Contrôle de la Surcharge et de la Congestion dans le contexte Machine To Machine (M2M)

EFORT
http://www.efort.com

1 Introduction

Sur le long terme il est attendu un nombre de devices M2M bien plus important que le nombre de devices de communication personnels.
Le nombre de devices M2M connectés au réseau mobile de l 'opérateur est déjà important et il existe des cas où un grand nombre de devices M2M on causé des situations de congestion sérieuses dans le réseau.
La surcharge et la congestion causées par des devices M2M est principalement le résultat d 'un comportement synchronisé de devices M2M qui accèdent tous simultanément au réseau. Ce phénomène est cause à la fois par les devices M2M ayant une souscription avec leur opérateur et par les devices M2M en situation de roaming dans le même réseau d 'opérateur. Dans le cas du roaming, le trafic est difficilement prédictible.
Le but de ce tutoriel est de présenter le problème de congestion lié à des objets M2M et de montrer les éléments de solution pour résoudre le problème.

2 Exemples de causes de surcharge et de congestion

Parmi les causes de surcharge et de congestion dus à des communications M2M, figurent :

- Des applications M2M transmettant de manière récurrente et synchronisée des données, à intervalles de temps précis (e.g., a chaque heure)
- Une demande de déclenchement provenant d 'un serveur M2M demandant à un grand nombre de devices M2M de s 'attacher et d 'établir un contexte PDP tous simultanément, e.g., très grand nombre de compteurs devenant actifs au même moment après une panne de courant.
- Un grand nombre de capteurs transmettant leurs données simultanément suite à un événement survenu, e.g., seuil de surveillance atteint (niveau de pluviométrie, magnitude d 'un tremblement de terre, niveau de température, etc).
- Un mauvais fonctionnement au niveau du serveur M2M peut conduire les devices M2M qui transmettent leur données de continuer à les retransmettre tant qu 'ils n 'ont pas reçu d 'acquittement du serveur M2M. De même si c'est le device M2M qui a un comportement défectueux, il peut être amené à transmettre continuellement le même trafic.
- Un très grand nombre de devices M2M perdant la couverture réseau suite à un problème sur une station de base ; ces devices vont tous simultanément changer de réseau qui doit prendre en charge un grand nombre de demandes d 'attachement simultanément et peut être aussi d 'établissement de contextes PDP. En effet, Si l 'opérateur de réseau M2M dispose d 'accords de roaming avec les opérateurs du pays dans lequel se trouve son client, le device M2M peut se rattacher à n 'importe quel opérateur mobile en fonction des signaux reçus.

La surcharge et la congestion sont principalement causées par :

- La transmission simultanée d'un grand nombre de devices M2M à intervalle de temps précis ou suite à un événement

- Le mauvais fonctionnement du device M2M ou du serveur M2M.
- L'indisponibilité du réseau

Il s'agit avant tout de la surcharge et la congestion du plan de contrôle. Bien qu 'Il ne soit pas impensable que des applications M2M puissent générer des volumes de données importants (plan d' usager), en règle générale, le volume généré est faible.

