montante. À ce niveau, l'ED initialise et envoie le préambule RACH au GW. Lorsque le GW reçoit la demande, il répondra avec Msg2. Si le GW ne reçoit pas la demande, l'ED ne recevra pas de réponse pour renvoyer la demande. Ensuite, l'ED envoie Msg3 pour démarrer le processus de résolution de contenu et le GW envoie la réponse dans Msg4 qui indique la réussite de la procédure RACH. Enfin, RRCConnectionRequest suggère que l'ED souhaite se connecter au réseau.

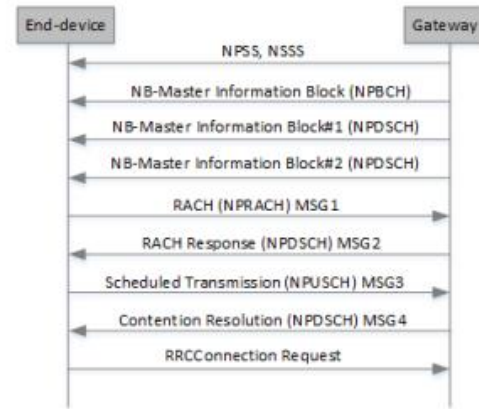


Figure 5. Configuration de la connexion

2) Mobilité: ED peut perdre la connexion en s'éloignant du GW. ED passe donc à l'état RRC IDLE pour ré-sélectionner un autre GW. Le temps de configuration est inférieur à 10 s.

les résultats montrent que le temps de configuration est de 6,6 s lorsque NB-IoT est déployé de manière autonome, et d'environ 9,882 s lorsqu'il est déployé en bande avec LTE et en supposant les mêmes résultats s'il est déployé en bande de garde. Lorsque le GW libère la connexion, il envoie à l'ED les contextes actuels de la strate d'accès (AS) pour les stocker.

Ces contextes AS seront utilisés ultérieurement par l'ED pour reprendre la connexion (plus rapidement que la configuration de cellule), comme illustré à la figure 6.

Le tableau 2 compare le nombre de messages utilisés parmi les trois méthodes disponibles dans NB-IoT: demande de service héritée, suspension / reprise de connexion RRC et transmission de données via le plan de contrôle. Dans la reprise du processus, il y a deux cas:

- La passerelle accepte la reprise: revient à la connexion. Le coût est de cinq messages.
- La passerelle rejette la reprise: ED libère le contexte AS stocké, revient à l'état IDLE, puis répétera la configuration de la connexion.

Le coût est de neuf messages.

En liaison montante, quand un ED se réveille, la connexion reprendra si elle a été établie. Sinon, l'ED recherchera un GW pour se connecter. Une fois la connexion établie, l'ED peut transmettre des données.

En liaison descendante, le GW utilise une méthode de radiomessagerie pour déclencher une connexion RRC qui indique une modification des informations système pour ED en mode RRC IDLE. Il est utilisé pour la configuration de la connexion ou la modification des informations système. Même si l'ED dans les états RCC IDLE est considéré comme dormant, il surveille toujours certaines des sous-trames (SF) qui sont liées à la pagination.

Dans la norme NB-IoT, ED peut se déplacer entre différents GW NBloT similaires à un téléphone mobile. Même si aucun transfert identique au transfert de système cellulaire n'est pris en charge, mais la mobilité peut toujours être réalisée sur l'interface X2 entre deux GW comme mentionné précédemment. Lorsque le GW actuel envoie les informations de reprise de connexion au nouveau GW, ED peut reprendre la connexion avec le GW d'origine. Cette méthode fournit à ED une connexion rapide.

Direction	Legacy Service Request	RRC Connection Resume	Control Plane Data Transmission
UL	Preamble		
DL	Random Access Response		
UL	RRC Connection Request	RRC Connection Resume Request	RRC Connection Request
DL	RRC Connection Setup	RRC Connection Resume	RRC Connection Setup
UL	RRC Connection Setup Complete	RRC Connection Resume Complete	RRC Connection Setup Complete
DL	Security Mode Command	-	-
UL	Security Mode Complete	-	-
DL	RRC Connection Reconfiguration	-	-
UL	RRC Connection Reconfiguration Complete	-	-

Table 2.COMPARAISON DE SIGNALISATION ENTRE DIFFÉRENTES MÉTHODES

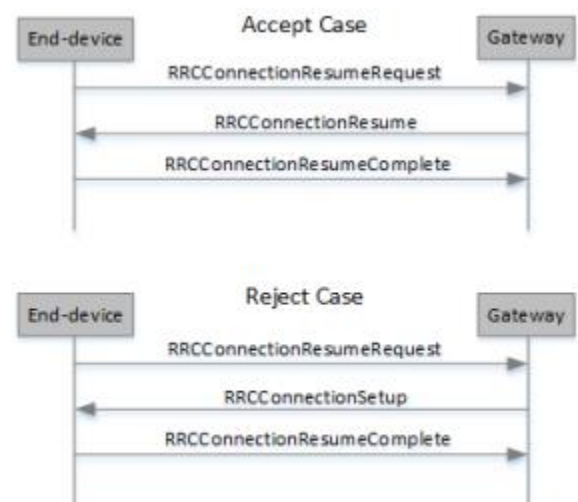


Figure 6.Processus de reprise de connexion

NB-IoT: pile de protocoles

Cette section présente la pile de protocoles NB-IoT basée sur l'état de l'art des couches PHY et MAC pour identifier le manque de connaissances et définir les futures orientations de recherche. NB-IoT adopte la même pile de protocoles que l'héritage LTE. Cependant, certains changements de conception dans les couches PHY et MAC ont été introduits pour prendre en charge les connexions massives à longue portée avec jusqu'à 20 dB MCL supplémentaires par rapport aux technologies héritées telles que LTE, GSM et GPRS. Ces changements sont décrits dans ce qui suit.

Couche physique

Sur la couche physique, NB-IoT adopte les mêmes numérolgies que le LTE hérité avec les formes d'onde de signal OFDM et SC-FDMA respectivement en liaison descendante et en liaison montante. Cependant, l'unité d'ordonnancement des ressources dans NB-IoT est la sous-porteuse (ou tonalité) au lieu de PRB, pour favoriser l'évolutivité du réseau en desservant plusieurs UE dans une bande passante de 180 kHz. Les structures de trame de liaison descendante et montante sont telles que représentées sur les figures 7 et 8, respectivement.

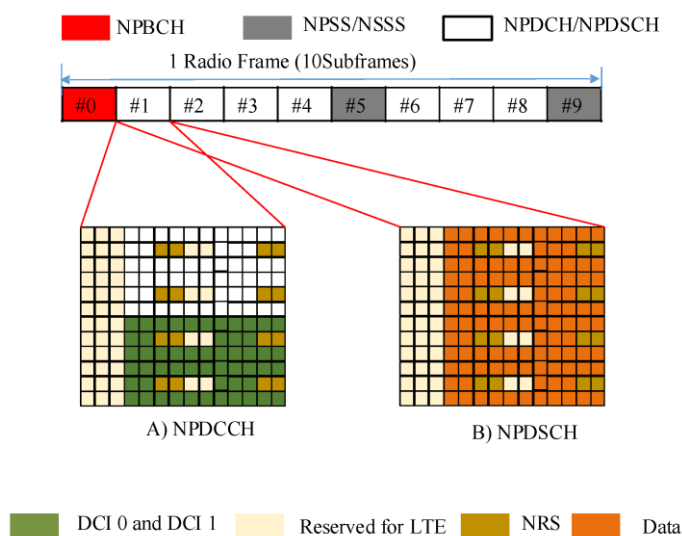


Figure 7. Structure de trame de liaison descendante NB-IoT la sous-trame numéro 0 porte le canal de diffusion physique à bande étroite (NPBCH), 1 à 4 et 6 à 8 portent le canal de commande de liaison descendante physique à bande étroite (NPDCCH) / canal partagé de liaison descendante physique à bande étroite (NPDSCH), et 5 et 9 transportent le signal de synchronisation primaire à bande étroite (NPSS) / signal de synchronisation secondaire à bande étroite (NSSS) (A) lorsque la sous-trame transporte des canaux de commande et (B) lorsque la sous-trame transporte des données.

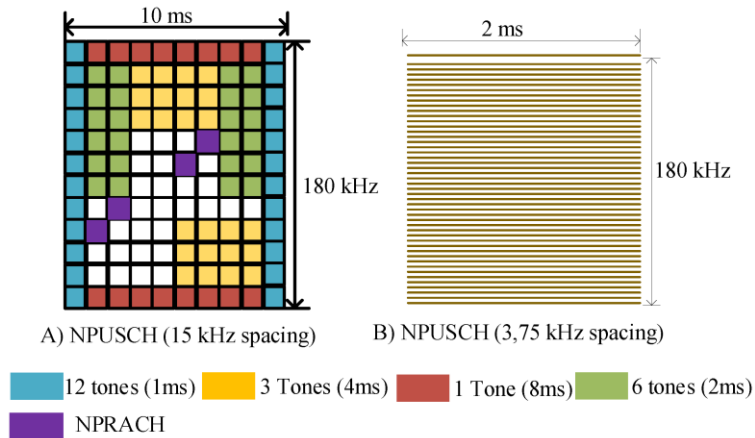


Figure 8 Structure de trame de liaison montante NB-IoT, (A) lorsque l'espacement de 15 kHz est utilisé avec différentes possibilités d'attribution de tonalité avec une durée de créneau de 0,5 ms et (B) lorsque 3,75 kHz est utilisé, seule l'allocation de tonalité unique est prise en charge 4 fois durée d'emplacement plus longue (2 ms).

