INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Etude comparative des protocoles MAC pour les réseaux de capteurs sans fil

Tom Lassalle

Table des matières

1. Introduction

1.1. Contexte général

Les réseaux de capteurs sans fil (WSN, Wireless Sensor Networks) sont devenus progressivement omniprésents dans notre environnement, permettant le déploiement de services innovants tels que la détection d'incendie à l'aide de capteurs LoRaWAN auto-alimentés, capables de déclencher des alertes quasi instantanées [1]

Ces capteurs fonctionnent souvent avec des batteries et peuvent parfois être installés dans des environnements difficiles, rendant leur recharge problématique. L'objectif central dans les réseaux de capteurs sans fil est donc la maximisation de la durée de vie du nœud et du réseau. La consommation d'énergie constitue ainsi un enjeu majeur dans les WSN. Son optimisation – qu'il s'agisse de la réduction des collisions, de l'écoute inutile ou des interférences – est essentielle pour maintenir une consommation d'énergie acceptable. [3]

La couche MAC (Medium Access Control) gère l'accès au média et contrôle ainsi la mise en veille et l'activation de la radio, le composant le plus énergivore du capteur. La couche MAC est donc le niveau le plus adapté pour mettre en œuvre des mécanismes d'économie d'énergie, tout en optimisant les autres performances, telles que la préservation d'un débit acceptable, la minimisation de la latence et l'évitement des collisions. [2]

La conception d'une couche MAC est particulièrement délicate, car elle nécessite de résoudre des problèmes complexes, notamment ceux liés à la synchronisation, aux collisions, et aux interférences externes. L'étude et la comparaison de ces protocoles sont essentielles : elles permettent de comprendre les compromis réalisés entre efficacité énergétique, performance de communication

1.2. Objectif du rapport

Ce rapport a donc pour objectif d'étudier et d'analyser différents protocoles de contrôle d'accès au canal (MAC) tous dédié aux réseaux sans fil de capteurs (WSN, Wireless Sensor Networks) en exposant leur fonctionnement et leur performance.

1.3. Plan du document

Dans un premier temps, nous aborderons la classification des protocoles MAC utilisés dans les réseaux de capteurs sans fil. Ensuite, nous présenterons la méthodologie d'analyse, où nous détaillerons les approches et critères qui ont guidé l'étude ainsi que l'évaluation des différents protocoles.

La partie principale de ce document est dédiée à une étude approfondie des protocoles MAC. Cette section a été structurée en plusieurs sous-parties, en fonction des différents types de protocoles. Après avoir étudié chaque protocole, nous procéderons à une analyse comparative afin de les évaluer selon divers critères. Un tableau récapitulatif viendra ensuite illustrer de manière claire et concise les différences entre les protocoles.

2. Classification des protocoles MAC pour le WSN

Il existe plusieurs classifications dans la littérature, basées par exemple sur le duty cycling et la collecte d'énergie [4]. La classification présentée dans [3] a été retenue, car elle offre une vue structurée des protocoles MAC en fonction de leurs mécanismes de synchronisation. Ces protocoles sont classés en quatre catégories : « Asynchrone », « synchronisation locale », « synchronisation globale » et « multi-canaux », comme illustré dans la figure 1.

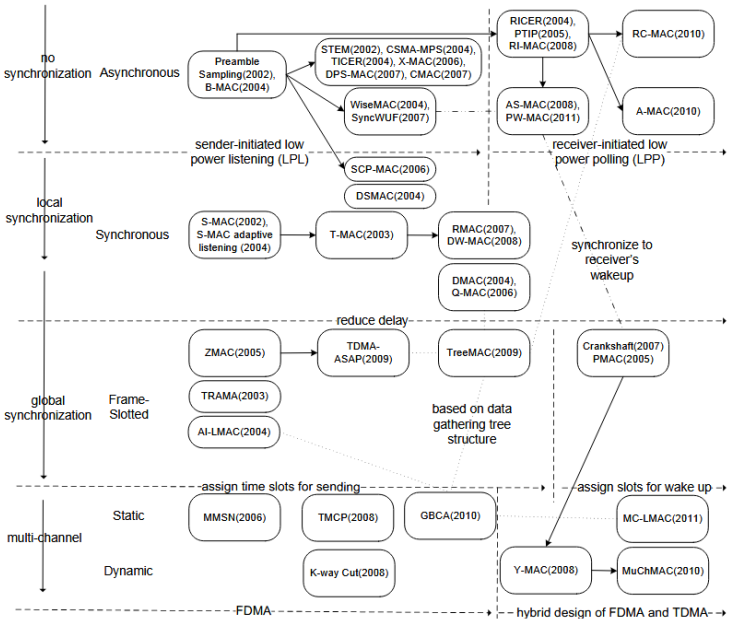

Figure 1 : Classification de protocole MAC WSN [3]

3. Méthodologie d'analyse

Chaque protocole MAC analysé dans le cadre de cette étude sera évalué en fonction d'un ensemble de critères permettant d'analyser ses performances et son adéquation aux exigences des réseaux de capteurs sans fil.

1. Le type d'accès au canal

Les protocoles de communication peuvent gérer le partage de l'accès physique de différentes manières : soit de manière aléatoire, en utilisant des mécanismes de détection de porteuses ou de collisions, comme dans le cas du CSMA/CD (Carrier Sense Multiple Access / Collision Detection).

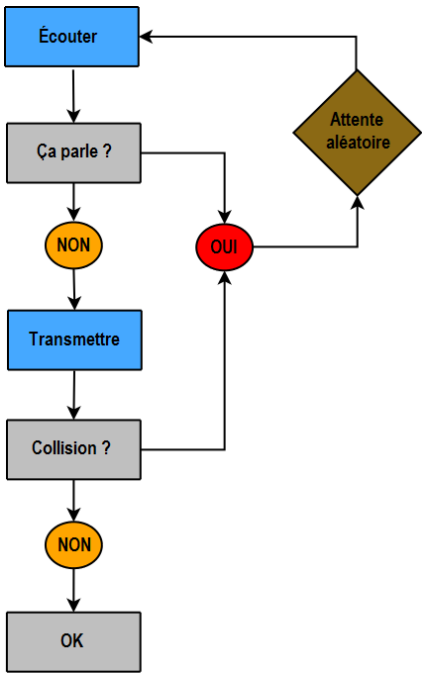

Figure 2: Diagramme de l'algorithme CSMA/CD [5]

Ou de manière déterministe, en séparant l'accès au média selon la fréquence (FDMA), le temps (TDMA) ou le code (CDMA), afin de minimiser les risques de collision. Certains protocoles comme le Z-MAC combinent ces deux approches pour optimiser la gestion de l'accès au medium.

2. Synchronisation

Les nœuds peuvent ou non partager une horloge commune dans ce cas, ils sont dits synchrones. La synchronisation permet de coordonner le temps entre plusieurs nœuds du réseau, afin qu'ils puissent collaborer de manière efficace (par exemple, pour se réveiller simultanément).

Il existe plusieurs approches de synchronisation, telles que la synchronisation locale, où des nœuds regroupés en clusters possèdent une horloge commune, ou encore la synchronisation globale, où une horloge unique est partagée par tous les nœuds du réseau [3].

3. Localisation

Aucun des protocoles analysés au cours de ce rapport n'intègre directement un processus de localisation. Cependant, il existe certains protocoles pouvant prendre en charge ou faciliter l'intégration d'un mécanisme de détermination de position, ce qui permet à un nœud de se localiser et de déterminer la position d'autres nœuds.

Il existe plusieurs méthodes de localisation, telles que celles basées sur la portée, qui utilisent des techniques comme le RSSI (Received Signal Strength Indicator) ou le ToA (Time of Arrival) pour calculer la distance entre les nœuds. Ces informations peuvent ensuite être exploitées par des méthodes comme la trilatération. D'autres approches reposent sur l'utilisation de la distance en "sauts" pour déterminer la position des nœuds [6].

4. Mécanismes de sécurité

La couche MAC (Medium Access Control) gère l'accès au médium partagé. Certaines attaques visent directement cette couche, telles que :

- Spoofing d'adresse MAC : un attaquant usurpe l'identité d'un appareil légitime.
- DoS (Denial of Service) : saturation du canal par des requêtes excessives.
- Man-in-the-Middle : interception des trames avant qu'elles n'atteignent la couche supérieure.

Dans les réseaux traditionnels, des mécanismes de sécurité tels que le chiffrement (WPA2/WPA3) et l'authentification sont utilisés pour garantir la confidentialité et l'intégrité des données. Cependant, les problématiques de sécurité dans les réseaux sans fil (WSN) sont particulièrement complexes. En effet, les mécanismes de sécurité exigent souvent une puissance de calcul, du temps de traitement et une consommation d'énergie, ce qui va à l'encontre des

principes de base des réseaux sans fil, où l'efficacité énergétique est primordiale. Par conséquent, l'intégration de ces mécanismes dans les WSN est particulièrement difficile.

Les protocoles abordés dans ce rapport ne bénéficient pas de mécanismes de sécurité spécialement intégrés. Toutefois, certains, en raison de leur architecture intrinsèque, offrent une sécurité améliorée par rapport à d'autres.

5. Mobilité des nœuds

Un WSN peut être amené à évoluer, en particulier dans des applications où les nœuds sont associés à des objets mobiles, tels que des patients, des travailleurs sur des sites dangereux ou des soldats en mission. La mobilité des nœuds permet de suivre les déplacements et de réagir rapidement aux changements, qu'il s'agisse de défaillances de certains nœuds ou de l'ajout de nouveaux nœuds. Toutefois, cette mobilité peut également affecter la connectivité du réseau et la qualité des communications entre les nœuds.

La mobilité dans les WSN peut être catégorisée en plusieurs formes, en fonction du type de mouvement des nœuds et de la fréquence de ces déplacements. Ces catégories incluent :

- Mobilité faible : Ce cas fait référence à des changements sporadiques dans la topologie du réseau, généralement dus à l'ajout ou à la défaillance de nœuds existants. Les déplacements sont peu fréquents et souvent liés à des modifications ponctuelles du réseau.
- Mobilité forte : Dans ce cas, les nœuds se déplacent de manière dynamique et rapide. Cela peut inclure des nœuds affectés par des facteurs externes tels que le vent ou l'eau, ou des nœuds attachés à des objets mobiles (par exemple, des patients, des travailleurs, etc.). Les déplacements fréquents des nœuds entraînent des changements réguliers de la topologie du réseau.