3 Eléments du réseau impactés par la surcharge et la congestion

Les nœuds du réseau cœur qui peuvent souffrir du congestion au niveau du plan contrôle incluent:
Tous les nœuds et gateways du réseau cœur paquet.
Avec un très grand nombre de requête GMM ou EMM Attach Request, le nœud MME/SGSN est très vulnérable. Avec les demandes de connexion data, ces nœuds sont aussi vulnérables car un grand nombre de messages de signalisation sont échangés à partir de ces nœuds pour l 'établissement d 'une connexion data (contexte PDP en 2G/3G et bearer en 4G).
Les gateways GGSN/PDN-GW sont aussi très vulnérables car les applications M2M utilisent généralement un APN dédié qui peut terminer sur un GGSN/PDN-GW. Toutes les demandes de connexion pour cette application doivent alors être prises en charge par ce GGSN/PDN-GW.
Il peut arriver que les devices M2M puissent faire des demandes en parallèle sur une aire de localisation limitée. Dans ce cas, la congestion sur le plan contrôle apparaît dans cette aire sur les liens de signalisation associés et qu 'il n 'y ait pas de congestion générale sur tous les nœuds ou gateways.
Les MSC/VLR ou MSC Server du domaine circuit sont aussi concernés par la congestion. Du fait que les opérateurs doivent configurer les devices M2M afin qu 'ils puissent recevoir des SMS (par exemple pour le déclenchement du device) et compte tenu du fait que très peu d 'opérateurs activent le traitement des SMS par le SGSN, les devices M2M doivent accéder au domaine circuit.
Il est important que les opérateurs mobiles puissent protéger leur réseau contre les problèmes de surcharge et de congestion afin de ne pas dégrader la QoS des services circuit (e.g., voix et SMS) et paquet (e.g., accès à Internet/Intranet) qu 'ils offrent à leurs clients non M2M.
Les éléments d'accès, e.g., l'eNodeB, sont aussi impactés compte tenu du nombre de devices M2M demandant leur prise en charge simultanément.
Dans tous les cas, c'est surtout le plan de contrôle qui est fortement impacté car les devices demandent leur attachement, l'établissement de contexte PDP/bearer, la mise à jour de leur localisation, sans compter les demandes de paging pour su trafic entrant. Sur le plan usager, les devices M2M délivrent en général peu de trafic, même si une forte concentration de ces devices sur une aire particulière peut être problématique si tous ces devices veulent transmettre des données simultanément. Toutefois déjà avec la LTE et demain avec la LTE Advanced les débits d'accès devraient pouvoir contenir les problèmes sur le plan usager.

4 Contrôle de la congestion pour les communications M2M

Il existe deux méthodes pour contrôler la congestion pour les communications M2M

1. Méthode d 'identification des terminaux M2M. 3GPP a classifié la communication comme pouvant être « low priority » ou « normal priority». Les communications M2M auront donc

dans certains scénariis une priorité basse comparée à celle des communications voix et données qui sera normale. Les devices M2M désignés comme devant avoir une priorité basse auront leur LAPI (Low Access Priority Indicator). Le LAPI peut être configuré au moment de la production du terminal par le constructeur ou peut être positionné à distance par l 'opérateur via la technologie OTA (Over The Air) ou par un autre moyen. Le LAPI est défini pour toutes les technologies d 'accès Radio 3GPP : 2G, 3G et 4G.

2. Méthode de contrôle de la congestion dans le réseau
   - Backhoff SM : Permet d'interdire, pendant la congestion réseau, aux devices M2M de basse priorité d'émettre du trafic de données,
   - Backoff MM ; Permet d'interdire, pendant la congestion réseau, aux devices M2M de base priorité d'émettre des demandes de gestion de mobilité telles d'attachement ou de mise à jour de localisation,
   - Backoff RRC : Permet d'interdire, pendant la congestion d'accès, aux devices M2M de basse priorité de disposer d'établir des connexion RRC avec l'eNodeB,
   - Fonctions de réduction de la signalisation : Parmi les solutions pour réduire la signalisation figurent l'extension de la valeur du temporisateur T3412, importante notamment pour les devices M2M avec mobilité réduite ou sans mobilité. Elle permet de réduire la charge de la signalisation MM relation à la mise à jour de localisation.

4.1 Identification des devices M2M dans le réseau data mobile

Lors de l'attachement au réseau, l'UE émet un message EMM Attach Request au MME (réseau 4G) ou SGSN (réseau 2G/3G) pour un attachement au réseau paquet. Le message **EMM Attach Request** contient un élément d'information appelé **Device Properties** sur 1 octet. Si le bit 1 est positionné à 0, l'UE n'est pas configuré pour la basse priorité de la signalisation NAS (MS is not configured for NAS signalling low priority). Si le bit 1 est positionné à 1, l'UE est configuré pour la basse priorité de la signalisation NAS (MS is configured for NAS signalling low priority.
Le réseau utilise cet élément d'information *Device properties* pour la gestion de la congestion dans le réseau cœur et pour les aspects taxation.