En général, la station de base utilise DCI pour spécifier les informations de programmation pour une transmission "liaison descendante / liaison montante" dans NB-IoT. NB-IoT UE apprend ensuite le mode de déploiement (autonome, intrabande ou bande de garde) ainsi que l'identité de la cellule grâce à son acquisition initiale, et il détermine quels éléments de ressource sont déjà utilisés par LTE. Il s'agit de la manière dont l'UE peut mapper les symboles NPDCCH et NPDSCH aux éléments de ressource disponibles. Par exemple, dans la liaison descendante, NPDCCH est transmis en agrégeant les éléments de commande à bande étroite (élément 0 et élément 1) où l'élément 0 est occupé dans la sous-porteuse 0 à 5 et l'élément 1 occupe la sous-porteuse 6 à 11 dans une sous-trame. Les éléments sont déterminés par le type de DCI qui est transporté par NPDCCH pour fournir la commande de planification. Soit deux DCI peuvent être multiplexés dans une sous-trame, soit un DCI peut être mappé dans une sous-trame, correspondant au niveau d'agrégation utilisé. Cependant, NPDCCH, NPDSCH et NRS ne peuvent pas être mappés aux éléments de ressource déjà occupés pour les signaux LTE tels que les symboles de référence spécifiques aux cellules (CRS) et le canal de commande de liaison descendante physique LTE (PDCCH). Lorsque NB-IoT UE reçoit NPDCCH qui transporte DCI, il le décode et utilise la fonction de programmation du périphérique (k0) pour connaître le délai pendant lequel il commencera à recevoir NPDSCH. Les informations de planification sont utilisées pour identifier les ressources allouées sur NPDSCH et NPUSCH, respectivement. Dans chaque NPDCCH, un maximum de deux DCI peut être transporté, et chaque UE peut recevoir jusqu'à un DCI. L'intervalle de temps entre deux opportunités NPDCCH successives est appelé période NPDCCH (PP)

i. Acquisition et synchronisation de cellules

NB-IoT UE passe par le même processus que LTE UE où camper sur une cellule, il passe par la synchronisation de fréquence et de synchronisation pour obtenir la fréquence porteuse centrale ainsi que le créneau alloué et la synchronisation de trame utilisés pour l'acquisition de cellule. En général, si MIB et SIB sont correctement décodés, l'ID de cellule, un numéro de sous-

trame, les informations de planification et la bande passante du système peuvent être détectés avec succès.

Dans NB-IoT, la faible complexité des dispositifs peut entraîner une mauvaise synchronisation et des performances d'acquisition de cellules, en particulier en raison des décalages de fréquence de la porteuse et de la faible capacité d'estimation des canaux.

ii. Procédure d'accès aléatoire

Comme dans le LTE, l'accès aléatoire (RA) NB-IoT est destiné à la synchronisation initiale de liaison montante de l'UE grâce à laquelle l'UE acquiert son ID UE unique utilisé pour la communication avec la station de base. RA est également utilisé pour récupérer l'accès UE perdu en raison du long état d'inactivité qui a conduit à la perte de synchronisation de liaison montante. Dans NB-IoT, l'AR fait face à plusieurs défis comme le montrent les discussions de recherche; quelques solutions pour améliorer les performances RA ont été proposées comme décrit dans ce qui suit.

Certains auteurs ont présenté le modèle de procédure d'accès aléatoire (RAP) et analysé les performances du système en prenant en considération le modèle de propagation de signal configurable, un certain nombre d'utilisateurs pris en charge par cellule et les paramètres de configuration RAP. Le document a utilisé l'accès aléatoire basé sur la contention avec des collisions Msg3 au lieu d'une collision Msg1 (comme transmission par trajets multiples) pour la procédure d'accès aléatoire. Les résultats du modèle proposé montrent l'impact des paramètres (mode de transmission Msg3, schéma de modulation et de codage Msg3 (MCS), schémas de commande de puissance et étape de rampe de puissance) sur les performances du taux d'erreur sur les bits (BER) des transmissions monotone et multi tons. Les résultats sont présentés en termes de nombre total de succès de transmission de préambule, de retransmissions de préambule et de tentatives de préambule perdues.

Ils analysent le délai de transmission NB-IoT ainsi que l'évaluation mathématique de la probabilité de réussite de la transmission du préambule de la procédure d'accès aléatoire. L'analyse est basée sur trois scénarios; le scénario un utilise des valeurs minimales de paramètres, le scénario deux utilise les valeurs intermédiaires et le scénario trois utilise des valeurs de paramètres maximales. Les paramètres utilisés sont la périodicité NPRACH, l'heure de début, le nombre de répétitions, le nombre de tentatives de préambule et la taille de la fenêtre de réponse à accès aléatoire. L'analyse du retard moyen a été effectuée de telle sorte que k séquences de préambule soient cartographiées en sous-porteuses. La collision de préambule se produit lorsque plusieurs UE envoient des séquences de préambule dans la même sous-porteuse. Une tentative de préambule réussie se produit lorsqu'un seul UE envoie le préambule à une sous-porteuse donnée.

iii. Estimation de canal et correction d'erreur

Comme dans les systèmes LTE, les performances du système NB-IoT dépendent dans une certaine mesure de la qualité de l'estimation du canal. Cependant, pour le déploiement massif

des systèmes NB-IoT, la mauvaise qualité des estimations de canal est fortement influencée par la faible complexité des UE qui peut entraîner une mauvaise détection de certains signaux, un décalage de fréquence, un bruit de phase, une intermodulation passive (PIM) au niveau de l'appareil, etc. Pour relever les défis qui affectent l'estimation du canal ainsi que pour améliorer la qualité de la correction des erreurs afin d'assurer les performances requises avec une faible complexité, plusieurs travaux ont proposé des solutions, comme résumé dans les paragraphes suivants.

Les auteurs ont présenté une méthode de détection NPSS dont la métrique de synchronisation est composée d'une autocorrélation par symboles et d'un facteur de normalisation dédié dans un système NB-IoT en liaison descendante en bande. Les auteurs ont proposé un nouvel algorithme de faible puissance pour le suivi des fréquences en utilisant plus de signaux pilotes par rapport au système LTE. Leur algorithme est implémenté pour compenser le décalage de fréquence accumulé lors de la transmission NB-IoT de NB-IoT. Leur algorithme de suivi de fréquence proposé offre une efficacité d'estimation élevée en termes d'erreur quadratique moyenne minimale (MMSE), de probabilité d'acquisition correcte des cellules, etc. Cependant, leur étude n'a pas précisé quel pourrait être l'impact de la mobilité et du support inter-RAT dans la procédure de recherche de cellules pour NB-IoT.

Il est montré que la solution proposée (où la station de base décide si le retard d'aller-retour compensé est court ou assez long pour décoder la séquence de préambule) a été faite en considérant la conception NPRACH et donc les auteurs ont proposé leur solution qui considère l'ajustement TA. La solution proposée a prouvé que la couverture NB-IoT pouvait atteindre jusqu'à 35 km. Cependant, le document n'élabore pas sur la faisabilité de la solution dans des environnements sans ligne de vue.

iv. Interférence dans le même canal

NB-IoT étant déployé dans le spectre LTE existant, des interférences dans le même canal peuvent se produire entre NB-IoT et UE LTE. Cela est dû à plusieurs raisons telles que l'inadéquation du taux d'échantillonnage, les interférences inter-PRB dues à une fuite de puissance entre NB-IoT et LTE PRB, etc.

Couche de contrôle d'accès aux médias

Le traitement des retransmissions (HARQ), le multiplexage, l'accès aléatoire, l'avance temporelle, le choix des formats de bloc de transport, la gestion des priorités et la planification sont les tâches exécutées par la couche MAC. La discussion sur cette partie se concentre sur des fonctionnalités telles que la gestion des ressources radio, l'adaptation des liaisons, la couverture et l'amélioration de la capacité, la réduction de la consommation d'énergie et d'énergie.

v. Allocation de ressources radio

Dans NB-IoT, l'allocation des ressources est la caractéristique clé pour garantir les connexions massives attendues dans une cellule. Les allocations de tonalité, les PRB, les options de

numéros de répétition, les configurations d'alimentation, les sous-trames ou les intervalles de temps, etc. doivent être optimisés pour maximiser les performances avec un minimum de ressources possibles. Étant donné que NB-IoT est destiné à des applications peu sensibles au temps et à faible débit mais avec les mesures de performances requises, une meilleure gestion des ressources radio garantira l'utilisation optimale des ressources pour le débit attendu, l'efficacité spectrale et l'amélioration de la couverture.

vi. Adaptation des liens

Comme dans le LTE, l'adaptation de liaison NB-IoT implique des schémas de modulation et de codage adaptatifs ainsi qu'une allocation de puissance adaptative. Cependant, les schémas de modulation sont limités à QPSK pour permettre une faible complexité et donc réduire la consommation d'énergie globale. Pour étendre la couverture et augmenter la fiabilité de la liaison, un nombre de répétition pouvant aller jusqu'à 128 fois est introduit.

vii. Couverture et capacité

La prise en charge NB-IoT pour une couverture étendue jusqu'à 164 dB de perte de couplage maximale vise à permettre l'utilisation de la technologie pour les services IoT cellulaires, en particulier pour les applications situées dans des zones difficiles d'accès. Sa bande passante étroite et sa prise en charge de la répétition sont les caractéristiques clés pour permettre une couverture améliorée.

viii. Gestion de l'énergie et de l'énergie

La complexité réduite NB-IoT est destinée à réduire la consommation d'énergie dans différents modes. PSM et eDRX sont les fonctionnalités implémentées dédiées à prolonger la durée de vie de la batterie.