Lorsque la mobilité des nœuds devient plus importante, plusieurs défis émergent, tels que la perte de liens, la retransmission des paquets et les conflits de transmission. Ces problèmes nécessitent des mécanismes adaptés pour maintenir une communication fiable et une connectivité optimale au sein du réseau [7]

6. Consommation énergétique

Dans de nombreux cas, les batteries des capteurs WSN ne peuvent pas être facilement remplacées ou rechargées en raison des environnements difficiles ou inaccessibles dans lesquels

ces réseaux sont déployés (par exemple, sous l'eau, dans des zones éloignées ou sur de grandes structures comme des ponts ou des bâtiments élevés). De plus, l'un des objectifs principaux des WSN est d'optimiser leur durée de vie tout en maintenant leur fonctionnalité. L'efficacité énergétique des nœuds joue un rôle crucial pour prolonger la durée de vie des capteurs sans nécessiter d'interventions physiques [8].

C'est pourquoi nous chercherons à analyser la consommation énergétique des différents protocoles. Toutefois, pour certains protocoles MAC, il existe peu de données et de mesures sur leur consommation. De plus, il est difficile de trouver des études utilisant un protocole d'estimation énergétique comparable, ce qui complique la comparaison des divers protocoles énergétiques. Afin d'obtenir une vue d'ensemble plus complète et réaliste de la comparaison énergétique des protocoles analysés, il serait nécessaire de mettre en place un même protocole expérimental et de réaliser des mesures sur une plateforme expérimentale commune.

4. Étude des protocoles

4.1. Les protocoles asynchrones

Dans cette partie, nous présenterons les protocoles MAC dits asynchrones. Un protocole MAC est qualifié d'asynchrone lorsque chaque nœud choisit librement son propre cycle d'activité, c'est-à-dire son propre horaire de réveil, sans nécessiter de synchronisation globale avec les autres nœuds. Dans un réseau de capteurs sans fil, les nœuds sont généralement alimentés par batterie. Pour maximiser leur autonomie, ils doivent rester en mode veille le plus longtemps possible afin d'économiser l'énergie. En permettant à chaque nœud de définir indépendamment son horaire d'activité, on évite le coût énergétique associé à la synchronisation avec les nœuds voisins. Cette indépendance rend possible l'obtention de cycles d'activité extrêmement faibles. Cependant, une problématique majeure apparaît : comment un nœud souhaitant envoyer un message peut-il s'assurer de rencontrer le nœud destinataire, qui reste endormi la plupart du temps ?

Une solution consiste à utiliser un mécanisme d'annonce de transmission : avant l'envoi des données, l'émetteur transmet un préambule suffisamment long pour que le récepteur ciblé ait le temps de se réveiller et de détecter le message.

Dans cette section, nous analyserons, selon la méthodologie décrite dans la section 3, le protocole B-MAC ainsi que l'une de ses évolutions : le protocole S-MAC.

4.1.1. B-MAC

Le protocole MAC, appelé B-MAC (Berkeley MAC), a été proposé en 2004 par des chercheurs de l'Université de Berkeley, spécifiquement pour les réseaux de capteurs sans fil, notamment dans le cadre des applications de surveillance environnementale. Son objectif principal est de concevoir un protocole à très faible consommation d'énergie, tout en garantissant de bonnes performances en termes de débit et de latence, grâce à la reconfiguration dynamique du MAC [9].

Accès au canal :

Le protocole B-MAC repose sur l'utilisation d'une forme de CSMA (Carrier Sense Multiple Access), combinée à un mécanisme de CCA (Clear Channel Assessment). Dans le cadre de B-MAC, chaque nœud écoute périodiquement le canal, ce qui permet de minimiser la consommation d'énergie.

A chaque période :

1. Le nœud se réveil pendant quelques millisecondes
2. Effectue son CCA pour détecter une activité (le préambule).
    a. Si le canal est libre, il peut se rendormir
    b. Dans le cas contraire, il doit rester éveillé pour recevoir le paquet

Le CCA repose sur le principe suivant : il mesure le niveau d'énergie à la fréquence de fonctionnement des nœuds. Si ce niveau est supérieur au bruit de fond, le canal est considéré comme occupé. Ce mécanisme permet de réduire le nombre de collisions sur le canal.

Le CCA de la B-MAC est une version améliorée de ce principe. Chaque nœud prélève d'abord des échantillons de puissance du signal à des moments où le canal est supposé libre (par exemple, immédiatement après avoir transmis une trame). Ces échantillons sont stockés dans une pile, et la médiane de cette pile est utilisée comme entrée d'une fonction de moyenne mobile exponentiellement pondérée, afin d'estimer le niveau de bruit ambiant.

Envoie d'un message :

Lorsque le nœud souhaite envoyer un message :

1. Il effectue un CCA afin de vérifier si le canal est libre
2. S'il l'est, il transmet un préambule supérieur à la période de sommeil suivit du paquet qu'il souhaite envoyer.

Dans le cas de la réception d'un message, c'est-à-dire de la détection d'un préambule, le récepteur reste éveillé plus longtemps afin de recevoir la trame dans son intégralité. Ce mécanisme est appelé LPL (Low Power Listening), car le nœud ne s'éveille pour écouter que lorsque cela est nécessaire, ce qui permet ainsi de réduire la consommation énergétique [8].

Synchronisation

Le protocole B-MAC est un protocole asynchrone, ce qui signifie qu'il ne dispose d'aucun mécanisme de synchronisation. Chaque nœud fonctionne indépendamment en se basant sur sa propre horloge pour se réveiller périodiquement. Ainsi, ce protocole compense l'absence de synchronisation en utilisant des mécanismes d'accès au canal, comme mentionné précédemment.

Localisation

La B-MAC n'inclut pas par défaut de moyen de localisation. Cependant il ne donc pas possible d'intégrer à ce protocole réaliser une localisation par TOA (Time of Arrival), car le système est asynchrone et ne dispose donc pas de référence temporelle commune.

Mécanismes de sécurité

Le protocole B-MAC est un protocole MAC simple et léger, conçu pour minimiser la consommation énergétique. En raison de sa simplicité, il ne comporte aucun mécanisme de sécurité intégré, ce qui le rend vulnérable à plusieurs types d'attaques. Parmi les vulnérabilités possibles, on trouve notamment :

Jamming Attack : Le B-MAC est particulièrement sensible au brouillage, car il est facilement ciblable. En effet, en raison de son préambule long, il est aisé de détecter l'origine de l'émission et de la cibler pour perturber la communication.

Mobilité des nœuds

Aucun mécanisme de mobilité de nœud n'est décrit dans [9], mais la mobilité des nœuds ne semble pas poser de problème, car le protocole B-MAC n'intègre pas de mécanisme de

synchronisation. Ainsi, le nœud n'a pas besoin d'échanger de messages lorsqu'il change de voisin. Il peut donc immédiatement communiquer avec tout nœud à portée.

Consommation énergétique

Afin de calculer la durée de vie d'un nœud, l'étude [9] propose une estimation de la consommation globale d'énergie. Pour le protocole B-MAC, l'énergie utilisée par un nœud inclut plusieurs composants : l'énergie consommée lors de la réception, de la transmission, de l'échantillonnage périodique du canal radio via le mécanisme de Low Power Listening (LPL), ainsi que l'énergie dépensée pendant les périodes de sommeil.

$$E = E_{rx} + E_{tx} + E_{listen} + E_{sleep}$$

Propose la table suivante :

Opération	Temps (s)	Courant (mA)
Initialisation radio (b)	350×10^{-6}	6
Mise sous tension radio (c)	1.5×10^{-3}	1
Passage en RX/TX (d)	250×10^{-6}	15
Échantillonnage radio (e)	350×10^{-6}	15
Évaluation échantillon (f)	100×10^{-6}	6
Réception 1 octet	416×10^{-6}	15
Transmission 1 octet	416×10^{-6}	20
Échantillonnage capteurs	1.120	—

Cette dernière a été obtenus à travers de mesures expérimentales sur les nœuds Mica2 avec radio CC1000. Chaque opération (initialisation, mise sous tension, RX/TX, échantillonnage, réception, transmission) a été chronométrée et son courant mesuré.

L'étude propose également les hypothèses suivantes :

- **L_preamble = 271 octets**, **L_packet = 36 octets** (taille des trames B-MAC).
- **n = 10** (taille du voisinage).
- **r = 1/300 s^{-1}** (un paquet toutes les 5 min).
- **t_i = 100 ms** (intervalle de vérification LPL).
- **C_{batt} = 2500 mAh**, **V = 3 V** (batterie AA).

C’est à partir de ces hypothèses que sera estimer la consommation du protocole.

Transmission :

L'énergie consommée lors de la transmission, E_{tx}, est déterminée par le produit de la longueur du paquet, incluant le préambule, et de la fréquence de génération des paquets.

$$t_x = r \times (L_{preamble} + L_{packet}) t_{xb}$$

$$t_x = 3001 \times (271 + 36) \times 416\,\mu s \approx 0.00043 s$$

Et

$$E_{tx} = = 0.00043 \times 20 \times 3 \approx 0.026\ \mathrm{mJ/s}$$

Réception :

L’énergie consommée par la transmission, E_{tx}, est la longueur du paquet avec le préambule multiplié par le taux de génération des paquets :

$$t_{rx} \leq nr(L_{preamble} + L_{packet}) t_{rxb}$$

$$E_{rx} = t_{rx} c_{rxb} V$$

Avec les hypothèses précédemment prises :

$$t_{rx} \leq 10 \times 3001 \times 307 \times 416\,\mu s \approx 0.0043 s$$

$$E_{rx} = 0.0043 \times 15 \times 3 \approx 0.19\,mJ/s$$

Ecoute :

La figure suivante illustre l'implémentation effectuer par l'étude de l’échantillonnage LPL dans le protocole B-MAC, modifié pour réduire au maximum la durée de l’échantillonnage (étape (e))