Si Devices Properties est positionné à « priorité basse pour la signalisation d 'accès » dans le message EMM ATTACH REQUEST , alors la demande d 'établissement de default bearer (ESM PDN Connectivity request) incluse dans le message EMMM Attach Request contient la même information. La demande GTPv2-C CREATE SESSION REQUEST échangée entre les éléments du réseau SGSN/MME → SGW → PGW inclut quant à elle un élément d 'information « signaling priority indication » positionné à « priorité d 'accès basse » ; il s'agit du LAPI. Le LAPI (Low Access Priority Indicator) permet en cas de congestion de traiter en priorité la signalisation et le trafic usager des terminaux dont la priorité n'est pas basse. Il est aussi possible en cas de congestion de ne pas accepter les terminaux de basse priorité.

La figure 1 illustre l'attachement au réseau 4G d'un objet M2M ayant une priorité d'accès basse.

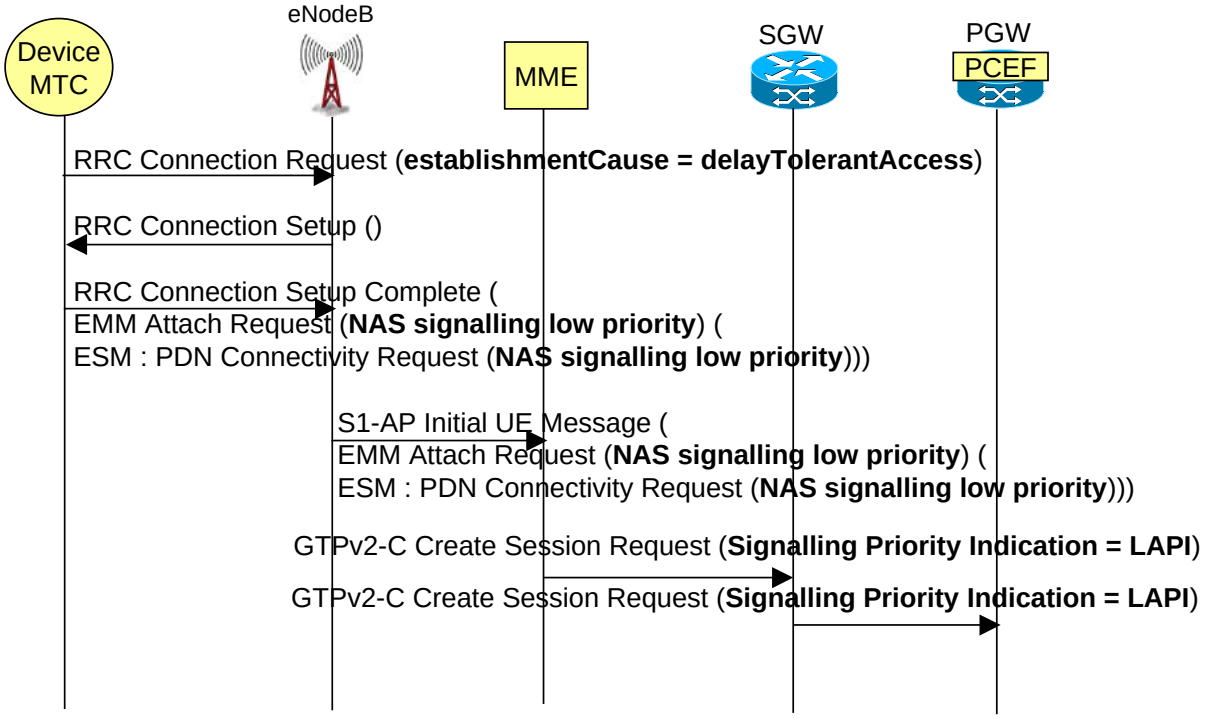

Figure 1. Procédure d'attachement d'un device M2M de priorité d'accès basse

4.2 Contrôle de la congestion réseau : Back-off SM

Le Back-off SM (Session Management) a lieu lorsqu'une congestion réseau est observée. Il permet d 'empêcher momentanément le terminal M2M de transmettre ou de recevoir des paquets. Lorsque l'UE veut établir un bearer pour transmettre des paquets, il doit échanger de la signalisation SM (Session Management).

1. Le terminal M2M demande l 'ouverture d 'un bearer pour l 'envoi de ses données via le message ESM PDN Connectivity Request). Ce dernier contient l'élément d'information Device properties permettant d'indiquer que l'UE est configuré pour la priorité basse pour la signalisation NAS

2. et 3. Le MME relaie la demande au PGW via le SGW mais indique dans le message GTPV2-C Créate Session Request via l 'élément d 'information Signaling Priority Indication le LAPI. Il s 'agit du Low Access Priority Indicator.