Couches supérieures

Bien que cet article se concentre principalement sur les fonctionnalités concernant les couches PHY et MAC, il est toujours impératif de répondre à certaines améliorations, défis et solutions potentielles aux couches supérieures. Surtout les changements qui sont implémentés dans Evolved Packet Core (EPC) en ajoutant la fonction de capacité d'exposition au service (SCEF) pour gérer les paquets de données IP et non IP.

ix. Contrôle et optimisation du plan utilisateur

Pour prendre en charge une connectivité massive de bout en bout avec une complexité extrêmement faible et réduire la signalisation de transmission, NB-IoT implémente de nouvelles procédures de transmission de petites données basées sur le système évolué de paquets IoT (CIoT) sur le plan de contrôle (CP) et le plan utilisateur (UP). Ces procédures de transmission prennent en charge efficacement les petites rafales de données tout en garantissant la couverture à longue portée par rapport au GPRS hérité. À cet égard, NB-IoT peut prendre en charge plus d'un chemin de données dans le CP pour la transmission de données d'utilisateur qui sont portées par les messages de signalisation gérés par l'entité de mobilité mobile (MME),

comme illustré à la figure 9 . Les procédures sont optimisées pour prendre en charge efficacement le petit transfert de données comme suit:

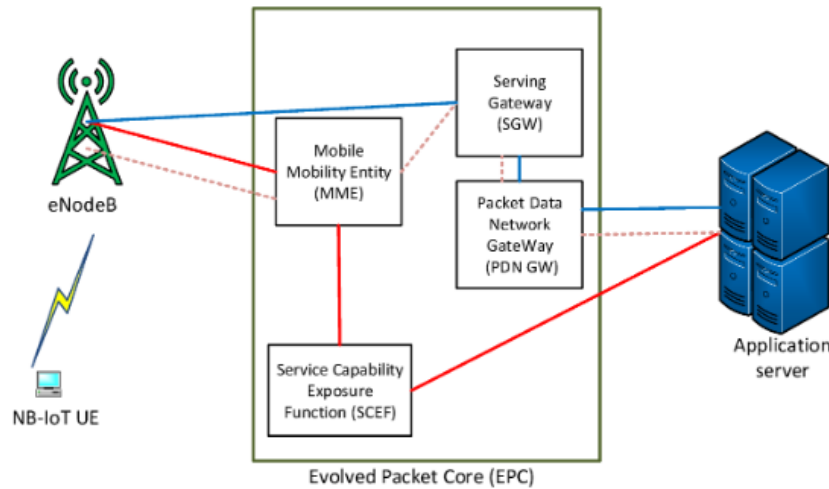


Figure 9 Représentation du chemin de données IP et non IP NB-IoT

Le figure 9 représentation du chemin de données IP et non IP NB-IoT où la ligne bleue affiche le chemin de données IP en mode UP (comme Legacy LTE), la ligne rouge affiche le chemin de données non IP en mode CP et les affichages en pointillés le chemin de données IP en mode CP.

- EPS CP CIoT obligatoire;
- UP CIoT EPS en option.

L'optimisation CP CIoT EPS encapsule les paquets de données dans la strate de non-accès (NAS) en utilisant des messages de signalisation du plan de contrôle. À cet égard, cette procédure est obligatoire. Par rapport à la procédure SR conventionnelle, le NB-IoT UE ignore certaines étapes requises pour chaque transfert de données, c'est pourquoi cette procédure d'optimisation s'adapte le mieux à la courte transmission ou réception de données.

D'un autre côté, l'optimisation UP CIoT EPS nécessite le mode connecté RRC pour obtenir les ressources radio programmées ainsi que la couche d'accès (AS) entre l'UE et le réseau. Ce mode utilise la connexion nouvellement introduite pour suspendre et reprendre les procédures. La procédure de suspension de la connexion permet de conserver le contexte du réseau afin que l'UE puisse reprendre la connexion lorsque le trafic est disponible. La conservation du contexte aide l'UE et le réseau à ignorer la reconfiguration AS et RRC dans chaque transfert de données. Puisqu'il utilise un plan utilisateur, le UP CIoT EPS convient aux petites et grandes transactions.

En outre, l'UE dans la procédure de demande de service (une procédure LTE utilisée par l'UE et la station de base pour transmettre ou recevoir des données à l'état inactif RRC) doit être dans un état connecté pour que la station de base alloue les ressources radio. Pour NB-IoT, ce SR est facultatif; cependant, NB-IoT UE qui prend en charge l'optimisation UP doit également prendre

en charge SR. Par exemple; si l'UE NB-IoT veut transmettre les données de liaison montante à l'état inactif, il enverra le préambule d'accès aléatoire à travers lequel la station de base et l'UE établiront une connexion RRC et UE sera allouée avec les ressources radio pour le transfert de données. Après une certaine période d'inactivité, la station de base lance la procédure de libération.

De même, pour la réception de données de liaison descendante UE, si l'UE est en mode DRX, l'UE écoute régulièrement la signalisation de liaison descendante et si l'UE remarque le message de radiomessagerie, il exécutera la procédure SR comme décrit dans la transmission de données de liaison montante. De plus, si l'UE est en mode PSM, il sera complètement inaccessible jusqu'à ce qu'il lance la même procédure SR pour l'octroi de la liaison montante ou en utilisant la mise à jour de la zone de suivi (TAU).

Il existe des travaux qui traitent des couches supérieures, où les auteurs ont proposé un schéma efficace de transmission de petites données en utilisant la procédure CP. Le schéma proposé permet aux appareils de transmettre des paquets de données via la procédure d'établissement de connexion RRC lorsque l'appareil est en mode veille. Ce processus réduit la surcharge de signalisation causée par le processus de configuration de la sécurité et le processus de configuration du support radio de données. Cependant, une suggestion pourrait être d'analyser la consommation d'énergie pendant cette petite transmission de données et de comparer son efficacité au moment où les mêmes données sont transmises pendant la procédure UP.

Synthèse:

La pile de protocoles NB-IoT commence par les couches de protocoles utilisées dans les protocoles LTE. Ces couches ont été réduites et optimisées pour répondre aux exigences de NB-IoT.

Ce protocole est construit sur un principe fondamental bien établi et peut être considéré comme une nouvelle technologie d'interface radio. Les piles de protocoles NB-IoT illustrées à la figure 10 sont identiques à celles du LTE mais avec des fonctionnalités optimisées.

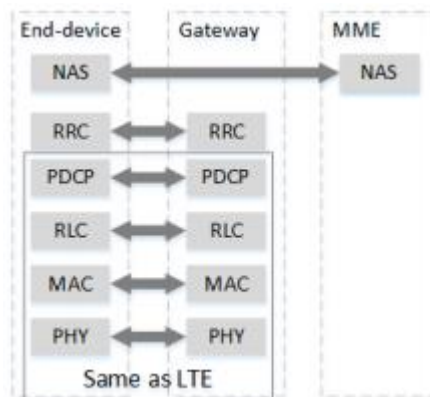


Figure 10:Pile de NB-IoT

Cette section a discuté des caractéristiques de la couche PHY, mettant en évidence les améliorations correspondantes sur la procédure d'acquisition de cellules, l'estimation de canal à accès aléatoire et l'atténuation des interférences. Il a ensuite abordé les améliorations de la couche MAC concernant l'allocation des ressources, l'adaptation des liaisons, la couverture et la capacité, et la gestion de l'alimentation. Il a également abordé les changements des couches supérieures liés à l'optimisation du système de paquets évolué IoT cellulaire via des plans

d'utilisateur et de contrôle pour améliorer les transmissions de petits paquets de données pour une connectivité massive de bout en bout.

Caractéristiques NB-IoT

NB-IoT ou Narrowband IoT ou encore appelé LTE-M2 est une technologie basse consommation et longue portée (LPWAN) validée en Juin 2016 qui peut fonctionner de trois manières différentes:

Sur la bande de fréquence 200 kHz anciennement le réseau GSM

Avec le réseau LTE qui réserve des ressources pour NB-IoT

Au sein d'un réseau indépendant

Le spectre de fréquence GSM de 200kHz est peu utilisé aujourd'hui et laisse donc potentiellement la place, pour ce type de technologie, d'apporter une nouvelle solution LPWAN.

Tout comme LoRa et Sigfox, ce standard permet à des objets basse consommation de communiquer avec des applications externes à travers le réseau cellulaire.

Echange d'un grand volume de données

A la différence de LTE-M, il n'est pas basé sur le protocole IP mais utilise tout de même un protocole basé sur l'échange de message (message based). Il a pour avantage de proposer un taux de modulation plus rapide que LoRa ou Sigfox. Il peut donc échanger une plus grande quantité de données à un rythme moins élevé. LTE-M quant à lui, est plus adapté à des applications qui nécessitent une plus grande bande passante.

Une latence élevée

Techniquement NB-IoT utilise donc la bande de fréquence de 200kHz et la modulation OFDM pour les communications entrantes et SC-FDMA pour les communications sortantes. Par son design, il n'est pas prévu d'avoir des temps de réponse de l'ordre de la milliseconde.

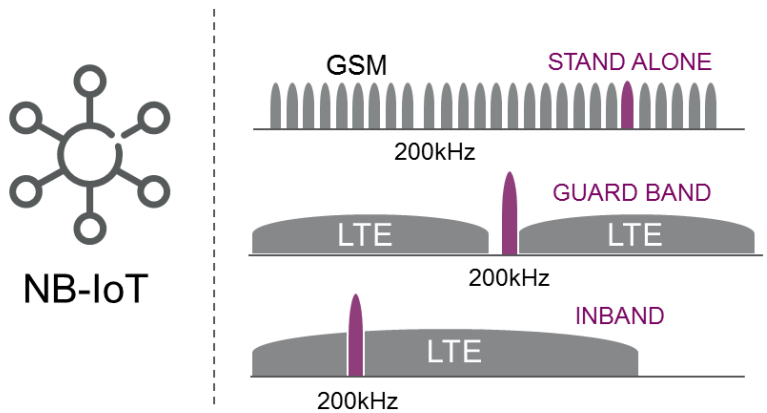


Figure 11: Operation modes of NB-IoT

Il permet d'avoir des débits de 20 à 250Kbit/s en download ou upload avec une latence inférieure à 10 secondes environ. La latence (latency), dépendra de la qualité de la puce de communication, du réseau, de la qualité de réception et de la distance avec l'antenne la plus proche.

Utilisation des réseaux mobiles existants

NB-IoT s'appuie sur les réseaux 4G existants dont un certain nombre de fonctionnalités et mécanismes sont hérités. Il est donc compatible avec une mobilité à l'international grâce à l'itinérance aussi appelé roaming. Cela signifie aussi que ces réseaux sont accessibles sous licence et sont pilotés par des opérateurs spécialisés dans le domaine. La qualité du réseau est donc gérée par des experts du métier.

NB-IoT est considéré **5G ready**, c'est à dire qu'à sa sortie il pourra être compatible avec cette nouvelle norme de transmission.