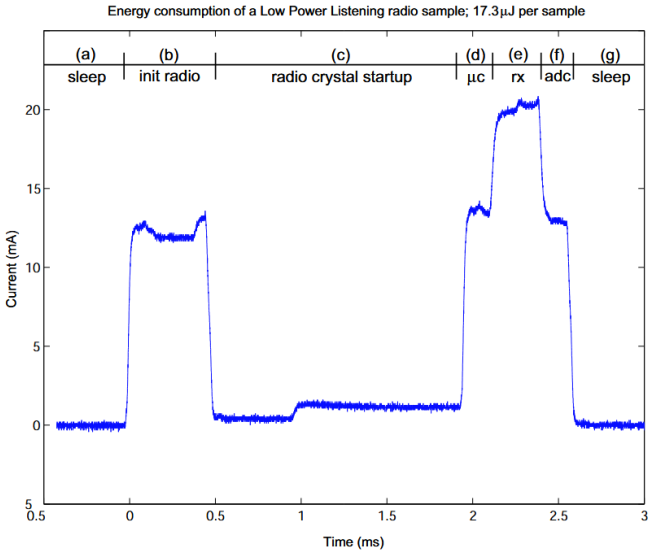

Figure 3 : Mesure de la consommation B-MAC sur un cycle [9]

$$E_{listen} = \frac{17.3}{0.1}\mu J = 0.173mJ/s$$

Veille :

Le nœud doit dormir pour le reste du temps. Le temps de sommeil, t_{sleep}, est simplement le temps restant chaque seconde qui n'est pas consommé par les autres opérations

$$t_{sleep} = 1 - t_{rx} - t_x - t_d - t_{listen}$$

$$E_{sleep} = t_{sleep} \times c_{sleep}$$

$$E_{sleep} \approx (1 - 0.0043 - 0.00043) \times 0.03 \times 3 \approx 0.086mJ/s$$

Total :

$$E \approx 0.026 + 0.19 + 0.173 + 0.086 = 0.475mJ/s$$

B-MAC est particulièrement efficace pour les réseaux à faible trafic et à faible densité, grâce à son mécanisme LPL qui permet d'éviter une écoute continue.

Cependant, dans des réseaux à forte densité ou avec des taux d'échantillonnage élevés, sa consommation d'énergie peut augmenter considérablement en raison des réceptions multiples et de la longueur des préambules.

4.1.2. X-MAC

Le protocole X-MAC est un protocole MAC à faible consommation d'énergie conçu par Michael Buettner, Gary V. Yee, Eric Anderson et Richard Han de l'Université du Colorado.

Certains protocoles MAC asynchrones, tels que le B-MAC, fonctionnent selon une méthode LPL, qui repose sur l'utilisation d'un préambule long. Ce préambule permet aux capteurs récepteurs de rester en mode veille tout en étant capables d'écouter les transmissions, optimisant ainsi la consommation d'énergie.

Cependant, cette approche présente plusieurs inconvénients :

- Latence : La longueur du préambule introduit un délai supplémentaire à chaque communication.
- Consommation d'énergie : Bien que le préambule long aide à économiser de l'énergie en mode veille, sa durée prolongée entraîne une consommation d'énergie non négligeable, notamment au niveau des récepteurs, qui n'ont pas toujours besoin de recevoir des données.

Dans ce contexte, le protocole X-MAC propose une solution en réduisant la durée du préambule. Cela permet de diminuer à la fois la latence et la consommation d'énergie, tout en conservant l'efficacité du mécanisme de veille [10].

Accès au canal

L'accès au medium dans X-MAC repose sur une technique de préambules courts et adressés.

Comme dans B-MAC, X-MAC utilise une écoute périodique du canal : chaque nœud se réveille à intervalles réguliers pour écouter brièvement le canal. S'il détecte une activité, il reste éveillé afin de recevoir la trame ; sinon, il retourne immédiatement en mode sommeil afin d'économiser de l'énergie.

La principale différence avec B-MAC concerne précisément la gestion du préambule. Dans B-MAC, l'émetteur envoie un long préambule continu pour s'assurer que le destinataire se réveillera pendant cette période. X-MAC, au contraire, envoie une séquence de courts préambules, chacun contenant l'adresse du destinataire. Cela permet au nœud ciblé de

reconnaître rapidement que la transmission lui est destinée, sans avoir à écouter le canal pendant toute la durée d'un long préambule [10].

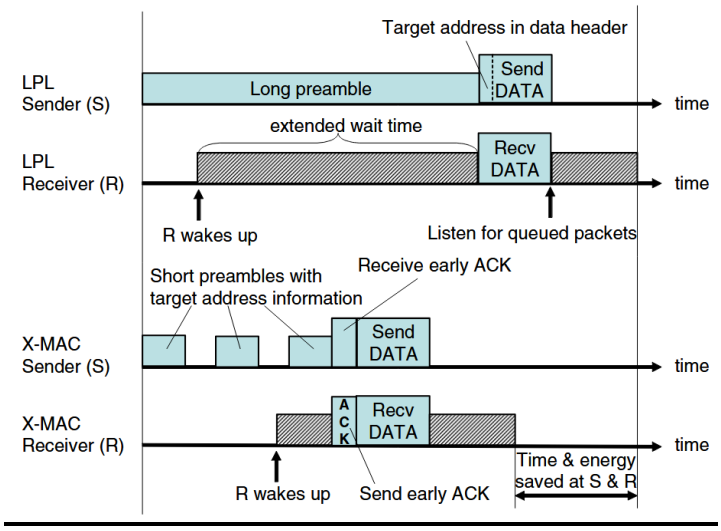

Figure 4 : Comparaison entre le préambule long de LPL et le préambule court de X-MAC [10]

Dès qu'un nœud destinataire détecte un préambule à son adresse, il envoie un ACK anticipé (early ACK) pour indiquer qu'il est prêt à recevoir. L'émetteur interrompt alors immédiatement l'envoi des préambules et transmet directement le paquet de données. Cette stratégie réduit la latence et diminue considérablement la consommation énergétique.

Comme B-MAC, X-MAC s'appuie sur un mécanisme d'accès au medium de type CSMA. Ainsi, si le canal est occupé ou si une collision est détectée, le protocole applique un temps d'attente aléatoire (backoff) avant de retenter une transmission, ce qui limite les risques de conflit entre émetteurs.

Synchronisation

Tout comme le B-MAC le X-MAC est un protocole asynchrone, ce qui signifie qu'il ne dispose d'aucun mécanisme de synchronisation. Chaque nœud fonctionne indépendamment en se basant sur sa propre horloge pour se réveiller périodiquement. Ainsi, ce protocole compense l'absence de synchronisation en utilisant des mécanismes d'accès au canal, comme mentionné précédemment.

Mécanismes de sécurité

À l'instar du protocole B-MAC, le protocole X-MAC est un protocole MAC simple et léger, conçu pour minimiser la consommation énergétique. Cependant, en raison de sa simplicité, il ne comporte aucun mécanisme de sécurité intégré, tel que le chiffrement, l'authentification ou la vérification d'intégrité, ce qui le rend vulnérable à divers types d'attaques.

Mobilité des nœuds

La mobilité ne fait pas partie des cas d'usage privilégiés du protocole X-MAC, bien qu'elle reste possible sous certaines conditions. En effet, X-MAC repose sur l'envoi de préambules courts successifs pour annoncer une transmission. Si le récepteur se déplace et quitte la portée radio entre deux préambules, l'ACK anticipé ne parvient pas à l'émetteur. Celui-ci continue alors inutilement l'envoi des préambules, ce qui entraîne une perte d'énergie, une augmentation de la latence et un risque de congestion.

Ainsi, la mobilité n'est pas incompatible avec X-MAC, mais elle peu dégrader son fonctionnement : augmentation du nombre de retransmissions, ruptures de liens plus fréquentes, et baisse globale de la fiabilité. X-MAC ne reste donc réellement efficace que dans des scénarios de mobilité faible ou lente, pour lesquels la structure des préambules courts n'est pas trop perturbée.

Consommation énergétique

Dans [10] les auteurs quantifient l'énergie consommée par des motes TelosB exécutant les protocoles X-MAC (préambule court) et LPL (préambule long). Pour cela, ils utilisent une mesure directe du courant consommé par chaque mote lors de différents états radio (TX, RX, Idle…).

Plateforme matérielle :

Les mesures ont été réalisées avec des motes TelosB, comprenant :

- Radio : Chipcon CC2420 (data rate : 250 kbps, ISM band : 2.4 GHz)
- Microcontrôleur : TI MSP430 à 8 MHz
- Flash externe : 1 MB
- Connexion USB : utilisée pour alimentation et communication

La radio étant la principale source de consommation énergétique, les mesures se focalisent sur le courant lorsque la radio change d'état.

Protocole expérimentale

Pour mesurer le courant, les auteurs insèrent une résistance de 10 Ω sur la ligne d'alimentation (5V) venant du port USB. Et un oscilloscope qui mesure la tension aux bornes de la résistance.

Il est ensuite extaite la valeur moyenne du courant pour chaque cas :

- radio éteinte
- radio en écoute (RX)
- transmission (TX)
- préambules

Les auteurs ont répété les mesures avec nombre variable de transmetteurs ($1 \rightarrow 9$) avec capture d'échantillons continus pour calculer un courant moyen réel.

Grâce aux mesures de courant issues de l'oscilloscope on peut comparer les le LPL vu précédemment qui possède : des préambules longs et un éveil prolongé des récepteurs et X-MAC qui possède : des préambules court et des réveils plus courts.

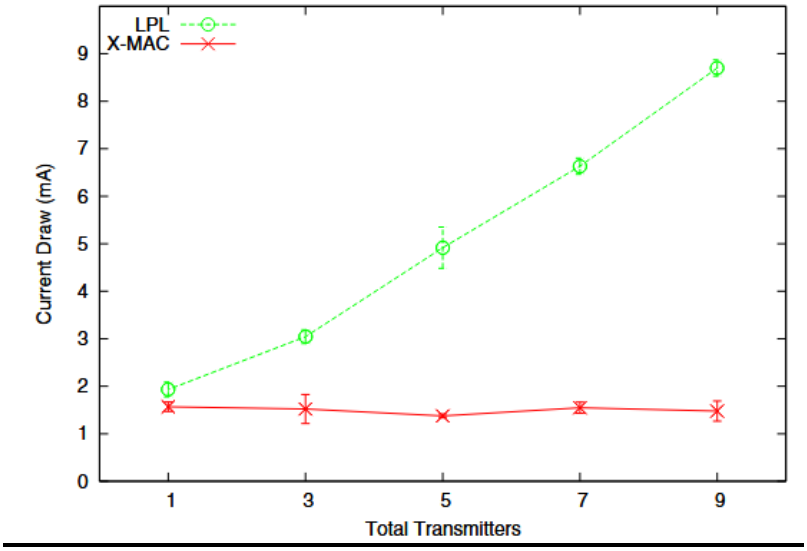

Figure 5 : Consommation électrique par nœud en fonction de la densité [10]

L'utilisation de préambules court, la réduction de la sur-écoute et le réveil anticipé du récepteur permettent à X-MAC de maintenir une consommation stable même lorsque la densité de nœuds augmente. À l'inverse, LPL voit sa consommation s'accroître proportionnellement au nombre de transmetteurs, notamment à cause de ses préambules prolongés et de l'absence d'optimisation du réveil radio. Ainsi, X-MAC se révèle nettement plus efficace énergétiquement pour les réseaux à forte densité.