4. et 5. Le PGW constate une congestion à sa niveau. Il rejette donc la demande. Le MME reçoit via le SGW la réponse du PGW, à savoir, GTPv2-C Create Session Response, contenant les éléments d 'information Reject Cause et PGW Back-off Time).

6. Le MME retourne au device M2M une réponse ESM PDN Connectivity Reject contenant la reject cause à savoir 26 qui signifie insufficient resources. Par ailleurs, un élément d 'information T3396 qui correspond au « PGW Back-off Time » est inclus. Le device M2M ne peut pas envoyer un nouveau message ESM PDN Connectivity Reject pour cet APN avant l 'expiration du temporisateur T3396.

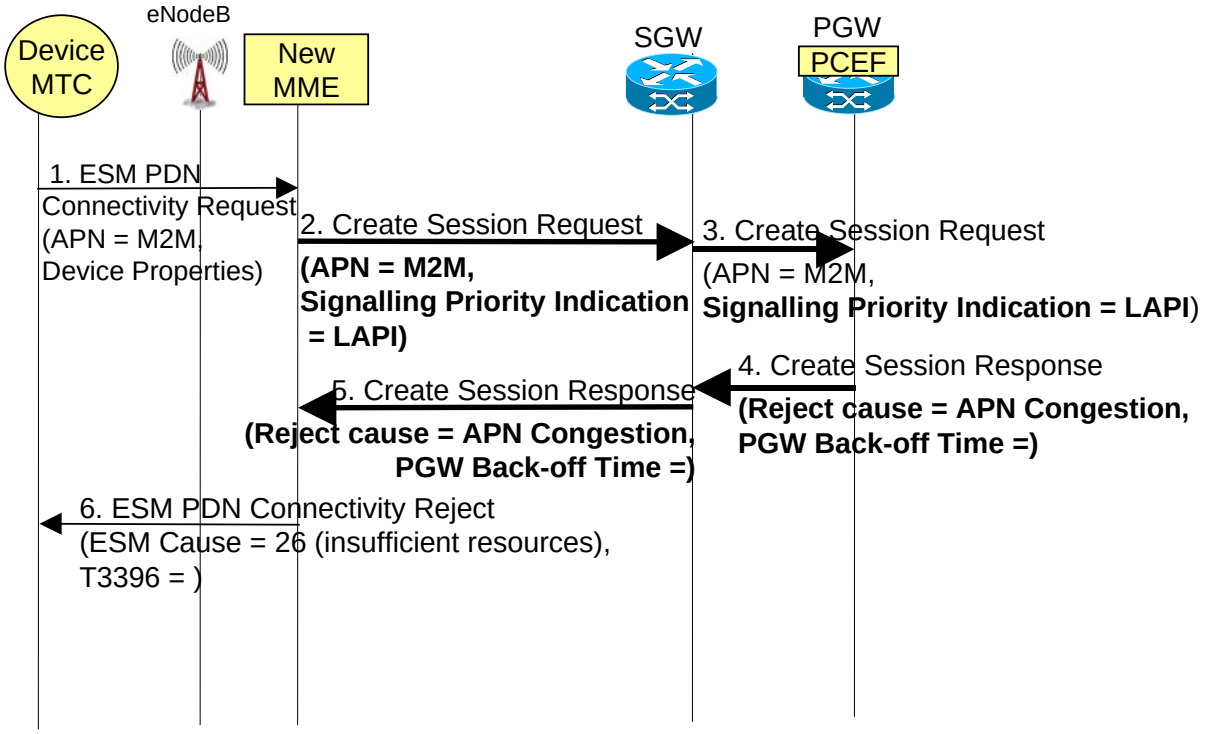

Figure 2 : Back-off SM

4.3 Contrôle de la congestion réseau : Back-off MM

Le Back-off MM (Mobility Management) a lieu lorsque le MME/S4-SGSN/SGSN ne peut accepter une demande d 'attachement ou de mise à jour de Tracking/Routing Area car une congestion est observée. Il s'agit des procédures de mobility management (MM). Le MME/S4-SGSN/SGSN retourne alors une réponse de reject à l 'UE contenant un back-off time.