Les modes de déploiement de NB-IoT

Le NB-IoT peut se déployer selon trois modes : ***In-band, Guard-band LTE et standalone.***

- 1. mode autonome**, pour les cas où les services cellulaires ne sont pas présents ou sont mis hors service pour rendre le spectre nb-iot disponible, ce qui est le cas du GSM cellulaire; en recadrant un ou plusieurs opérateurs GSM pour acheminer le trafic NB-IoT, les opérateurs peuvent assurer une transition en douceur vers le LTE pour une communication de type machine massive
- 2. Mode bande de garde**, pour les cas où des services cellulaires sont présents et NB-IoT est positionné dans la bande de garde des porteuses LTE, sans allouer de ressources LTE et éviter d'éventuelles interférences
- 3. mode en bande**, pour les cas où des services cellulaires sont présents et NB-IoT est positionné dans la porteuse LTE partageant les ressources LTE; ce mode de fonctionnement est peut-être le plus rentable et le plus transparent pour les opérateurs mobiles car il ne nécessite aucune modification matérielle du réseau d'accès radio et utilise efficacement les ressources du

spectre pour les services LTE ou NB-IoT en fonction de la demande des utilisateurs ou des appareils mobiles

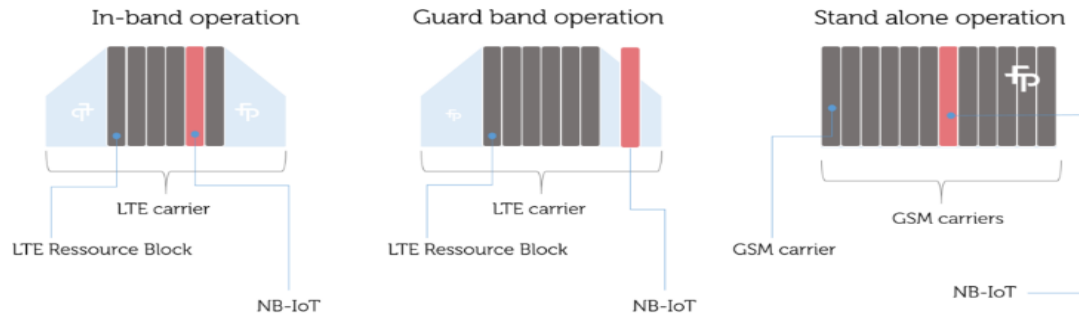


Figure 12: modes de déploiement de nb-iot

Exigences de sécurité de NB-IoT

Les exigences de sécurité de NB-IoT sont similaires à celles de l'IoT traditionnel. Cependant, il existe de nombreuses différences, qui concernent principalement les équipements matériels IoT à faible consommation d'énergie, le mode de communication réseau et les exigences de service réelles. Par exemple, le système terminal de l'IoT traditionnel a généralement une puissance de calcul élevée, un protocole de transmission réseau compliqué et adopte un plan de renforcement de la sécurité plus strict; De plus, la consommation d'énergie est généralement élevée et une charge fréquente est requise. D'un autre côté, un équipement IoT de faible puissance se caractérise par une faible consommation d'énergie, une faible puissance de calcul et une charge non fréquente, ce qui signifie également que les problèmes de sécurité sont plus susceptibles de menacer les terminaux. De plus, une simple consommation de ressources peut provoquer un état de déni de service. De plus, dans le déploiement réel, le nombre de terminaux IoT à faible consommation d'énergie est beaucoup plus important que dans l'IoT traditionnel. En conséquence, toute vulnérabilité de sécurité minuscule peut produire des accidents de sécurité beaucoup plus importants car le système intégré du terminal est plus simple et plus léger, il est donc beaucoup plus facile pour un attaquant de maîtriser toutes les informations sur le système.

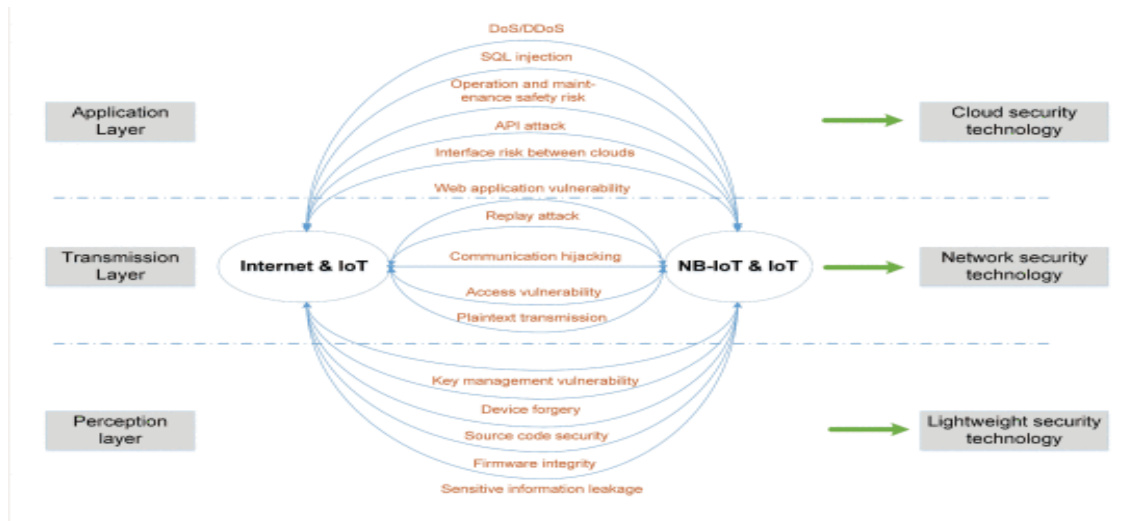


Figure 13: La similitude entre NB-IoT et IoT traditionnel en termes d'exigences de sécurité.

L'analyse suivante présente les exigences de sécurité de NB-IoT visant une architecture à 3 couches composée d'une couche de perception, d'une couche de transmission et d'une couche d'application.

A. Couche de perception

La couche de perception est la couche inférieure de NB-IoT qui représente le fondement des couches supérieures de l'architecture et des services. Semblable à la couche de perception IoT commune, la couche de perception de NB-IoT a tendance à être soumise à la fois à des attaques passives et actives. L'attaque passive signifie que l'attaquant ne vole que les informations sans apporter aucune modification. Les principales méthodes incluent l'écoute, l'analyse du trafic, etc. Comme la transmission de NB-IoT repose sur un réseau sans fil ouvert, les attaquants peuvent obtenir des informations sur les terminaux NB-IoT avec des méthodes telles que le vol de liaison de données et l'analyse des caractéristiques du trafic dans le but de mener une série d'attaques ultérieures.

La durée de vie de la batterie dans les équipements NB-IoT peut atteindre 10 ans en théorie. Étant donné que le débit de perception des données au niveau du nœud NB-IoT est faible, pour des raisons de sécurité, un mot de passe léger (tel que le chiffrement de flux et le chiffrement par blocs) doit être déployé dans la couche de perception pour réduire la charge de calcul aux terminaux et prolonger la durée de vie de la batterie.

Différent de la couche de perception dans l'IoT traditionnel, le nœud de la couche de perception peut ici communiquer directement avec la station de base dans la cellule, évitant ainsi les problèmes de sécurité de routage potentiels lors de la mise en réseau. D'autre part, l'authentification d'identité entre les nœuds dans la couche de perception de NB-IoT et la station de base dans la cellule doit être bidirectionnelle, c'est-à-dire que l'authentification d'accès doit être effectuée par la station de base vers le certain nœud de perception de NB-IoT, et il doit également être effectué par le nœud NB-IoT jusqu'à la station de base dans la cellule actuelle afin d'éviter toute menace de sécurité pouvant être apportée par une pseudo station de base

B. Couche de transmission

Contrairement à la couche de transmission dans l'IoT traditionnel, NB-IoT modifie le déploiement de réseau compliqué dans lequel la passerelle relais collecte des informations puis les renvoie à la station de base. Par conséquent, de nombreux problèmes tels que la mise en réseau multi-réseaux, le coût élevé et la batterie haute capacité sont résolus. Un réseau pour une ville entière peut apporter des avantages pour la maintenance et la gestion et des avantages tels que l'adressage et l'installation faciles en se séparant du service immobilier. Cependant, de nouvelles menaces à la sécurité sont également présentes:

x. Accès aux terminaux NB-IoT haute capacité

Un secteur de NB-IoT peut prendre en charge la connexion à environ 100 000 terminaux. Le principal défi consiste à effectuer une authentification d'identité et un contrôle d'accès efficaces pour ces connexions massives à haute capacité en temps réel afin d'éviter l'injection de fausses informations par un nœud malveillant.

xi. Environnement réseau ouvert

La communication entre la perception de NB-IoT et la couche de transmission se fait entièrement via un canal sans fil. La vulnérabilité intrinsèque du réseau sans fil présente des risques potentiels pour le système. À savoir, l'attaquant pourrait transmettre un signal d'interférence pour provoquer une panne de communication. De plus, comme il y a une grande quantité de nœuds dans un seul secteur, l'attaquant pourrait parrainer l'attaque par déni de

service (DoS) avec des nœuds contrôlés par lui, donc il pourrait influencer les performances du réseau.

La solution des problèmes ci-dessus est d'introduire un mécanisme d'authentification de bout en bout efficace et un mécanisme d'accord clé, afin d'assurer la confidentialité et la protection de l'intégrité de la transmission des données ainsi que l'identification de la légalité des informations. À l'heure actuelle, il existe des normes de sécurité de transmission pertinentes pour les réseaux informatiques et les communications mobiles LTE, telles que IPSEC, SSL et AKA. Cependant, le principal problème est la réalisation de ces technologies dans le système NB-IoT grâce à l'optimisation de l'efficacité.

C. La couche d'application

La couche d'application de NB-IoT a pour objectif de stocker, d'analyser et de gérer efficacement les données. Après la couche de perception et la couche de transmission, une grande quantité de données converge dans la couche d'application. Ensuite, des ressources massives sont formées pour fournir un support de données pour diverses applications. Par rapport à la couche d'application du réseau IoT traditionnel, la couche d'application de NB-IoT transporte une plus grande quantité de données. Les principales exigences de sécurité sont les suivantes:

xii. Identification et traitement de données hétérogènes massives

En raison de la diversité des applications NB-IoT, les données convergées dans l'application sont hétérogènes, ce qui augmente la complexité du traitement des données. Par conséquent, l'identification et la gestion efficaces de ces données avec les ressources informatiques existantes deviennent le problème central de la couche d'application NB-IoT. De plus, la tolérance aux catastrophes en temps réel, la tolérance aux pannes et la sauvegarde sont également des questions qui méritent d'être examinées. Le fonctionnement efficace des services NB-IoT devrait être garanti autant que possible dans divers cas extrêmes.

xiii. Intégrité et authentification des données

Les données convergées dans la couche application proviennent de couches de perception et de transmission. La seule exception se produit lors de la collecte et de la transmission, où l'intégrité des données est soumise à divers degrés de dommages. En outre, une opération illégale par des initiés sur les données entraînerait également une perte d'intégrité des données. Ainsi, l'utilisation des données dans la couche application peut être influencée. La solution de ces problèmes de sécurité réside dans la mise en place de mécanismes efficaces de vérification et de synchronisation de l'intégrité des données. En outre, la technologie de

déduplication des données, la technologie d'autodestruction des données, la technologie d'audit des flux de données et d'autres technologies sont également nécessaires pour garantir la sécurité des données pendant les processus de stockage et de transmission dans toutes les directions.

xiv. Contrôle d'accès aux données

Il existe un grand nombre de groupes d'utilisateurs dans NB-IoT. Les autorisations d'accès et d'exploitation pour différents utilisateurs de données sont différentes. Les autorités correspondantes pour les différents niveaux d'utilisateurs devraient être mises en place pour permettre aux utilisateurs de procéder à un partage contrôlé des informations. Actuellement, les mécanismes de contrôle d'accès aux données sont principalement le mécanisme de contrôle d'accès obligatoire, le mécanisme de contrôle d'accès discrétionnaire, le mécanisme de contrôle d'accès basé sur les rôles et le mécanisme de contrôle d'accès basé sur les attributs. Différentes mesures de contrôle d'accès doivent être prises selon la différence de confidentialité des scènes d'application.