4.2. Les protocoles synchrones

Dans cette partie, sera présenté les protocoles MAC synchrones. La synchronisation des nœuds leur permet d'aligner leurs périodes d'activité : ainsi, si deux nœuds sont éveillés en même temps, ils peuvent communiquer plus facilement.

Le fonctionnement des protocoles MAC synchrones repose sur le principe suivant : chaque nœud commence par écouter le canal pendant un certain temps. Si un nœud n'entend aucun horaire transmis, il choisit son propre horaire et le diffuse aux autres nœuds, il devient alors synchroniseur. En revanche, si un nœud reçoit l'horaire d'un voisin avant d'avoir choisi le sien, il adopte cet horaire et devient un suiveur. Un ensemble de nœuds se synchronisant autour d'un même synchroniseur forme ainsi un cluster.

Dans le cas où un nœud reçoit un second horaire différent après s'être déjà synchronisé, il adopte les deux afin de servir de pont entre deux clusters. Ce nœud se réveille donc à la fois selon les horaires de son propre cluster et selon ceux du cluster voisin.

Les protocoles MAC synchrones présentent l'avantage de faciliter l'établissement de la communication entre nœuds : ils n'ont pas besoin de « trouver » le moment où l'autre nœud est éveillé, ce qui simplifie considérablement l'échange de données. En revanche, la synchronisation est coûteuse en énergie et en messages. De plus, les nœuds partageant une même fenêtre active, la compétition sur le canal est accrue [3].

4.2.1. S-MAC

Le protocole S-MAC (Sensor-MAC) est un protocole MAC développé par Wei Ye, John Heidemann et Deborah Estrin de l'Université de Californie à Los Angeles (UCLA) de l'Université de Californie à Berkeley, dans le cadre de recherches sur les réseaux de capteurs sans fil au début des années 2000. L'objectif était de concevoir un protocole MAC capable de réduire la consommation d'énergie et de permettre l'autoconfiguration des nœuds, afin d'optimiser la durée de vie des réseaux de capteurs [11].

Accès au canal :

L'accès au canal dans le protocole S-MAC est inspiré du protocole 802.11, mais modifié afin de permettre d'économiser de l'énergie. Ce dernier est organisé en 3 composantes majeurs :

1. Écoute/sommeil périodiques

S-MAC impose un cycle alterné entre les phases "Listen" (écoute) et "Sleep" (sommeil). Un nœud ne peut ni émettre ni recevoir en dehors de la phase "Listen". Pendant la phase "Sleep", toute communication est suspendue. Le canal de communication n'est donc accessible que durant la phase "Listen", ce qui modifie de manière significative la philosophie d'accès au médium par rapport à celle de la norme 802.11.

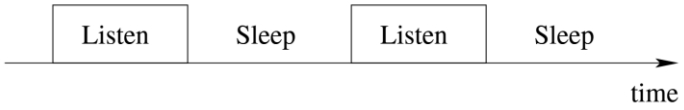

Figure 6 : Ecoute/sommeil périodiques [11]

De plus, afin de pouvoir à la fois recevoir des synchronisations et des données, la période Listen est divisée en deux sous-fenêtres.

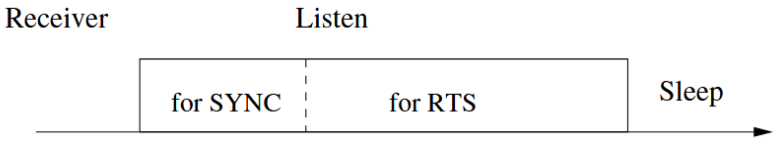

Figure 7: Période d'écoute S-MAC [11]

Chaque nœud diffuse régulièrement des paquets SYNC, même s'il n'a pas de suiveurs, pour permettre à de nouveaux nœuds de rejoindre le cluster.

2. Évitement des collisions

Plusieurs émetteurs peuvent vouloir communiquer simultanément avec un même récepteur.

Pour éviter ce problème, chaque paquet transmis contient la durée restante de la transmission. Les nœuds voisins mettent alors à jour leur NAV (Network Allocation Vector) et restent silencieux tant que NAV > 0.

Ce mécanisme prévient les collisions en réservant virtuellement le canal.

3. Envoie d'un message

L'envoi de données repose sur un mécanisme de CSMA/CA avec un RTS/CTS (Request to Send / Clear to Send) :

1. Lorsqu'un nœud souhaite transmettre, il envoie un RTS au destinataire, indiquant la durée estimée de la transmission.
2. Si le récepteur est disponible, il répond par un CTS. S'il ne peut pas transmettre (canal occupé), il ignore le RTS et l'émetteur attend avant de réessayer.

3. Les voisins qui entendent le RTS ou le CTS savent que le canal sera occupé pour la durée annoncée et s'abstiennent d'émettre.
4. Après réception du CTS, l'émetteur envoie les données.
5. Le récepteur confirme la bonne réception avec un ACK.

Synchronisation

Le mécanisme de synchronisation est similaire à celui présenté dans l'introduction [11] :

1. Phase d'écoute initiale : Le nœud écoute pendant un certain temps. S'il n'entend pas de planning émis par d'autres nœuds, il choisit aléatoirement son propre horaire de sommeil et le diffuse via un message SYNC. On l'appelle alors synchroniseur.
2. Adoption d'un horaire existant : Si un nœud reçoit l'horaire d'un voisin avant d'avoir choisi le sien, il adopte cet horaire. Après un délai aléatoire, il le rediffuse. Il devient alors un suiveur.
3. Gestion des multiples horaires : Si un nœud reçoit un nouvel horaire différent après avoir déjà choisi et diffusé le sien, il adopte et maintient les deux horaires, afin de rester compatible avec plusieurs clusters.

Les nœuds mettent périodiquement à jour leurs horaires via des paquets SYNC pour éviter une trop grande dérive d'horloge.

Localisation

Il n'existe aucun système de localisation natif dans le protocole S-MAC. Étant un protocole synchrone, on pourrait envisager de récupérer, à un niveau supérieur, les différents délais de transmission pour mettre en place une méthode de localisation basée sur la trilatération ou la triangulation.

Cependant, cette approche semble difficile à mettre en œuvre, car elle nécessiterait une synchronisation extrêmement précise des différents nœuds. De plus, la présence de plusieurs références horaires complique encore davantage le processus. Il serait possible d'imaginer un protocole exploitant S-MAC pour la localisation, mais celui-ci serait probablement très peu précis.

Mécanismes de sécurité

Tout comme la B-MAC, la S-MAC est un protocole conçu pour minimiser la consommation énergétique. Dans ce contexte, la gestion de la sécurité devient paradoxale. En effet, ce protocole est vulnérable à plusieurs types d'attaques, telles que le jamming ou l'eavesdropping [12].

Mobilité des nœuds

La mobilité n'est pas gérée par S-MAC en effet le protocole S-MAC est conçu pour maximiser la durée de vie des batteries des capteurs. Pour cela, il met les nœuds en sommeil la plupart du temps et ne les réveille que périodiquement pour communiquer. Cette approche fonctionne très bien dans les réseaux stationnaires, où les connexions entre nœuds sont stables.

Dans les applications avec capteurs mobiles ou les nœuds se déplacent à des vitesses variables le protocole S-MAC standard ne peut pas recréer rapidement de nouvelles connexions pour suivre les nœuds mobiles. Ce qui implique une dégradation de la performance réseau (latence, pertes de paquets) [13].

Consommation énergétique

L'étude [11] vise à comparer la consommation énergétique du protocole S-MAC avec celle d'un MAC basé sur IEEE 802.11.

La plateforme matérielle utilise des motes Rene de l'Université de Berkeley est composé de :

- Microcontrôleur Atmel AT90LS8535
- Transceiver radio TR1000

La topologie du réseau expérimentale est la suivante :

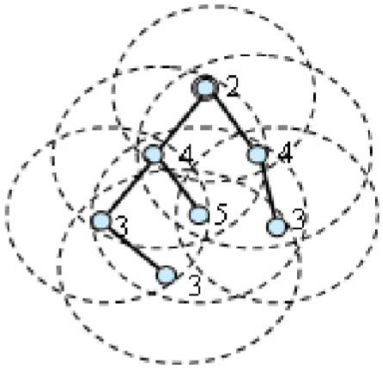

Figure 8 : Topologie du réseau expérimental [11]

Protocole expérimentale :

Les sources génèrent un message toutes les 1 à 10 secondes. À chaque fois, 10 tests indépendants sont effectués, et la mesure est prise pour chaque nœud :

- Durée totale de la transmission de tous les paquets
- Pourcentage de temps passé en TX/RX/écoute/sommeil
- Énergie = Σ (Temps_mode × Puissance_mode)

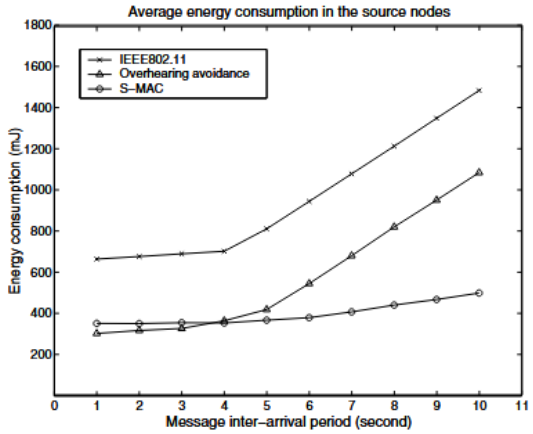

Figure 9 : Consommation d'énergie dans les nœuds sources [11]

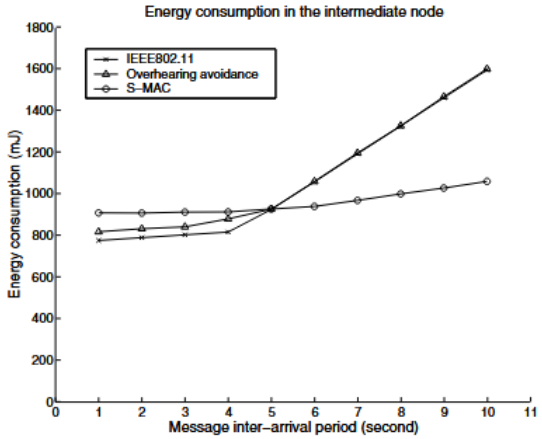

Figure 10 : Consommation d'énergie mesurée au niveau du nœud intermédiaire [11]

L'efficacité énergétique du réseau varie en fonction de la charge et du rôle des nœuds. En présence d'une charge lourde (inférieure à 4 secondes), l'écoute en mode veille est pratiquement inexistante, et S-MAC économise principalement de l'énergie grâce à l'échange de messages et à l'évitement des périodes d'écoute inutiles.