1. Le terminal M2M envoie une demande EMM d 'attachement EMM au MME en indiquant une basse priorité dans l'élément d'information « Device properties ».
2. LE MME rejette la demande et indique un back-off time via le temporisateur T3346 . Le terminal M2M ne doit donc pas tenter de s 'attacher de nouveau tant que le temporisateur T3346 n 'a pas expiré.

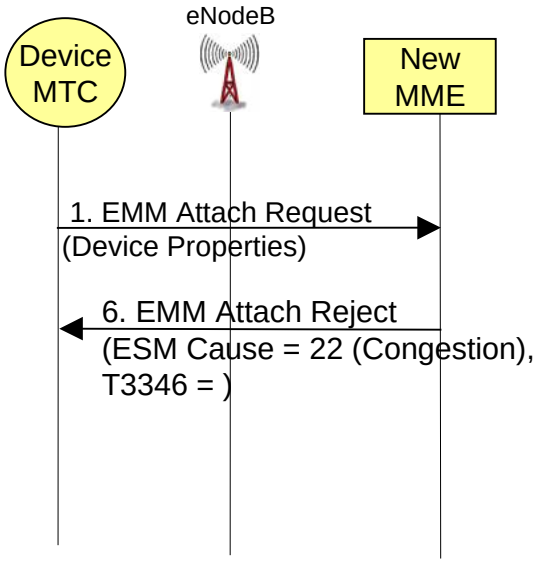

Figure 3 : Back-off MM

4.4 Contrôle de la congestion d'accès : Back-off RRC

Le Back-off RRC a lieu lorsque l 'eNodeB reçoiut une demande de connexion RRC pendant une situation de congestion. La demande indique que le device a une priorité basse. La demande du terminal M2M est rejetée et la réponse de l 'eNodeB contient la rejection Cause positionné à « Congestion » et le back-off time via l 'élément d 'information ExtendedWaitTime dont la valeur est comprise entre 1 et 1800 secondes. Sans connexion RRC le device ne peut émettre ni message MM, ni message SM à son MME/SGSN.