NB-IoT et 5G

La génération 5G est déjà là! Vous voyez, la 5G n'est pas seulement pour les smartphones, elle couvre un large éventail d'applications, ce qui peut être attribué à deux directions parallèles de la couverture du réseau sans fil: l'une permet une bande passante ultra élevée avec une communication directionnelle à courte portée, et l'autre couvre un large zone et utilise une puissance ultra-faible.

Le réseau à très haut débit permet de transmettre un débit de données élevé et une latence ultra faible devient enfin possible, dépassant même les performances du haut débit fixe. Parce que ces performances élevées nécessitent un modem très complexe et une consommation d'énergie élevée, elles seront principalement utilisées dans les appareils personnels ou de grandes tailles telles que les véhicules.

Le réseau étendu à faible consommation d'énergie (LPWA) est la description générale utilisée pour la future infrastructure de connectivité IoT, où un grand nombre de dispositifs à faible consommation d'énergie sont placés pratiquement n'importe où, même dans des endroits auparavant inimaginables. Le potentiel de ce déploiement à grande échelle peut apporter une énorme valeur commerciale, mais il n'est pas sans défis; il existe potentiellement une grande variété d'applications IoT, dont certaines seront déployées pendant de nombreuses années et ne nécessitent presque aucune interaction ou maintenance manuelle. Cela nécessitera une conception résiliente alimentée souvent par batterie tout au long de sa période d'installation.

L'infrastructure des opérateurs commerciaux existants (2G / 3G / 4G) et les fréquences sans licence telles que le Wi-Fi ne sont pas en mesure de répondre aux besoins de milliards de dispositifs dans le monde.

Après la phase initiale de recherche et de discussions sur la façon de réutiliser l'espace réseau disponible pour mieux s'adapter à l'avenir de l'IoT, les technologies de mise en réseau étendu ont progressivement été divisées en deux groupes.

L'un se concentre sur le spectre non autorisé de Lora et SigFox, l'autre opère dans les zones de spectre sous licence des technologies mobiles 2G / 3G / 4G et est pris en charge par 3GPP comme LTE-Cat-M et NB-IoT.

Dans la compétition des normes, Lora et SigFox fonctionnent déjà depuis plusieurs années, il existe donc des défenseurs de la technologie qui utilisent la technologie. Cependant, elle s'appuie sur l'utilisation d'un spectre sans licence pour prendre en charge son service. En tant que telle, cette technologie ne peut pas attirer efficacement un public mondial. Mais les limites de Lora et SigFox sont plus importantes que cela; avec la sécurité des données, les coûts de construction du réseau, la prise en charge des secteurs verticaux et la couverture réseau manquant par rapport aux alternatives 3GPP. Simplement: les technologies 3GPP LPWA peuvent atteindre plus de clients, à moindre coût, avec une plus grande échelle et un support.

Comparison with different LPWA Standards

Standard	SigFox	LoRa	NB-IoT
Bandwidth	100Hz	125KHz	200KHz
Data Rate	100bps	0.3-50kbps	200kbps
Coverage	Good (17km)	Good (14km)	Excellent (22km)
Battery Life	5-10 yr	5-10 yr	5-10 yr
Cost	Good	Better	Excellent
Ecosystem	Weak	Fragmented by region	Excellent

MEDIATER

Figure 14: comparaison entre les différent LPWA standards

Avec la marche de l'évolution des normes de télécommunications, le retrait des anciennes technologies GPRS / GSM a donné une opportunité au réseau LPWA de réutiliser cet espace. Dans ce domaine, la technologie 3GPP a trois normes principales: LTE Cat-M, EC-GSM et NB-IoT. Toutes ces technologies ont un avantage significatif sur Lora et SigFox, avec une (ré) utilisation intelligente des spectres sous licence mondiale. Malgré un démarrage ultérieur, le 3GPP LPWA devrait à la fois limiter et remplacer les développements antérieurs du marché de Lora ou SigFox.

Le LTE Cat-M est principalement axé sur les appareils Machine-to-Machine (M2M) et, comme son nom l'indique, fonctionnera grâce à l'utilisation du spectre 4G LTE existant, offrant l'option d'une plus grande bande passante au détriment d'une consommation d'énergie plus élevée et d'une portée moindre par rapport à aux autres technologies LPWA. En comparaison, NB-IoT nécessite un matériel beaucoup plus simple que LTE Cat-M; la mémoire requise est plus faible et la complexité du modem et des RF est moindre. Cela permet un produit beaucoup plus axé sur les coûts qui peut être facilement mis à l'échelle pour les grands déploiements.

Alternativement, EC-GSM (Extended Coverage-GSM) est uniquement basé sur la mise à niveau de la technologie GSM 2G traditionnelle pour les applications IoT. Comme NB-IoT, il utilise également une technologie de réseau à bande étroite (200 kHz), tout en offrant une couverture plus large que le GPRS 20 dB traditionnel. Mais le protocole de communication GSM d'origine est obsolète et doit être redéfini afin de créer un environnement de communication «propre» capable de prendre en charge efficacement des milliers à des millions d'appareils connectés. Le résultat de cette nouvelle réflexion est NB-IoT.

En tant que tel, NB-IoT est considéré comme la force dominante dans les réseaux LPWA. Il peut répondre aux cinq exigences cruciales de l'ère de l'IoT:

- **Améliorer les performances de la couverture intérieure et apporter une couverture pour rendre les zones auparavant non connectables**
- **Prend en charge une très grande échelle de connexions,**
- **Réduire la complexité de l'équipement (principalement le modem),**
- **Minimisez la consommation d'énergie**
- **Réduisez les délais.**

NB-IoT, en tant que technologie mondiale de couverture de qualité télécom, est supérieure aux autres technologies en termes de faible consommation d'énergie, de faible coût, de large couverture et de portée accrue. Couplé à une percée dans la quantité de transmission de données, NB-IoT gagne déjà un soutien croissant de la part des opérateurs de télécommunications. Nous avons observé que la vitesse de construction du réseau NB-IoT s'accélère déjà dans différentes régions.

Alors que le processus de normalisation de base NB-IoT s'achève très bientôt, les fabricants de dispositifs en silicium, comme MediaTek, coopèrent activement avec les opérateurs de réseau

mondiaux pour tester sur le terrain les déploiements en état de préparation. Avec un tel engagement de soutien, la chaîne de l'industrie NB-IoT arrivera à maturité rapidement, découvrant véritablement le potentiel de l'IoT.

Comparaison entre LTE-M et NB-IOT

NB-IoT et LTE-M sont des technologies de communication réseau sans fil spécialement conçues pour l'IoT. Elles sont toutes deux appelées LPWAN pour Low Power Wide Area Network. Ces deux technologies sont d'excellentes solutions pour les objets connectés ou besoins dans l'industrie

LTE-M et NB-IoT ont chacune des différences clés, comme le temps de réponse (latence ou latency) et le débit.

Le débit

Dans les réseaux IoT, le débit nécessaire varie en fonction des besoins. Par exemple, le débit nécessaire pour les caméras industrielles est bien plus important que pour un simple capteur connecté.

LTE-M est le protocole qui propose le plus grand débit. Il possède d'ailleurs un débit bien supérieur aux technologies comme SIGFOX ou LoRaWan. Cependant, ses spécifications ne lui permettent pas d'atteindre des débits tels que ceux des technologies LTE comme la 4G. D'après ses caractéristiques techniques théoriques, LTE-M permet d'atteindre un débit de l'ordre de 1Mb/s en envoi ou réception (Upload/Download) de données.

NB-IoT, quant à lui propose un débit bien inférieur, de l'ordre de 24Kb/s. Celui-ci répondra cependant largement à des besoins IoT simples pour l'envoi de données de capteurs ou d'applications simples.

La latence ou temps de réponse

Le temps de réponse sera, tout comme le débit, un critère déterminant dans la sélection de la technologie la plus à même de répondre à vos besoins. En effet, un équipement peut être implémenté pour communiquer en temps réel ou pour collecter des données et les envoyer à intervalles de temps régulier. Là aussi LTE-M et NB-IoT diffèrent.

LTE-M possède la latence la plus faible (de l'ordre de 10ms). Ce protocole pour réseau mobile est donc particulièrement intéressant pour la communication temps réel. A l'opposé, **NB-IoT** propose des temps de réponse de l'ordre de la seconde (1 seconde).

D'autres différences subsistent bien entendu, comme notamment le coût. Le débit plus élevé et la latence plus faible de LTE-M rendent cette technologie plus coûteuse que NB-IoT.

Support de la mobilité

Une caractéristique majeure du LTE qui a été laissée de côté dans le contexte NB-IoT est la gestion de la mobilité dans l'état actif (handover). Si un device NB-IoT détecte qu'il pourrait être mieux servi par une autre cellule, il doit d'abord passer à l'état repos, puis re-sélectionner l'autre cellule. De plus, NB-IoT ne prend pas en charge les mesures sur les canaux radio et leur envoi à l'eNodeB. Les deux caractéristiques ont été jugées contreproductives comme le système a été optimisé pour transférer seulement de très petits volumes de données. Enfin, la rétrocompatibilité avec LTE, GSM ou UMTS n'est également Copyright EFORT 2018 2 pas pris en charge, un appareil NB-IoT doit uniquement prendre en charge la partie NB-IoT des spécifications. Au contraire, LTE-M supporte le handover permettant au device LTE-M de changer de cellule en communication.