Lorsque la charge est légère (supérieure à 4 secondes), l'écoute en mode veille devient plus marquée. Cependant, le mode sommeil périodique de S-MAC permet une réduction significative de la consommation d'énergie, rendant S-MAC plus efficace que le standard 802.11.

Pour un nœud intermédiaire, les gains énergétiques apportés par S-MAC sont moindres en raison des mécanismes de synchronisation. Enfin, en cas de trafic très lourd, l'efficacité énergétique de S-MAC tend à se rapprocher de celle du 802.11, car le temps de sommeil disponible devient insuffisant pour tirer pleinement parti des mécanismes de réduction de la consommation d'énergie.

4.3. Les protocoles par créneaux d'utilisation

Cette catégorie regroupe l'ensemble des protocoles basés sur l'utilisation du TDMA (Time Division Multiple Access). Le TDMA est un mode d'accès au médium dans lequel le temps est découpé en intervalles appelés créneaux, et où chaque nœud se voit attribuer un créneau spécifique pour transmettre. Cela garantit l'absence de collisions, puisque les nœuds n'émettent jamais simultanément.

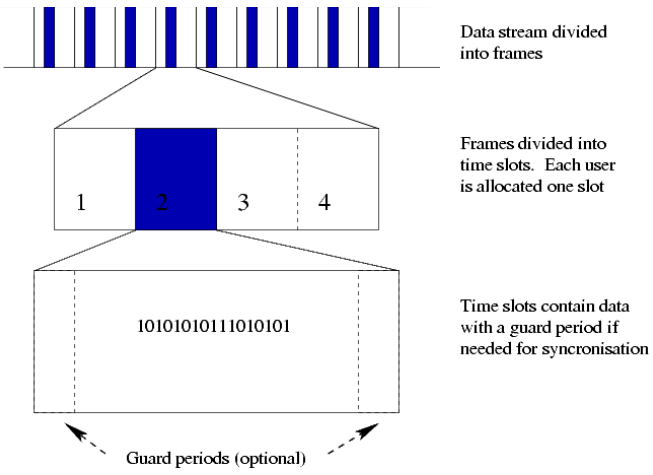

Figure 11 : Fonctionnement TDMA [14]

Le TDMA est particulièrement utile dans un réseau où de nombreux nœuds souhaitent communiquer en même temps. Dans ce type de situation, les méthodes aléatoires comme CSMA/CA entraînent : Des collisions, des retransmissions est donc une diminution du débit.

Avec le TDMA, les transmissions sont planifiées, ce qui élimine les collisions et permet une utilisation optimale du canal. Ainsi, même en cas de forte demande d'accès au médium, l'utilisation du TDMA permet de maintenir un débit élevé et stable.

Dans le cadre des protocoles synchrones précédemment analysés, la synchronisation des nœuds était locale, c'est-à-dire que les nœuds étaient regroupés en clusters, chacun étant synchronisé par un nœud maître local. Cette approche, cependant, n'est pas compatible avec l'utilisation du TDMA : si les clusters ne partagent pas la même référence temporelle, leurs périodes d'activité peuvent se chevaucher, provoquant des collisions entre clusters.

C'est pourquoi les protocoles basés sur le TDMA utilisent une synchronisation globale, afin que toutes les trames temporelles soient alignées et cohérentes entre l'ensemble des nœuds du réseau.

Cependant, cette synchronisation globale représente une contrainte énergétique importante, car elle nécessite : de recevoir régulièrement des messages de synchronisation et de maintenir l'horloge interne active. Elle nécessite de plus de s'appuyer sur une référence temporelle commune, par exemple via l'utilisation du GPS [3].

4.3.1. Z-MAC

Le Z-MAC (Zebra-MAC) est un protocole MAC conçu par Injong Rhee, Ajit Warrier, Mahesh Aia et Jeongki Min, chercheurs à la North Carolina State University (NCSU). Il s'agit d'un protocole hybride développé pour combiner les avantages du CSMA et du TDMA.

Z-MAC permet une forte utilisation du canal avec une faible latence en situation de faible contention, comme le fait le CSMA. En revanche, lorsque la contention est élevée, il offre une meilleure utilisation du canal et réduit les collisions entre nœuds voisins, à l'image du TDMA [15].

Accès au canal :

L'accès au canal de transmission se déroule en deux grandes phases : une phase d'initialisation, suivie d'une phase de transmission [15].

Phase d'initialisation

Cette phase est réalisée une seule fois, sauf en cas de changements significatifs de la topologie (par exemple, en cas de déplacement de capteurs). Elle est structurée de la manière suivante :

1. Découverte des voisins

Pour découvrir ses voisins à un saut, chaque nœud envoie un ping toutes les 30 secondes, chaque ping contenant sa liste de voisins à un saut. Cela permet à chaque nœud d'apprendre sa propre liste de voisins à 1 saut, et, grâce aux pings reçus de ses voisins, d'obtenir sa liste de voisins à 2 sauts. Cette information est cruciale pour éviter que deux nœuds proches utilisent le même slot TDMA [15].

2. Attribution des slots : DRAND

Le protocole Z-MAC utilise DRAND, une version distribuée du protocole RAND. Il permet d'attribuer un slot différent à chaque nœud situé à 2 sauts, afin d'éviter les collisions. En effet, deux nœuds qui ne sont pas directement voisins mais partagent un voisin (à 2 sauts) ne doivent pas transmettre en même temps, sous peine de provoquer des collisions chez le voisin commun. Le principe est simple : chaque nœud envoie une requête pour obtenir un slot et avertit une fois celui-ci obtenu [15].

4. Trames locales

Une fois qu'un nœud a obtenu un slot, il doit définir la période durant laquelle il peut l'utiliser. Dans un protocole TDMA classique, on utilise une trame globale : tous les nœuds partagent la même taille de trame, qui est déterminée par le plus grand numéro de slot du réseau (MSN). Pour connaître ce MSN, il est nécessaire de le diffuser dans l'ensemble du réseau.

Le protocole Z-MAC cherche à éviter cette diffusion et adopte la règle TF (Trame Flexible) : chaque nœud utilise une trame de taille différente, adaptée à son voisinage local. Ainsi, chaque nœud choisit une trame locale, qui est un multiple du plus grand slot dans son voisinage à deux sauts.

5. Phase de transmission

Après l'initialisation, le réseau commence à transmettre. Chaque nœud peut se trouver dans l'un des deux états possibles :

- Mode LCL (Low Contention Level)

Cet état est actif lorsqu'il y a peu de trafic sur le réseau. Dans ce mode, tous les nœuds, y compris ceux qui ne sont pas propriétaires, peuvent transmettre à n'importe quel moment, bien que les nœuds propriétaires bénéficient d'une priorité supérieure.

Ainsi, dans ce mode, le protocole Z-MAC fonctionne de manière similaire au CSMA et offre un très bon débit.

- Mode HCL (High Contention Level)

Cet état est activé lorsqu'il y a une congestion importante sur le réseau. Il est déclenché lorsqu'un nœud reçoit un ECN (Explicit Contention Notification). Un ECN est envoyé lorsqu'un nœud détecte une forte contention (par exemple, 0,3 backoffs/paquet). Le nœud envoie alors un ECN à sa destination, à un saut, puis cette dernière diffuse un ECN à deux sauts. Ainsi, tous les nœuds recevant un ECN passent en mode HCL (High Contention Level).

Dans la phase HCL, seul le propriétaire du créneau et ses voisins à un saut peuvent transmettre, les autres doivent attendre. Le comportement du réseau devient alors similaire à un système TDMA (Time Division Multiple Access) [15].

Synchronisation

Contrairement à un TDMA classique, où tous les nœuds doivent être parfaitement synchronisés, Z-MAC adopte une synchronisation allégée. Grâce à l'intégration du mécanisme de backoff CSMA, les petites erreurs de synchronisation sont automatiquement compensées. Ainsi, même si un nœud estime qu'un créneau commence légèrement plus tôt ou plus tard, il vérifiera toujours l'état du canal avant de transmettre, ce qui permet d'absorber les décalages temporels sans perturber la communication.

La synchronisation dans Z-MAC repose sur un principe simple : chaque nœud dispose de sa propre horloge interne et, lorsqu'il reçoit un message d'un voisin, il peut en déduire le décalage temporel et ajuster localement son horloge en conséquence. Il n'est donc pas nécessaire d'envoyer des messages spécifiques dédiés à la synchronisation [15].

Localisation

Aucun service de localisation n'est directement intégré dans le protocole Z-MAC. Cependant, comme les nœuds transmettent des messages à intervalles réguliers, il est possible d'enregistrer le temps d'arrivée de ces messages afin d'appliquer un algorithme de trilatération.

Toutefois, bien que Z-MAC bénéficie d'une synchronisation globale, celle-ci n'est pas aussi précise que celle d'un TDMA pure. Par conséquent, les positions obtenues risquent d'être fortement biaisées, notamment si l'on utilise des techniques de localisation basées sur le temps.

Mécanismes de sécurité

Le protocole Z-MAC n'inclut pas de mécanismes de sécurité, comme c'est souvent le cas dans les réseaux de capteurs sans fil. Il a été conçu principalement pour l'efficacité énergétique et la gestion du médium.