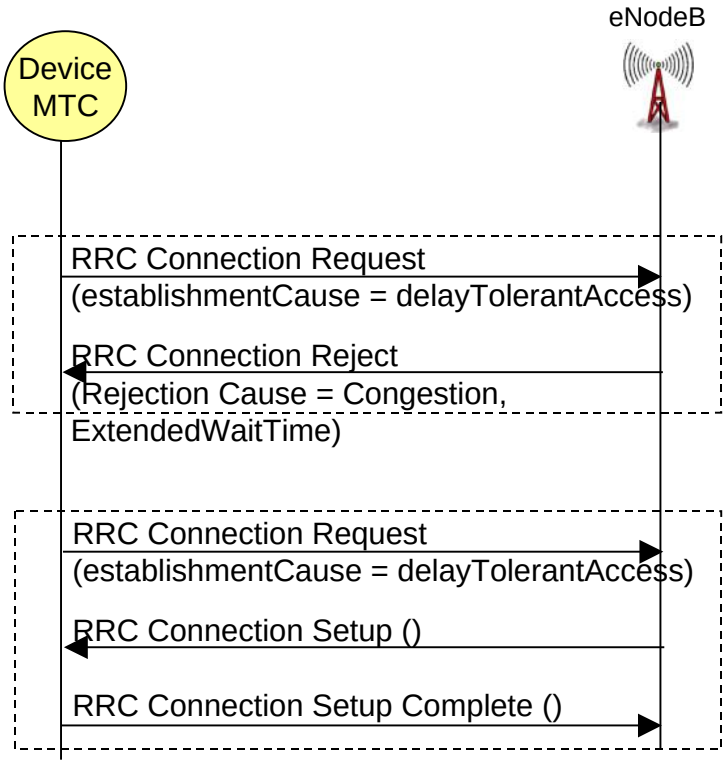

Figure 4 : Back-off RRC

4.5 Contrôle de congestion réseau préventif (trafic uplink)

L 'indication de priorité d 'accès basse permet aux nœuds d 'accès (eNoeB, RNC) et aux nœuds du réseau coeur (MSC Server, MME, SGSN, SGW et PGW) de décider d 'accepter ou pas la demande d 'établissement de connexion RRC ou la requête NAS sur la base de la charge courante du réseau. Les nœuds d 'accès et de réseau qui font face à une surcharge peuvent rejeter les requêtes des devices ayant indiqué une priorité d 'accès basse avant de rejeter les requêtes des devices qui ne sont pas concernées pas la priorité d 'accès basse.
Un MME concerné par la surcharge peut aussi demander au réseau d 'accès de restreindre l 'accès au devices qui ont été configurés avec une priorité d 'accès basse en émettant un message "OVERLOAD START" (Figure 5) à un ensemble d ' 'eNodeB appropriés. Si nécessaire, le MME peut aussi demander le rejet des requêtes d 'établissement de connexion RRC pour les devices qui n 'ont pas été configurés avec la priorité d 'accès basse, c 'est à dire rejeter les requêtes ne concernant pas le type « emergency » ou le type «high priority ».
Le message OVERLOAD START contient un IE Overload Action positionné à :
"reject RRC connection establishments for non-emergency mobile originated data transfer" (i.e., reject traffic corresponding to RRC cause "mo-data" and "delayTolerantAccess" ou
"reject RRC connection establishments for signalling" (i.e., reject traffic corresponding to RRC cause "mo-data", "mo-signalling" and "delayTolerantAccess" ou "only permit RRC connection establishments for emergency sessions and mobile terminated services" (i.e.,

only permit traffic corresponding to RRC cause “emergency” and “mt-Access” ou “only permit RRC connection establishments for high priority sessions and mobile terminated services” (i.e., only permit traffic corresponding to RRC cause “highPriorityAccess” and “mt-Access” ou “reject only RRC connection establishment for delay tolerant access” (i.e., only reject traffic corresponding to RRC cause “delayTolerantAccess”

L ’eNodeB rejette la demande d ’établissement de connexion RRC pour les devices ayant une priorité d ’accès comme décrit à la figure 4.
Losque le MME a pu résoudre son problème de surcharge et souhaite accroître sa charge concernant les devices configurés pour une priorité d ’accès basse, il émet un message “Overload Stop” aux eNodeBs concernés.
Le mécanisme décrit ici permet le contrôle et si nécessaire le rejet du trafic de signalisation montant émis par le device.