Transfert de données

Il existe différentes options de connectivité de données pour les connexions PDN disponibles pour les devices IoT utilisant l'EPS:

- IP sur le plan de contrôle (UDP et TCP) à partir de Rel. 13, i.e., PDN Type = IP, autrement dit, l'UE gère la couche IP et obtient une adresse IP pour émettre et recevoir ses données sur le plan contrôle.
- IP sur le plan usager (UDP et TCP) avec PDN Type = IP
- Non-IP sur le plan de contrôle, i.e., PDN Type = non-IP, autrement dit, le device IoT ne gère pas la couche IP, n'obtient donc pas d'adresse IP pour émettre et recevoir ses données, et utilise des protocoles d'application directement sur le plan contrôle. De tels protocoles standard sont à titre d'exemple CoAP (Constrained Application Protocol) et MQTT-SN (Message Queue Telemetry for Sensor Networks).

Certaines optimisations sur le plan contrôle et le plan usager sont considérées notamment pour l'allocation des ressources lors de l'émission ou la réception. Le plan contrôle EPS CIoT peut être utilisé pour transporter des données utilisateur ou des messages SMS via MME en les encapsulant dans des messages NAS (Non-accessStratum); cela réduit le nombre total de messages de plan de contrôle lors de la gestion d'une transaction de données courte. Le terme DoNAS est utilisé pour Data over NAS.

Pour les services qui transmettent occasionnellement des quantités raisonnablement faibles de données, l'utilisation du plan de contrôle optimisera la consommation d'énergie en raison du fait que la quantité de signalisation requise est réduite. La consommation d'énergie peut être optimisée en utilisant non-IP, UDP/IP et TCP/IP. Non-IP permet l'utilisation de protocoles optimisés pour un usage spécifique. UDP est asynchrone, ce qui réduit le temps de connexion, tandis que TCP maintiendra la connexion ouverte jusqu'à ce qu'un accusé de réception soit reçu.

Les services qui doivent envoyer plus d'informations pourraient bénéficier de la connexion du plan usager, qui peut être utilisée pour envoyer plusieurs paquets. Dans l'ensemble, cette approche pourrait consommer moins d'énergie que d'envoyer plusieurs messages sur le plan de contrôle.

Pour LTE-M, l'utilisation du plan usager avec optimisation est obligatoire alors que l'utilisation du plan contrôle avec optimisation optionnelle. C'est l'inverse pour NB-IoT.

NB-IoT et La sécurité

Lorsque nous parlons d'Internet des objets (IoT), la sécurité est l'un des problèmes qui inquiètent le plus les utilisateurs. Les nouveaux réseaux IoT, tels que NarrowBand IoT (IoT), ont permis d'accéder plus économiquement et depuis longtemps à Internet sans maintenance en raison de la faible consommation d'énergie. Mais le marché est préoccupé par la manière de gérer la sécurité des données que ces appareils signalent. Dans cet article, nous nous concentrerons sur la sécurité des communications des appareils qui utilisent le réseau NB-IoT et communiquent avec un serveur dans le cloud.

- Le premier, l' **authentification** . Avec cela, nous garantissons que l'appareil qui envoie des données vers le cloud est autorisé et que personne ne l'a remplacé par un autre. De même, nous garantissons à l'appareil que le cloud avec lequel il échange des informations et que personne ne le remplace ou ne s'approprie illicitement les données.
- Avec le **cryptage** , nous garantissons qu'un observateur des communications ne peut pas comprendre les messages et seul le cloud avec les clés de décryptage peut récupérer les messages.
- Et avec la **non-manipulation** , nous garantissons que personne n'a modifié le message que l'appareil IoT envoie au cloud.

Au sein d'un réseau NB-IoT, les données voyagent cryptées et donc de manière sécurisée. Le problème avec les informations apparaît une fois que les données quittent le réseau NB-IoT et sont envoyées sur Internet, des serveurs de l'opérateur du réseau au serveur cloud final où le client a installé son centre de réception et le traitement des données.

En règle générale, le NB-IoT utilise le protocole UDP. Il s'agit d'un protocole très simple et idéal pour NB-IoT en raison de sa faible consommation, car il n'a pas besoin d'établir de connexion pour envoyer des données. Lorsqu'un paquet UDP plat se déplace sur Internet, toutes ses données sont visibles par des tiers.

Si nous voulons utiliser l'une des principales caractéristiques de NB-IoT: pour avoir la consommation la plus faible possible de tous les réseaux LPWAN, nous devons passer par le

protocole UDP, ce qui est dangereux par nature. Nous pouvons encore avoir une faible consommation d'énergie en utilisant UDP et assurer la sécurité des communications.

Méthodes de gestion de la sécurité dans NB-IoT

Il existe différentes méthodes de gestion de la sécurité dans un réseau de communication NB-IoT, entre les appareils et le serveur cloud où les informations sont signalées.

- **APN ou plate-forme d'opérateur:** certains opérateurs offrent à NB-IoT la possibilité de monter un serveur intermédiaire qui collecte les données du réseau NB-IoT sans passer par Internet. La plate-forme finale du client est généralement connectée via une connexion VPN sécurisée à la plate-forme de l'opérateur, ce qui sécurise le chemin d'accès complet de l'appareil au serveur cloud du client
- **Sécurisation du protocole UDP:** dans ce cas, les données voyagent de bout en bout cryptées par la même technologie, et le serveur cloud est responsable de l'authentification et du décodage des données.
- **Ne pas appliquer de sécurité:** c'est la possibilité la plus simple, mais elle n'est pas recommandée. Cette option ne peut être mélangée que dans les tests de performances, car les projets réels et en volume peuvent recevoir plusieurs attaques sans aucune capacité à faire face.

Authentification mutuelle

Authentification mutuelle entre le client et l'entité d'authentification doit être effectuée, le client est alors authentifié au domaine de sécurité. Les mécanismes d'authentification sont dépendants de la situation. Dans un réseau local, avec des appareils contrôlés par une seule entité, utiliser des clés préconfigurées comme mécanisme d'authentification est un scénario réaliste. Si le déploiement comporte de nombreux clients, les certificats avec une durée de validité limitée peut être un meilleur choix : le serveur de ressources effectuant l'authentification n'aura pas à garder un état pour chaque client. Enfin, si les certificats ont une durée de validité limitée, le serveur de ressources doit vérifier la date d'expiration des certificats et la signature.

Les avantages de NB-IoT

Cette nouvelle technologie apporte un certain nombre d'avantages par rapport à son domaine d'utilisation :

La faible consommation

Le premier point critique dans le domaine des objets connectés est la consommation électrique. Comme vu plus haut, le nombre de devices intelligents ne fait qu'augmenter. Il est donc primordial que ces supports consomment le moins possibles pour plusieurs raisons:

- Lutter contre la surconsommation électrique
- Il n'est pas envisageable de recharger ou changer des batteries d'un tel nombre d'IoT
- Pourquoi consommer de l'énergie alors que ce n'est pas nécessaire ?

Cette technologie est dite LPWAN donc répond aux standards de consommation minimale.

La fiabilité

La communication de ces objets via **NB-IoT** n'est certes pas temps réel mais se doit d'être fiable dans le temps. En s'appuyant sur des réseaux existants et sous licence, les opérateurs sont déjà en charge de la qualité de service de ceux-ci. Ils pourront ainsi garantir une **QoS** (Quality Of Service) suffisante pour ce type de fonctionnement.

Diminution des coûts

La simplicité du standard sur lequel repose cette technologie permet de créer des puces de communication peu onéreuses. En effet, une puce qui supporte uniquement NB-IoT est beaucoup moins chère à produire qu'un module qui implémente LTE-M par exemple. De plus, le fait d'être orienté très faible consommation, c'est encore une économie substantielle. Contrairement à certaines autres technologies, il n'y a aucunement besoin d'une passerelle (gateway) pour que cela fonctionne.

Une couverture plus adaptée

Reposant sur le réseau actuel de la 4G ce mode de communication est aussi bien adapté pour une **utilisation en intérieur** (Indoor) ou **en extérieur**. Ainsi la seule problématique, quand il sera implémenté, sera de vérifier la couverture des localisations de vos devices IoT.

Les inconvénients du protocole Nb-IoT

Aujourd'hui techniquement, il y a peu **"d'inconvénients"** à ce genre de technologies. Normés par la 3GPP, les modules proposés, en version Global, fonctionnent dans le monde entier.

Contrairement aux technologies Sigfox ou LoRa qui fonctionnent sur des fréquences libres (868MHz/433MHz et 169Mhz en Europe), le Nb-IoT n'est pas une technologie propriétaire, elle s'appuie sur une normalisation mondiale de réseaux et permet ainsi l'interopérabilité. Les fabricants de modules cellulaires répondent aux mêmes normes, ainsi les « industriels » peuvent basculer d'un fabricant à un autre (même si cela ne nous arrange pas toujours !).

Aussi, utiliser un module SIM7020G vous permettra de vous connecter au réseau NB-IoT, et ce, quel que soit le pays dans lequel votre device sera.

Si on peut lui trouver un inconvénient, pour l'instant, les réseaux ne sont pas totalement déployés, ou en tous cas pas dans la release 14- NB2 de la 3GPP, ainsi les débits attendus doivent encore être optimisés. Ce n'est qu'une question de temps !

En conclusion, nous sommes en train de préparer la ville de demain, le Nb-IoT et le Cat M sont des technologies qu'on appelle 5G ready... la partie Low Power de la 5G."

Application

NB-IoT est une authentique révolution. Jusqu'à présent, nous avons connecté de gros appareils coûteux, comme des téléviseurs, des ordinateurs et des smartphones, mais à partir de maintenant, TOUT peut être intelligent. Voici quelques-uns des principaux marchés potentiels pour les services NB-IoT:

VILLES INTELLIGENTES

Grâce à NB-IOT, les gouvernements locaux pourront contrôler plus efficacement l'éclairage public, les places de stationnement gratuites, les conditions environnementales, etc.