Mobilité des nœuds

Z-MAC a été conçu pour des réseaux de capteurs plutôt statiques, mais il conserve une certaine tolérance à la mobilité grâce à son architecture hybride. Comme vu précédemment en fonctionnement normal, Z-MAC utilise un accès CSMA, tandis qu'en situation de congestion il bascule automatiquement vers un fonctionnement TDMA.

Cette flexibilité permet au réseau de rester opérationnel même lorsque certains nœuds se déplacent. Toutefois, cette tolérance reste limitée : les performances se dégradent rapidement en présence d'une mobilité élevée.

En effet, Z-MAC repose sur une connaissance précise du voisinage pour gérer les priorités de contention et attribuer les slots. La mobilité entraîne donc des changements fréquents de topologie, nécessitant des mises à jour régulières de cette information. Ces réactualisations sont coûteuses.

Consommation énergétique

Une évaluation de la consommation énergétique de la Z-MAC a été réalisé dans [15], c'est cette dernière qui sera présenté ci-dessous afin de mesurer le coût énergétique du protocole Z-MAC.

Nou analyserons la consommation durent :

1. La phase d'initialisation (setup phase) qui comprend :
    a. DRAND
    b. TPSN
    c. Construction des trames
    d. ECN
2. En fonctionnement normal, selon différentes charges réseau dans différents scénarios :
    a. Scénario à 1 saut
    b. Multi-sauts (42 nœuds)

Plateforme matérielle :

La plateforme matérielle mis en place est similaire à celle mise en place pour l'étude de la consommation énergétique de la B-MAC :

- Mica2 (microcontrôleur Atmel ATMega 128L, radio CC1000)
- Alimentation : batterie 2500 mAh, 3 V

Consommation énergétique pendant la phase de setup :

La consommation énergétique mesurée dans le tableau ci-dessous repose sur une exécution complète du protocole d'initialisation de Z-MAC. La phase de configuration a été exécutée 30 fois afin d'obtenir des valeurs moyennes. Les mesures ont été réalisées dans un scénario multi-sauts composé de 42 nœuds, et la consommation a été exprimée en Joules. Ainsi, la phase de configuration coûte en moyenne 7,22 Joules par nœud. Bien que ce coût initial ne soit pas négligeable comparé à la consommation énergétique par transmission, il est jugé acceptable, car il est amorti par les gains en efficacité énergétique au cours de la vie du réseau.

Opération	Moyenne	Ecart-type
Neighbor discovery	0.73	0.0018
DRAND	4.88	3.105
Local Frame Exchange	1.33	1.39
TPSN	0.28	0.036

Les auteurs évaluent ensuite comment Z-MAC consomme l'énergie pendant les transmissions, en comparant systématiquement avec B-MAC.

Ce test reprend exactement la méthodologie de B-MAC décrite dans l'article original étudié dans la partie B-MAC, il est mesureé la puissance totale consommée (périodes d'écoute + émissions + backoff), la consommation moyenne par paquet, le ratio débit énergétique.

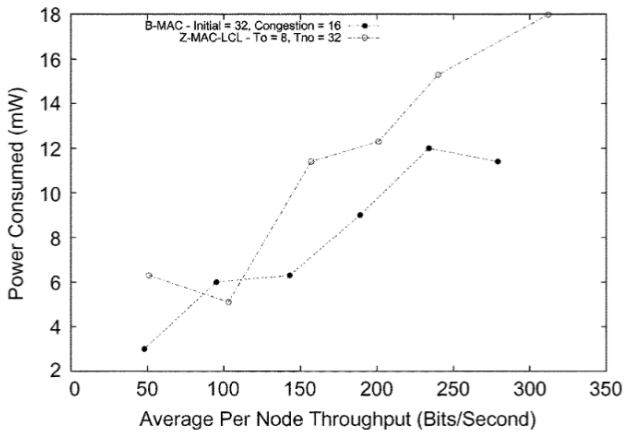

Figure 12 : Efficacité énergétique dans les applications à faible débit [15]

Z-MAC exploite les fonctionnalités CCA et LPL de B-MAC, ce qui lui confère une efficacité énergétique comparable à celle de B-MAC pour les applications à faible débit de données. Le test décrit dans la section 6.2 de [11] est appliqué permettant ainsi de comparer avec la consommation de la B-MAC précédemment évaluée, en variant le taux de transmission, on observe que la consommation d'énergie de Z-MAC est légèrement supérieure à celle de B-MAC. Cela s'explique par le fait que, dans Z-MAC, les nœuds restent éveillés plus longtemps pour la transmission.

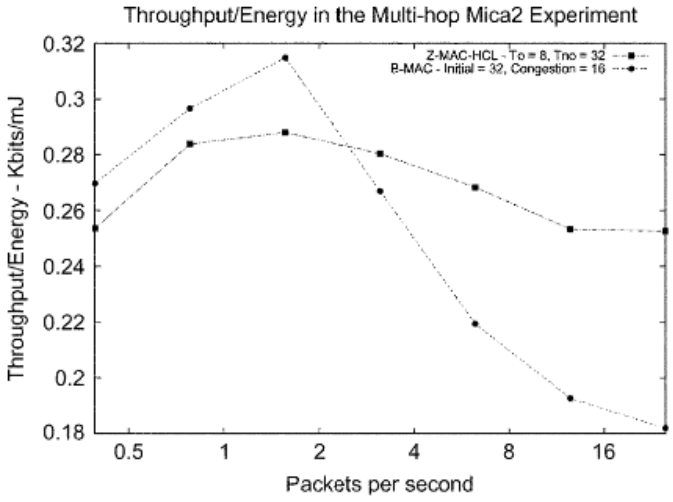

Figure 13 : Efficacité énergétique multi-sauts avec Mica2 [15]

L'article [] mesure à nouveau l'efficacité énergétique de Z-MAC et B-MAC, cette fois avec un réseau de 42 nœuds. La figure ci-dessus présente le rapport entre le débit et la consommation d'énergie. L'analyse montre que B-MAC consomme légèrement moins d'énergie (jusqu'à 10 %) pour les faibles débits de transmission. Cette différence s'explique par la taille plus petite de la fenêtre de contention de B-MAC. Cependant, lorsque le taux de transmission dépasse trois paquets par seconde, l'efficacité énergétique de Z-MAC s'améliore et surpasse celle de B-MAC d'environ 40 % à plein débit [15].

4.3.2. TRAMA

Le protocole TRAMA (Traffic-Adaptive Medium Access) a été proposé en 2003 par Venkatesh Rajendran, Katia Obraczka et J. J. Garcia-Luna-Aceves de l'Université de Californie. Son objectif est d'adapter les principes du TDMA pour offrir un accès au médium à la fois énergétiquement efficace et compatible avec les réseaux de capteurs sans fil.

TRAMA répartit les créneaux temporels de manière déterministe en fonction du trafic réel, met en place une procédure d'élection des nœuds transmetteurs, et inclut un mécanisme de mise en

veille pour les nœuds non sollicités. Cela permet de réduire de manière significative la consommation énergétique tout en minimisant les risques de collisions [16].

Accès au canal

Le protocole TRAMA repose principalement sur 3 composantes :

1. Neighbor Protocol (NP)
2. Exchange Protocol (SEP)
3. Adaptive Election Algorithm (AEA)

Organisation du temps :

Le temps dans TRAMA est divisé 2 types en créneaux horaires. Ces créneaux sont utilisés pour organiser les transmissions et les échanges de signalisation.

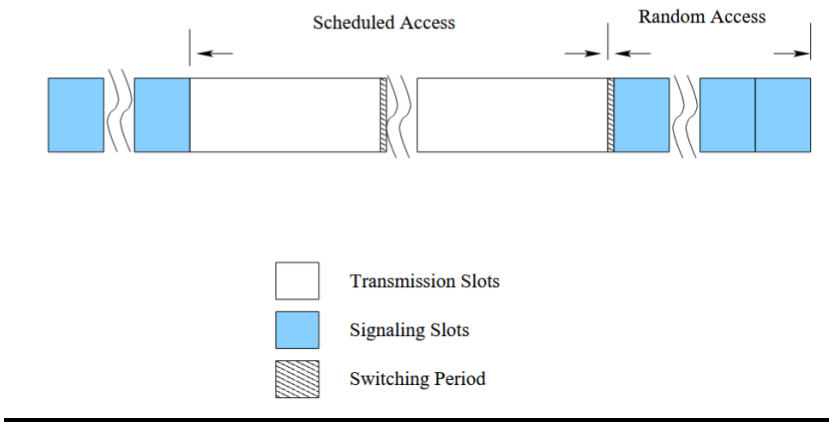

Figure 14 : Organisation des créneaux horaires [16]

Signaling slots :

Les nœuds peuvent transmettre des paquets de signalisation pour annoncer leurs informations de voisinage (NP) et se synchroniser. Ces créneaux sont sujets à des collisions, car plusieurs nœuds peuvent tenter de transmettre en même temps

Transmission slots :

Ces créneaux sont utilisés pour l'échange de données, sans collisions. Et la diffusion des plannings (SEP) [16].

1) Neighbor Protocol (NP)

Durant les signaling slots, chaque nœud : diffuse les changements dans son voisinage directs (ajouts / suppressions) ; reçoit les mises à jour des voisins ; et peut reconstituer ainsi une vue cohérente à 2 sauts. L'objectif est de garantir que chaque nœud connaisse ses voisins à 2 sauts pour éviter des collisions entre nœuds qui ne se voient pas directement.

Comme mentionner précédemment : le Signaling slot est assujettie aux collisions ainsi pour garantir une probabilité élevée que les mises à jour soient reçues malgré tout le protocole effectue 7 retransmissions espacées de 1.44 × N slots [16].

2) Schedule Exchange Protocol (SEP)

Chaque nœud annonce les créneaux pendant lesquels il prévoit de transmettre des données à ses voisins. Il évalue ces créneaux en fonction du trafic dans sa file MAC. Il procède également au calcul des winning slots correspond aux créneaux où il a la plus haute priorité. Pour chaque winning slot, il précise : Le bitmap des récepteurs, ou 0 si le créneau est libre [16].

Tous les voisins doivent écouter ce dernier créneau afin de resynchroniser leur copie du planning du nœud.