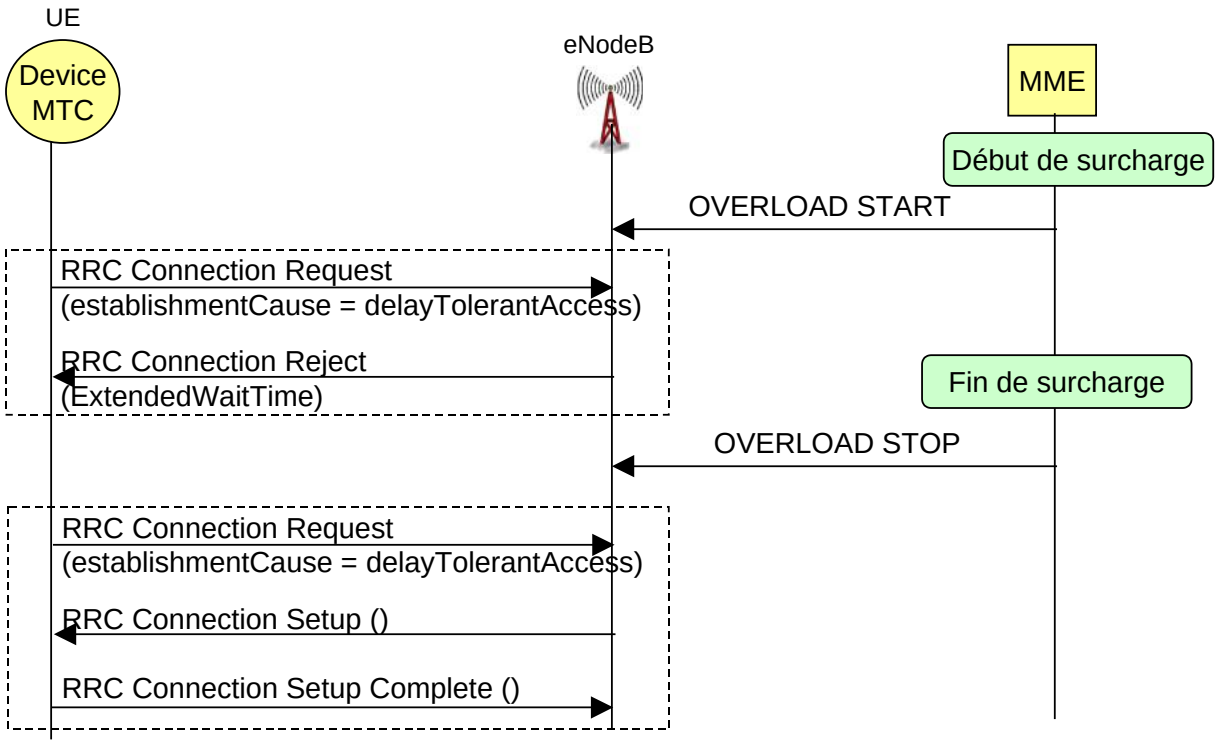

Figure 5 : Procédure de surcharge afin de restreindre l ’accès réseau aux UEs de priorité d ’accès basse

4.6 Contrôle de congestion réseau préventif (trafic downlink)

Il existe aussi un mécanisme permettant de protéger le MME suite à une réception de trafic descendant très important sur le plan usager émis par les serveurs M2M à destination des devices M2M dont la priorité d ’accès est basse. Lorsqu ’il un trafic descendant arrive au Serving GW alors que le device est en mode idle, il est nécessaire de réaliser l ’opération de paging même s ’il dispose d ’un bearer permanent. En effet le E-RAB est automatiquement libéré par l’eNodeB lorsque le device est en mode idle (le device n’a plus de trafic de données sur le plan usager à envoyer ou recevoir). La procédure de paging est demandée par le Serving GW au MME (message Downlink Data Notification, DDN) qui la réalise en émettant une demande de paging à l ’ensemble des eNodeB de la Tracking Area dans laquelle se trouve le device. Un MME qui identifie une situation de surcharge peut restreindre

la charge de signalisation générée par les Serving GWs suite à la réception par ces derniers de trafic entrant sur le plan usager.

Le mécanisme est décrit à la figure 6.

Lorsque le Serving GW reçoit le trafic entrant sur le plan usager à destination d 'un device en mode idle, il émet une requête DDN au MME. Le MME peut rejeter les requêtes DDN concernant des devices ayant une priorité d 'accès basse ou demande au Serving GW de rejeter un pourcentage des requêtes DDN concernant des devices ayant une priorité d 'accès basse pour une durée donnée.

Les Serving GW et PDN GW déterminent qu 'un bearer concerne une priorité basse d 'accès en fonction de son niveau d 'ARP (Allocation and Retention Priority). Le paramètre ARP est reçu par le MME dans la requête DDN. C 'est une politique d 'opérateur de définir des niveaux d 'ARP considérés comme de priorité basse d 'accès.

Lorsque le Serving GW décide de ne pas envoyer le message DDN au MME (selon le pourcentage décidé par le MME), il rejette les paquets IP entrants concernés . Le Serving GW se remet à fonctionner normalement et à envoyer les DDN au MME après la durée de rejet de DDN spécifiée par le MME.