MAISONS ET BÂTIMENTS INTELLIGENTS

Gérer les alarmes d'intrusion et d'incendie pour les maisons et les propriétés commerciales; comptage intelligent (électricité, gaz et eau); éclairage intelligent et confort thermique; qualité de l'air; la sécurité physique... avec un faible coût et un impact environnemental moindre. Ce ne sont que quelques-unes des possibilités de NB-IOT dans les maisons et les bâtiments intelligents.

INDUSTRIE DE L'AGRICULTURE ET DU RANCHING

Les fermes du futur. Avec l'étendue de NB-IOT, apparaît une grande variété de solutions intelligentes d'agriculture et d'élevage, pour réaliser une ferme connectée autonome: plus de précision dans les techniques agricoles, la détection du sol et de l'atmosphère, le suivi du bétail (avec des alertes de mouvement quand hors de portée), surveiller de terre, pollution, pluie...

SOINS DE SANTÉ

La connectivité NB-IOT offrira la possibilité de surveiller ceux qui souffrent de maladies chroniques ou liées à l'âge. Avec un appareil portable, le médecin contrôlera ses patients à distance et en temps réel.

PERSONNES ET ANIMAL TRACKER

Grâce à ces appareils portables, NB-IOT pourra contrôler les personnes, en particulier les personnes âgées et les enfants, et les animaux (animaux domestiques, fermes, élevage...). Vous pourrez savoir où se trouvent vos proches et vos animaux partout. À n'importe quel moment; à tout moment.

FABRICATION ET LOGISTIQUE

Avec la connectivité NB-IOT, les industries seront beaucoup plus automatisées, efficaces et productives. Par exemple, localisera et surveillera facilement l'inventaire clé pour optimiser la logistique, ou permettra une surveillance en temps réel et des diagnostics prédictifs des actifs

Remarque

Il existe de nombreux cas d'utilisations auquel répond NB-IoT. Les cas présentés ci-dessus se veulent réels et sont des problématiques ou des sujets de réflexion actuels. Mais de manière générale tout objet connecté qui aurait besoin de communiquer sur de longues distances et qui ne nécessitent pas des temps de réaction trop rapides pourraient être concernés

Implémentation

En raison des conditions actuelles, on n'a pas pu acheter les équipements pour faire l'implémentation de notre technologie et car elle est difficile de simuler des objets qui sont connectées à l'aide de NB-IOT parce qu'il est nécessaire d'avoir des appareils NB-IOT.

Nous avons fait une simulation de technologies GPS et GSM dans le logiciel Proteus. Cette simulation est un peu loin de NB-IOT, mais elle s'inscrit dans le même contexte des technologies cellulaires.

Envoi de données de localisation GPS via GSM à l'aide de Proteus

Les outils utilisés

Pour faire notre simulation on a besoin d'installer et configurer les composants suivants :

Proteus (ISIS): est la composante de Proteus qui permet la création de schémas et la simulation électrique.

Arduino IDE : est une application multiplateforme (pour Windows, macOS, Linux) qui est écrite dans des fonctions de C et C ++ [2]. Il est utilisé pour écrire et télécharger des programmes sur des cartes compatibles Arduino, mais aussi, avec l'aide de tiers, d'autres cartes de développement de fournisseurs, on a utilisé pour créer le programme et converti vers une extension `.hex` pour intégrer le fichier dans le simulateur uno.

Le module GPS : Ce module GPS que j'ai conçu pour Proteus est un simple GPS qui a des broches TX et RX et lorsque vous démarrez la simulation, ce module commence à envoyer les données NMEA sur sa broche TX, que vous pouvez facilement vérifier en utilisant Virtual Terminal .

Le module GSM : Le module SIM900D de SIMCom permet au microcontrôleur de communiquer en utilisant le réseau GSM en envoyant des commandes AT à l'UART.



Le module GSM : Le module SIM900D de SIMCom permet au microcontrôleur de communiquer en utilisant le réseau GSM en envoyant des commandes AT à l'UART.




Le module Arduino UNO : Cette bibliothèque arrive pour faciliter la simulation de nos circuits.

Configuration

Tout d'abord, téléchargez la bibliothèque GSM, GPS et Arduino pour Proteus.

Lorsque nous le téléchargez, on a obtient les fichiers suivants :

 ARDUINO2.IDX
 ARDUINO2.LIB

 GpsTEP.HEX
 GpsTEP.IDX
 GpsTEP.LIB





 GSMLibraryTEP.hex
 GSMLibraryTEP.IDX
 GSMLibraryTEP.LIB

Figure 17: la bibliothèque Arduino

Figure 16: la bibliothèque GPS

Figure 15: la bibliothèque GSM

Puis on a placé tous ces fichiers dans le dossier Bibliothèques de notre logiciel Proteus 8

 > This PC > Local Disk (C:) > ProgramData > Labcenter Electronics > Proteus 8 Professional > LIBRARY

Remarque :

Si nous avons utilisé Proteus 7 l'emplacement du dossier LIBRARY est différent, où on trouve dans :

C: \ Program Files (x86) \ Labcenter Electronics \ Proteus 7 Professional \ LIBRARY

Après que nous avons ajouté les bibliothèques nous allons construire notre schéma de la simulation à l'aide d'ISIS Proteus.

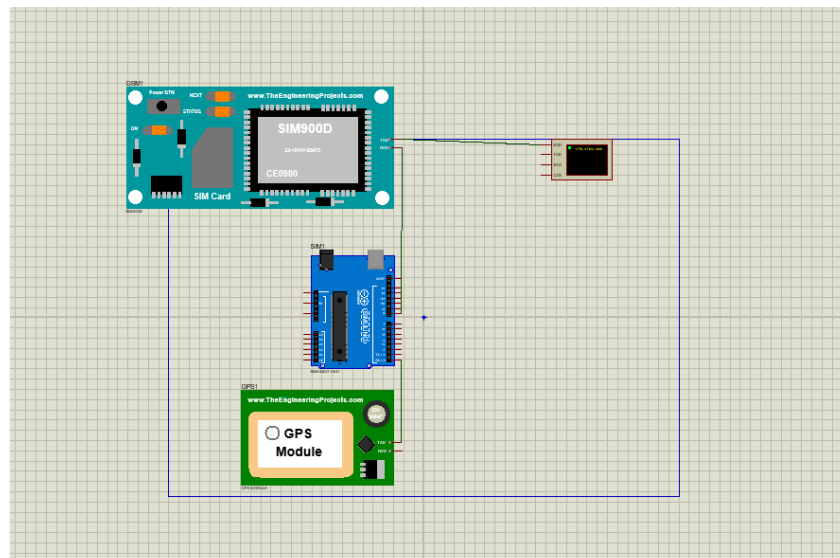


Figure 18: schéma de la simulation

Dans le schema ci-dessus nous allons ajouter

- une carte arduino de type simulino uno
- un composant GPS module
- un composant GSM SIM900D
- un terminal virtuel pour visualiser le résultat

Les ports TX et RX utilisé pour la communication entre la carte Arduino et un ordinateur ou d'autres appareils.

Par la suite on ajouté le fichier GSMLibraryTEP.HEX dans le module SIM900D et le fichier GpsTEP.HEX dans le module GPS

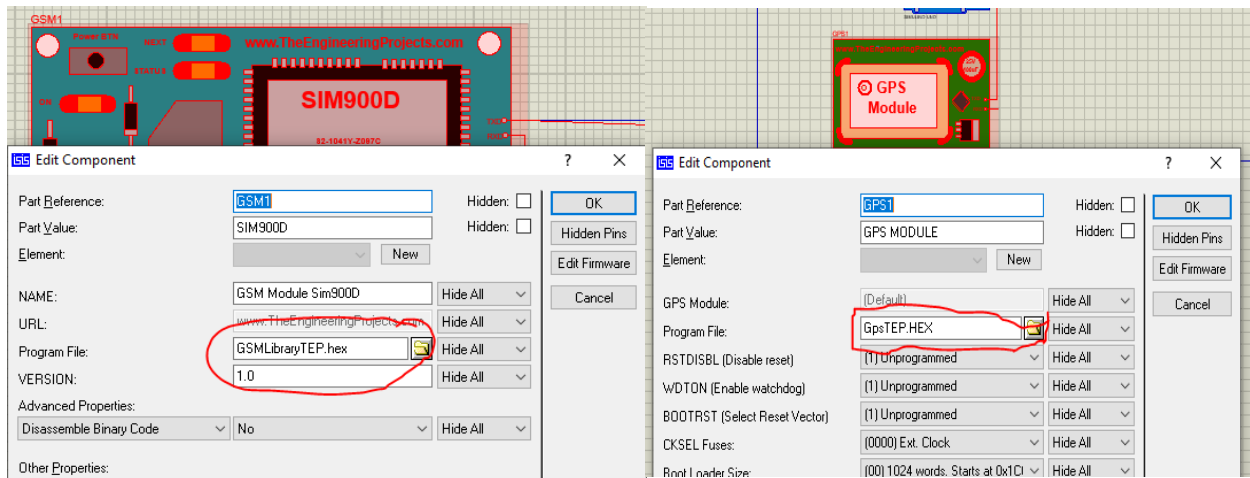


Figure 19:Ajouter le fichier HEX

Arduino : utiliser les fichiers .hex

Programmer un arduino se fait en plusieurs étapes : d'abord écrire le code, puis le compiler, c'est à dire le transformer en commandes adaptées au circuit, enfin le téléverser dans le microcontrôleur.

Le fichier compilé est du "code machine" au format hexadécimal (.hex), il n'est plus lisible pour nous autres mammifères, mais parfaitement adapté pour un circuit électronique. On ne peut pas retrouver le code d'origine depuis le fichier .hex (dans le meilleur des cas on peut le décompiler pour récupérer un programme en assembleur)

Pourquoi utiliser un fichier .hex ?

Quelques raisons d'utiliser le fichier .hex :

- le programme a été récupéré depuis un arduino, on n'en a donc pas le code source,
- pour programmer rapidement plusieurs arduino identiques avec le même programme,
- le programme n'a été diffusé que sous forme de .hex pour une quelconque raison...

Codage.