3) Adaptive Election Algorithm (AEA)

L'Algorithme de Sélection Adaptatif (AEA), qui constitue la partie centrale de TRAMA, est chargé de la sélection des émetteurs et des récepteurs pour chaque créneau temporel (slot). L'AEA s'appuie sur les informations fournies par le NP et le SEP afin de déterminer les créneaux durant lesquels chaque nœud doit transmettre.

Si seul l'émetteur était sélectionné, les nœuds voisins devraient rester en écoute inutilement, ce qui entraînerait un gaspillage d'énergie. En incluant également les récepteurs dans le processus de sélection, seuls ces derniers demeurent éveillés pendant le créneau, optimisant ainsi la consommation d'énergie [16].

Synchronisation

Étant donné que les débits de données dans un réseau de capteurs sont relativement faibles, la durée des créneaux de transmission est bien supérieure aux dérives typiques de l'horloge. Par exemple, pour une radio fonctionnant à 115,2 Kbps, un créneau de transmission d'environ 46 ms permet d'envoyer des unités de données de 512 octets au niveau de la couche application. Ainsi, des dérives d'horloge de l'ordre de la milliseconde peuvent être tolérées, alors que les dérives réelles sont généralement de l'ordre de la microseconde, voire moins.

Cela rend possible la synchronisation dite post-facto, telle que décrite dans [17] où tous les nœuds démarrent avec leurs horloges locales, qui peuvent être légèrement différentes de celles des autres. Chaque nœud diffuse périodiquement des paquets de synchronisation contenant son horodatage local. À la réception de ces paquets, chaque nœud compare son horodatage avec celui reçu de ses voisins et ajuste progressivement son horloge pour se rapprocher de la moyenne ou du consensus des horloges voisines.

Mobilité des nœuds

L'algorithme sélectionne les émetteurs et récepteurs en fonction des priorités à deux sauts. Toutefois, en raison de la mobilité, les informations à deux sauts peuvent rapidement devenir obsolètes, ce qui entraîne une inefficacité et des pertes de paquets. Si un nœud se déplace et change de voisin pendant un créneau (slot), il peut manquer des transmissions, car il n'a pas encore connaissance de son nouveau voisin.

En revanche, l'algorithme TRAMA est capable de gérer l'ajout ou la suppression de nœuds statiques grâce aux créneaux de signalisation (signaling slots), ce qui permet une tolérance aux ajouts et suppressions ponctuels. Cependant, il présente une limitation en ce qui concerne la mobilité rapide des nœuds : les plannings de transmission (schedules) et les priorités à deux sauts deviennent rapidement invalides, ce qui compromet son efficacité dans des environnements mobiles.

4.4. Les protocoles MAC multicanaux

Dans un réseau de capteurs, plusieurs contraintes limitent l'utilisation d'un unique canal radio. D'une part, la bande passante est généralement faible, car les modules radio employés sont volontairement simples afin de réduire les coûts et la consommation d'énergie. D'autre part, les capteurs sont soumis à de fortes contraintes énergétiques, ce qui limite encore la capacité de transmission. À cela s'ajoute l'irrégularité du trafic : les données ne sont pas toujours émises de manière continue mais peuvent arriver par pics soudains, par exemple lorsqu'un événement est détecté simultanément par plusieurs capteurs.

L'utilisation simultanée de plusieurs canaux radio apparaît donc comme une solution efficace pour augmenter le débit global et réduire les interférences. Cependant, cette approche soulève deux défis majeurs : l'attribution optimale des canaux aux différents nœuds du réseau, afin d'assurer une répartition équilibrée et de maximiser les performances.

Et la communication entre nœuds opérant sur des canaux différents, qui doit rester possible sans perte d'efficacité. De plus les solutions envisagées doivent tenir compte des contraintes énergétiques et du coût matériel afin de rester compatible avec les exigences des réseaux de capteurs [3].

4.4.1. TMCP

Le protocole TMCP (Tree-based Multi-Channel Protocol) a été proposé par Yafeng Wu, John A. Stankovic, Tian He et Shan Lin dans un article publié lors de la conférence INFOCOM 2008. Ce protocole a été conçu en réponse aux limitations des protocoles multi-canaux traditionnels, qui ne sont pas adaptés aux réseaux sans fil de capteurs, en raison du nombre limité de canaux disponibles et des erreurs temporelles inévitables qui surviennent dans les réseaux réels.

Le protocole TMCP propose une solution innovante basée sur une architecture en arbre pour la gestion des canaux dans les WSN, visant à améliorer l'efficacité et la fiabilité des communications. Il est spécifiquement conçu pour les applications de collecte de données dans ces réseaux, où plusieurs nœuds doivent échanger des informations tout en minimisant les interférences et en optimisant l'utilisation des canaux disponibles [18].

Accès au canal :

L'accès au canal dans TMCP se décompose en trois étapes majeures :

1. Détection des canaux disponibles (Channel Detection, CD)
2. Assignation des canaux aux sous-arbres (Channel Assignmen, CA)
3. Communication des données (Data Communication, DC)

1) Détection des Canaux Disponibles (CD)

Avant d'accéder au canal, TMCP commence par évaluer la qualité des canaux disponibles. Cette étape permet de s'assurer que seuls les canaux fiables seront utilisés.

2) Pour cela, deux nœuds sont chargés d'évaluer la qualité de la liaison de chaque canal en échangeant des paquets. Ensuite, parmi les canaux ayant une bonne qualité de liaison, seuls ceux qui ne sont pas adjacents sont sélectionnés. Cela permet de constituer un ensemble de k canaux.
3) Assignation des canaux (CA)

Une fois les canaux fiables identifiés, TMCP divise le réseau en k sous-arbres disjoints. Chaque sous-arbre se voit attribuer un canal unique, et tous les nœuds d'un sous-arbre utilisent ce même canal. L'attribution d'un canal par sous-arbre permet d'éliminer les interférences inter-arbres, car deux sous-arbres ne peuvent pas émettre simultanément sur le même canal. Cependant, étant donné que tous les nœuds d'un sous-arbre utilisent le même canal, l'interférence intra-arbre devient inévitable et constitue le principal goulot d'étranglement en termes de performance dans le système.

L'objectif de la partition du réseau est donc de diviser celui-ci en sous-arbres de manière à minimiser ces interférences intra-arbres et à optimiser les performances globales.

Pour ce faire, le protocole TMCP utilise l'algorithme PMIT (Proportional Minimizing Inter-Tree Interference), qui détermine la manière dont les nœuds sont affectés à chaque sous-arbre. L'objectif de cet algorithme est de minimiser les interférences entre sous-arbres tout en maintenant un équilibre entre la taille des sous-arbres.

Algorithm 1 Greedy PMIT

Input: k channels, a graph $G = (V, E)$, a root r and the interference set of every node.
Output: For each node u, c_u and p_u
Use BFS-Fat-tree algorithm to construct a fat-tree with rooted at r.
for each channel i **do**
$T_i = r$;
end for
for each node u **do**
$c_u = 0$; $p_u = null$;
end for
$level = 1$;
repeat
$node\_list = \{u | height(u) == level; c_u == 0\}$
sort $node\_list$ in ascending order by the number of node's parents.
for each node u in $node\_list$ **do**
find T_i which keep connected and has the least interference after adding u.
$T_i = T_i \cup \{u\}$; $c_u = i$; $p_u = v$, which connects to u and has the least interference among all nodes in T_i.
update the interference value of T_i.
end for
$level++$;
until $level >$ the maximum height of the fat tree

Figure 15 : Algorithme PMIT [18]

4) Accès au canal pendant la phase Communication (DC)

Lors de la phase de communication, l'accès au canal dans TMCP de la façon suivante : Chaque nœud utilise de manière permanente le canal qui lui est assigné par son sous-arbre, il n'y a donc

pas besoin de négociation ou de synchronisation ; l'accès au canal au sein de chaque sous-arbre fonctionne selon le principe classique de CSMA/CA

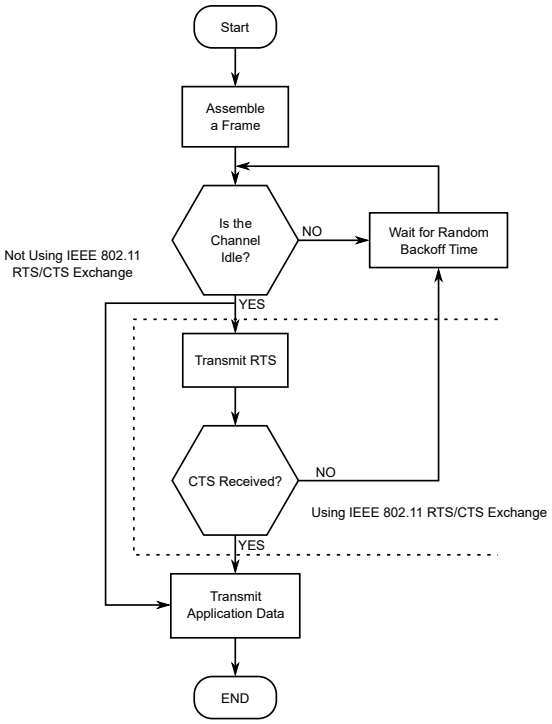

Figure 16 : CSMA / CA [17]

Synchronisation

Le protocole TMCP ne nécessite pas de synchronisation, ce qui constitue un avantage majeur. Cela permet d'éviter la complexité liée à la gestion des horloges, ainsi que la consommation d'énergie nécessaire pour l'échange de messages de synchronisation.

De plus, il élimine les erreurs de synchronisation accumulées, qui rendent souvent les protocoles multi-canaux peu fiables. TMCP supprime totalement cette dépendance grâce à deux mécanismes principaux : d'une part, les nœuds ne changent jamais de canal après la phase d'assignation des sous-arbres, d'autre part, chaque branche de l'arbre fonctionne de manière asynchrone, le protocole d'accès à chaque canal reposant sur un mécanisme de CSMA [17].

Localisation

Le protocole MAC TCMP ne dispose pas de mécanismes intégrés pour la localisation. De plus, son caractère asynchrone empêche l'utilisation de l'horloge interne pour des méthodes basées sur le temps. Toutefois, une estimation de la position utilisant le RSSI pourrait être potentiellement intégré au protocole. Sous réserve que la topologie du réseau le permette. En effet, la précision de cette méthode dépendrait de la configuration et de la densité des points

d'accès ainsi que de la propagation du signal dans l'environnement. Dans des réseaux bien structurés, cette approche pourrait offrir une possible localisation, bien que moins précise que d'autres techniques nécessitant une synchronisation temporelle.