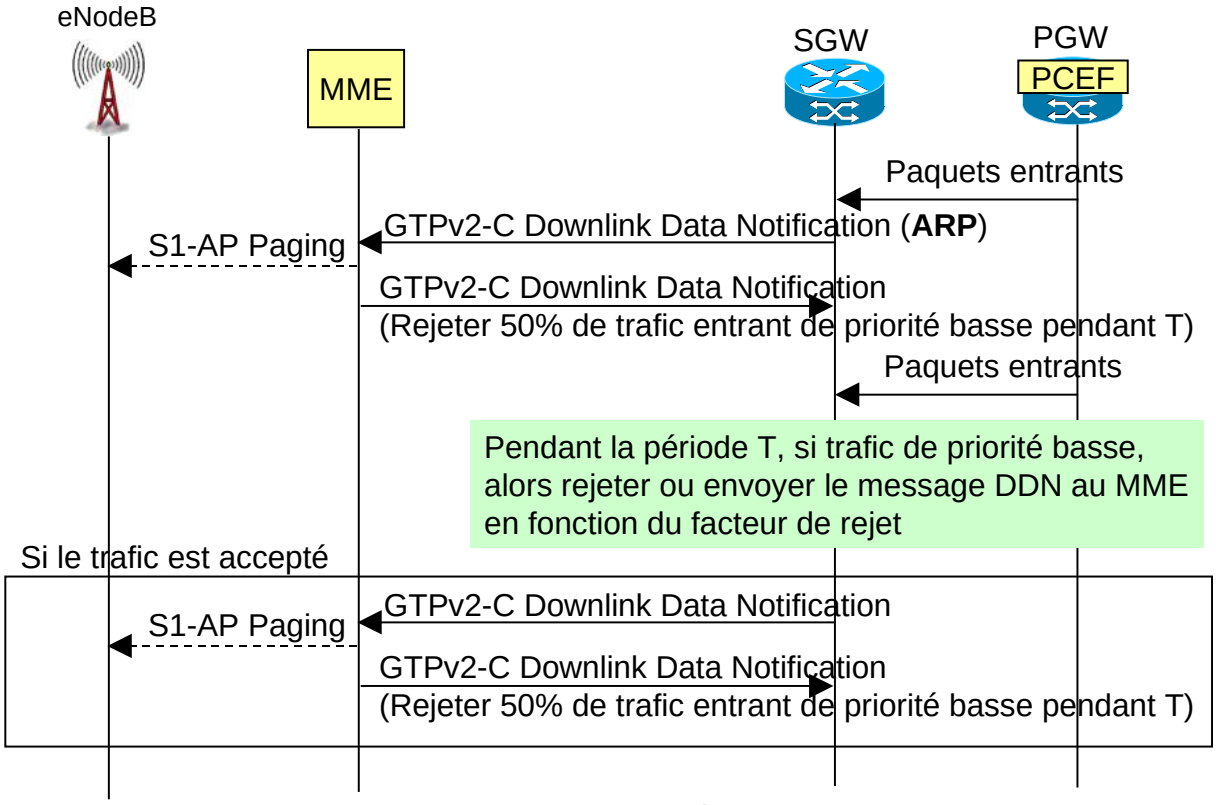

Figure 6 : Rejet des DDNs pour du trafic basse priorité reçu pour des devices MTC dans l 'état Idle

4.7 Fonctions de réduction de la signalisation

Parmi les solutions pour réduire la signalisation figurent l'extension de la valeur du temporisateur T3412, importante notamment pour les devices M2M avec mobilité réduite ou sans mobilité. Elle permet de réduire la charge de la signalisation MM relation à la mise à jour de localisation.

Le Temporisateur T3412 est retourné à l 'UE dans la réponse GMM/EMM Attach Accept lors de son attachement au réseau. Sa valeur par défaut retournée par un MME est 54 mns, et sa valeur maximum est 184 mns.

Lorsqu ’il n ’y a plus de connexion dédiée entre l ’UE et le réseau, l ’UE décrémente ce temporisateur. Avant qu ’il n ’expire, l ’UE doit émettre un message Tracking/Routing Area Update (TAU/RAU) à sont MME/SGSN.
Si le temporisateur expire sans que l ’UE n ’émette de TAU/RAU, l ’UE est considéré par le réseau comme implicitement détaché.
Si l ’UE rétablit une connexion avec le réseau (soit pour envoyer du trafic sur le plan de contrôle, soit du trafic sur le plan usager), alors le temporisateur T3412 repasse à sa valeur négociée lors de l ’attachement ou lors de la procédure TAU/RAU.
Pour minimiser le nombre de TAU/RAU échangés, notamment lorsque l ’UE est un device M2M sans mobilité ou avec mobilité réduite, une valeur étendue peut être retournée pour le temporisateur T3412, dont la valeur maximum est 310 heures.

Références

3GPP TS 24.301, Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 12)
3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 12)
3GPP 29.274, Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 12)

La formation EFORT « M2M : Marché, Applications, Services et Architectures » fournit toutes les clés de compréhension du monde M2M et montre l’architecture réseau mobile nécessaire pour supporter le business M2M de demain.