Dans cette partie nous allons expliquer notre code qui se trouve ci-dessous :

```
#include <TinyGPS.h>
#include <SoftwareSerial.h>

SoftwareSerial SIM900(7, 8); //Les broches 7 et 8 sont déclarées comme TX et RX
TinyGPS gps; //Créer une nouvelle instance de tinyGPS

void setup() {
  Serial.begin(9600); //réglage taux de baud du module gsm
  SIM900.begin(9600); //réglage taux de baud du moniteur série
}
```

Figure 20:initialisation de code et setup fonction

Tout d'abord nous allons inclure 2 fichiers .h :

TinyGPS : est conçu pour fournir la plupart des fonctionnalités GPS NMEA que j'imagine qu'un utilisateur Arduino voudrait - position, date, heure, altitude, vitesse et cap - sans la grande taille qui semble accompagner des corps de code similaires. Pour réduire la consommation de ressources, la bibliothèque évite toute dépendance en virgule flottante obligatoire et ignore tous les champs GPS clés à l'exception de quelques-uns.

SoftwareSerial est une bibliothèque d'Arduino qui permet la communication de données série via d'autres broches numériques d'Arduino. La bibliothèque réplique les fonctions matérielles et gère la tâche de communication série.

La fonction setup() est appelée au démarrage du programme. Cette fonction est utilisée pour initialiser les variables, le sens des broches, les librairies utilisées. La fonction setup n'est exécutée qu'une seule fois, après chaque mise sous tension ou reset (réinitialisation) de la carte Arduino.

begin() : a pour utilité d'initialiser la vitesse de transmission des données série pour communiquer avec le.

```
void loop()
{
    bool newData = false;
    unsigned long chars;
    unsigned short sentences, failed;

    //Pendant une seconde, nous analysons les données GPS et rapportons certaines valeurs clés
    for (unsigned long start = millis(); millis() - start < 1000;)
    {
        while (Serial.available())
        {
            char c = Serial.read();
            if (gps.encode(c))
                newData = true;
        }
    }
}
```

Figure 21:loop fonction

La fonction loop() Après avoir créé une fonction setup(), qui initialise et fixe les valeurs de démarrage du programme, la fonction loop () (boucle en anglais) fait exactement ce que son nom suggère et s'exécute en boucle sans fin, permettant à votre programme de s'exécuter et de répondre. Utiliser cette fonction pour contrôler activement la carte Arduino.

Nous avons alimenté les données série NMEA de l'objet un caractère à la fois à l'aide de la méthode **encode ()** : (Chaque octet de données NEMA doit être donné à TinyGPS en utilisant encode (). True est renvoyé lorsque les nouvelles données ont été entièrement décodées et peuvent être utilisées). TinyGPS ne gère pas la récupération des données série d'une unité GPS. Lorsque **encode ()** renvoie «vrai», changer l'état interne de l'objet TinyGPS **NewData**.

```

if (newData)          //si newData est true
{
  float flat, flon;
  unsigned long age;
  gps.f_get_position(&flat, &flon, &age);
  SIM900.print("AT+CMGF=1\r");
  delay(400);
  SIM900.println("AT + CMGS = \""+212xxxxxxxxx"\"); // numéro de mobile du destinataire avec le code du pays
  delay(300);
  SIM900.print("Latitude = ");
  SIM900.print(flat == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flat, 6);
  SIM900.print(" Longitude = ");
  SIM900.print(flou == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flon, 6);
  delay(200);
  SIM900.println((char)26); // Fin de la commande AT avec un ^ Z, ASCII code 26
  delay(200);
  SIM900.println();
}
Serial.println(failed);
}
  
```

Figure 22:suite de code (loop fonction)

Si l'objet TinyGPS devient vrai nous allons utiliser la méthode `f_get_position`

f_get_position (&flatitude, &flongitude, &age): Obtenez la position, où la latitude et la longitude sont des variables de type flottant, et les valeurs réelles sont retournées. Les types flottants sont plus faciles à utiliser, mais entraînent un code plus volumineux et plus lent. La variable d'âge doit être de type long non signé.

Après on va compiler le programme et on a obtenu un fichier .hex qui a une emplacement dans le dossier temp

"C:\\Users\\EL-Aydi\\AppData\\Local\\Temp\\arduino_build_917205\\Sending_GPS_Location_data_over_GSM.ino.hex"

On ajoute le fichier dans le Component SIMULINO UNO

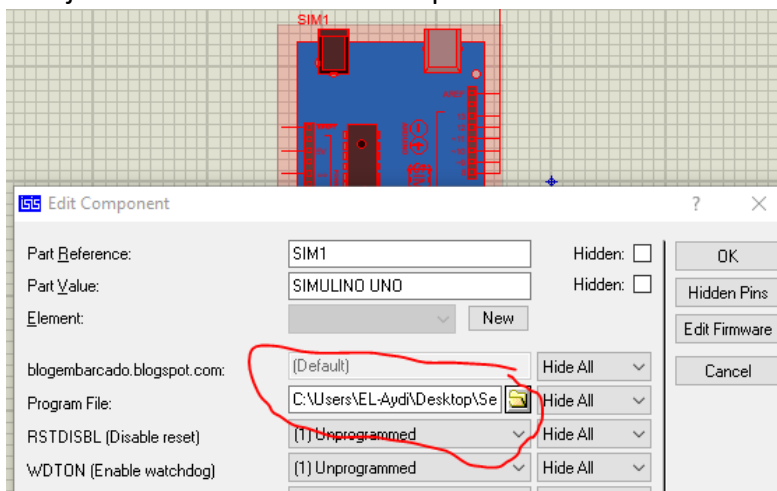


Figure 23: ajouter le fichier .HEX au SIM

Le teste

Pour conclure nous allons tester le fonctionnement de notre projet comme vous voyez ci-dessous on a obtenu la position à l'aide de latitude et longitude

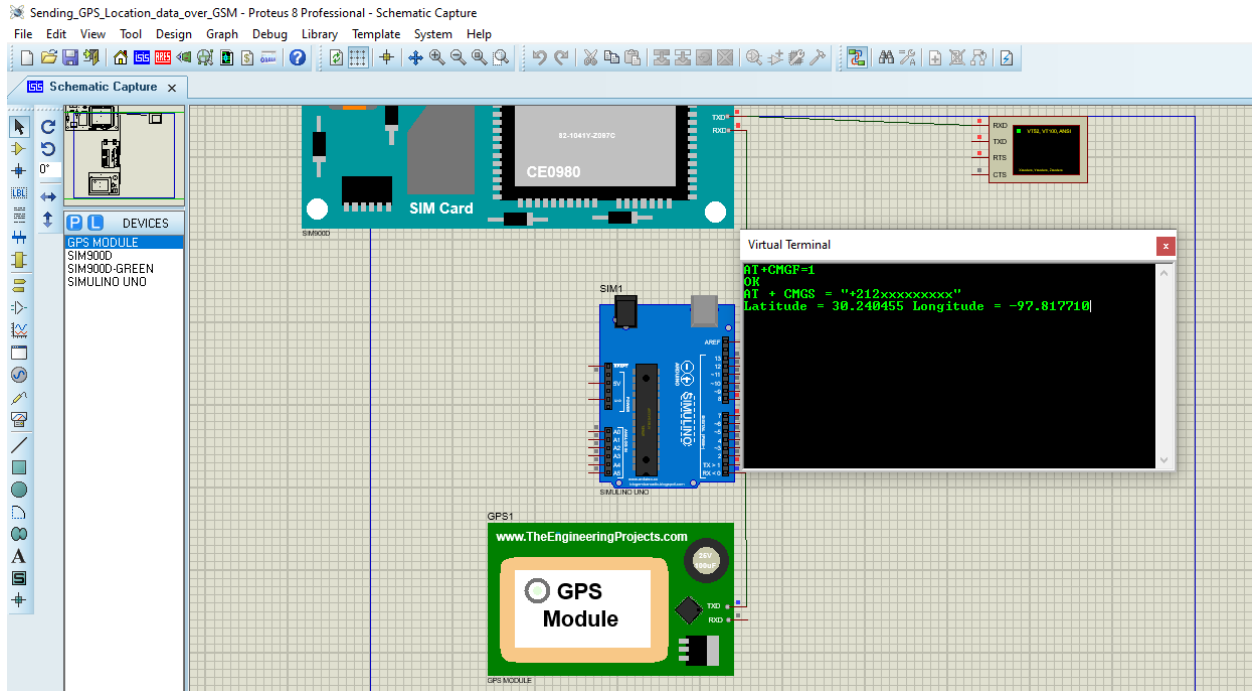


Figure 24: test de fonctionnement de projet

Conclusion

Le NB-IoT s'est démontré être une excellente alternative, car il a su rassembler tous les avantages que l'on connaît avec les réseaux mobiles tout en restant un réseau adapté à l'Internet des Objets de demain. En ce sens, il s'agit d'un réseau à mi-chemin entre le LPWAN et le LTE.

- Une faible consommation (objet sur batterie jusqu'à 10 ans et plus)
- Adapté aux fortes densités de capteurs (5G ready)
- Il entre dans la catégorie LPWAN avec des distances jusqu'à 50 km (milieu rural)
- Il a un excellent taux de pénétration dans les bâtiments
- Les modules sont low-cost (<10€) par rapport à du modem 2G et 3G

Le choix du réseau 2G et 3G n'est plus une option que l'on estime viable surtout si votre objet a vocation à avoir une durée de vie au-delà de 10 ans. Le NB-IoT répond clairement aux usages de l'IoT et là où hier l'option 2G et 3G était possible pour vos projets, l'option NB-IoT est aujourd'hui une alternative beaucoup moins onéreuse et adaptée.

Webographie

<https://accent-systems.com/nb-iot/>

<https://www.i-scoop.eu/internet-of-things-guide/lpwan/nb-iot-narrowband-iot/>

<https://www.gsma.com/iot/deployment-map/#deployments>

<https://www.ericsson.com/en/blog/2016/9/narrowband-iot-in-the-cloud>

<https://www.gsma.com/iot/wp-content/uploads/2019/07/201906-GSMA-NB-IoT-Deployment-Guide-v3.pdf>

<https://ieeexplore.ieee.org/document/8038776?denied=>

https://en.wikipedia.org/wiki/Narrowband_IoT

<https://www.3gpp.org/news-events/3gpp-news/1733-niot>

<https://itectec.com/technotes/nb-iot-physical-layer/>

<https://www.ericsson.com/en/blog/2017/5/robust-scrambling-for-nb-iot-broadcast-channels>

http://www.efort.com/r_tutoriels/EVOLUTIONS_MTC_EFORT.pdf