Mécanismes de sécurité

Le protocole TMCP ne prévoit aucun mécanisme de sécurité dans sa conception. Il se concentre principalement sur la performance et la fiabilité des transmissions multi-canaux. En conséquence, il ne propose ni chiffrement, ni vérification de l'intégrité des messages, ni protection contre les attaques par déni de service (DoS) [17].

Mobilité des nœuds

Le protocole TCMP ne prend pas en charge la mobilité et a été conçu pour des réseaux de capteurs statiques, avec une topologie fixe. Les canaux sont assignés une seule fois, au démarrage du réseau, et ne sont pas réassignés en cas de mouvement d'un nœud. Cela peut entraîner des interférences si un nœud se déplace, car il pourrait se retrouver sur un canal déjà occupé ou ne plus être sur un canal optimal. Le protocole ne prévoit pas de mécanisme pour réaffecter dynamiquement les canaux en cas de mobilité.

De plus, si un nœud se déplace, il peut se retrouver hors de portée de son nœud parent, ce qui interrompt la communication avec la station de base [17].

5. Analyse comparative des protocoles

5.1. Tableau comparatif

	Classe	**Accès au canal**	**Localisation**	**Sécurité**	**Mobilité**	**Synchronisation**	**Consommation énergétique**
B-MAC	Asynchrone	CSMA/LPL	Non	Non	Faible mobilité	Non	Faible
X-MAC	Asynchrone	CSMA/LPL	Non	Non	Faible mobilité	Non	Faible

		préambules courts					
S-MAC	Synchrone	CSMA + duty cycle	Non	Non	Mauvaise (synchronisation dure à maintenir)	Oui	Moyenne à faible
Z-MAC	Synchrone	Hybride TDMA/CSMA	Non	Non		Oui	Moyenne
TRAMA	Synchrone	TDMA adaptatif planifié	Non	Non	Mauvaise (grande dépendance à la synchro)	Oui	Faible
TCMP	Synchrone	CSMA	Non	Non		Non	Moyenne

	Avantage	Limite
B-MAC	Très faible consommation grâce au Low Power Listening (LPL) ; simple à mettre en œuvre ; bonne portée ; et mobilité	Latence potentiellement élevée en forte densité ; collisions fréquentes en forte densité ; préambules longs et coûteux
X-MAC	Réduction de l'énergie grâce aux préambules courts ; meilleure latence que B-MAC ; détection d'adresse anticipée	Reste sensible aux collisions ; performances réduites en forte congestion
S-MAC	Bonne économie d'énergie grâce au duty-cycle ; prévisible et adapté aux réseaux stables	Synchronisation difficile ; latence élevée ; performances faibles en mobilité

Z-MAC	Combine les avantages CSMA et TDMA ; très efficace en réseau dense ; bonne tolérance à la congestion	Complexité élevée
TRAMA	Très bonne efficacité énergétique ; évite complètement les collisions grâce au planning TDMA	Synchronisation stricte nécessaire ; complexité élevée ; latence importante en trafic léger

5.2. Analyse qualitative

Protocole le plus économe selon le trafic ?

Parmi les protocoles présenté, X-MAC semble être le protocole le plus économe, en effet il améliore le protocole B-MAC en réduisant la durée du préambule. X-MAC permet au récepteur de désactiver sa radio lorsqu'il n'est pas concerné par la transmission, réduisant ainsi la consommation d'énergie. Ce protocole est particulièrement efficace en conditions de trafic faible ou variable, ce qui est typique des WNS.

B-MAC : Bien adapté pour des situations de faible trafic, mais son préambule long, entraînant une perte d'énergie importante.

TRAMA / Z-MAC : Bien que plus performants en termes de gestion des collisions, ces protocoles sont plus coûteux en énergie, particulièrement en faible trafic, ce qui les rend moins adaptés pour des réseaux à faible consommation.

Le plus performant en forte densité de nœuds ?

Les protocoles TRAMA et Z-MAC sont les plus adapté pour des conditions de forte charge, de part leurs utilisation de TDMA permettant d'allouer des créneaux de transmission fixes à chaque nœud, ce qui élimine les risques de collisions, un problème majeur dans le cas des réseaux à forte densité.

Le meilleur protocole pour la mobilité ?

Parmi les protocoles étudiés, aucun n'est spécifiquement conçu pour supporter une forte mobilité. Cependant, les protocoles B-MAC et X-MAC sont ceux qui tolèrent le mieux la mobilité.

En effet, les protocoles TDMA, tels que TRAMA, rencontrent des difficultés en conditions de mobilité, car les créneaux de transmission (slots) doivent être régulièrement réattribués pour s'adapter aux déplacements des nœuds. Cela peut entraîner des perturbations et une perte d'efficacité dans des environnements mobiles. De plus, S-MAC repose sur un mécanisme de synchronisation veille/sommeil, qui est fortement perturbé par la mobilité, car la synchronisation doit être constamment mise à jour pour chaque nœud en mouvement.

Celui avec la latence la plus faible

Les protocoles asynchrones, comme B-MAC et X-MAC, ne nécessitent pas d'attendre un slot de transmission, contrairement aux protocoles fonctionnant en mode TDMA (comme TRAMA). Cette absence de synchronisation stricte leur permet de réagir immédiatement dès que le récepteur se réveille, ce qui réduit la latence et les rend particulièrement performants en situation de faible trafic.

En revanche, lorsque le trafic augmente fortement, la situation change complètement. Les protocoles asynchrones comme B-MAC et X-MAC perdent alors leur avantage : les collisions se multiplient, entraînant des retransmissions et une hausse importante de la latence. Dans ces conditions, les protocoles basés sur le TDMA comme TRAMA deviennent plus efficaces, car ils éliminent les collisions grâce à une planification déterministe des transmissions.

Parmi ces protocoles, Z-MAC se distingue par sa grande flexibilité face à la variation du trafic. En effet, il combine CSMA et TDMA : il fonctionne en mode CSMA lorsque la charge est faible afin de minimiser la latence, puis bascule en mode TDMA lorsque le trafic devient intense pour éviter les collisions. Cette adaptativité fait de Z-MAC un protocole performant en situation de fort trafic.

6. Conclusion

Il n’existe pas, dans les réseaux de capteurs sans fil, de protocole MAC optimal pour tous les contextes. Le choix du protocole dépend largement de l’environnement, des contraintes propres au déploiement et du type d’application visée. Chaque usage des WSN surveillance

environnementale, détection d'événements, sécurité, agriculture intelligente impose des exigences particulières qui influencent directement la sélection du protocole MAC le plus adapté.

Chaque protocole représente un compromis entre plusieurs dimensions essentielles : consommation énergétique, latence, robustesse, complexité, sécurité, mobilité, capacité du réseau et tolérance aux collisions. Aucun protocole ne parvient à optimiser simultanément l'ensemble de ces paramètres.

Ainsi, les protocoles asynchrones se montrent très efficaces lorsque le trafic est faible, grâce à leur faible consommation énergétique et à leur grande réactivité. Néanmoins, leur performance se dégrade rapidement dans les environnements à forte densité de nœuds ou en cas de trafic intense, où les collisions et les retransmissions deviennent fréquentes. À l'inverse, les protocoles TDMA offrent d'excellents résultats sous forte charge en garantissant l'absence de collisions, mais ils imposent une synchronisation stricte et une complexité opérationnelle notable.

Dans ce contexte, les protocoles hybrides comme la Z-MAC occupe une place particulièrement intéressante, car ils parviennent à tirer parti du meilleur des deux approches. En mode léger, il adopte un comportement proche des protocoles asynchrones, assurant une faible consommation et une grande souplesse sous trafic réduit. Lorsque la charge augmente, il bascule progressivement vers un fonctionnement typé TDMA, permettant de limiter les collisions et de maintenir de bonnes performances. Cette adaptabilité fait de Z-MAC une solution hybride efficace et robuste, même si elle implique une implémentation plus complexe et une performance qui peut varier selon les conditions réelles du réseau.

Enfin, il est important de souligner que la consommation d'énergie n'a pas été suffisamment prise en compte dans ce rapport. Or, elle doit impérativement être prise en compte lors du choix du protocole, car elle impacte directement la durée de vie du réseau. Idéalement, il serait nécessaire d'établir un protocole ou une méthodologie expérimentale reproductible permettant de mesurer de manière fiable la consommation énergétique associée aux différents protocoles MAC afin d'obtenir une comparaison objective.

7. Sources

[1] « IQspot connecte les bâtiments pour réduire leurs consommations | Techniques de l'Ingénieur ». Techniques de l'Ingénieur. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://www.techniques-ingenieur.fr/actualite/articles/iqspot-connecte-les-batiments-pour-reduire-leurs-consommations-117062/

[2] P. P. Czapski, « A survey : MAC protocols for applications of wireless sensor networks », Tencon 2006, s. d.

[3] P. Huang, L. Xiao, S. Soltani, M. W. Mutka et N. Xi, « The evolution of MAC protocols in wireless sensor networks : A survey », IEEE Commun. Surv. & ; Tut., vol. 15, no 1, p. 101–120, 2013. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://doi.org/10.1109/surv.2012.040412.00105

[4] A. A. Khan, S. Ghani et S. Siddiqui, « A taxonomy for MAC protocols in wireless sensor networks based on traffic prioritization », Wireless Pers. Commun., vol. 104, no 4, p. 1493–1522, déc. 2018. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://doi.org/10.1007/s11277-018-6095-5

[5] Contributeurs aux projets Wikimedia. « Carrier sense multiple access with collision detection — wikipédia ». Wikipédia, l'encyclopédie libre. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://fr.wikipedia.org/wiki/Carrier_Sense_Multiple_Access_with_Collision_Detection#/media/Fichier:CMSA-CD.png

[6] J. Kuriakose et S. Joshi, « Localization in wireless sensor networks : A survey », s. d. [En ligne]. Disponible : https://arxiv.org/pdf/1410.8713

[7] Q. Dong et W. Dargie, « A survey on mobility and mobility-aware MAC protocols in wireless sensor networks », IEEE Commun. Surv. & ; Tut., vol. 15, no 1, p. 88–100, 2013. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://doi.org/10.1109/surv.2012.013012.00051

[8] E. Chukwuka et K. Arshad, « Energy efficient MAC protocols for wireless sensor network : A survey », Int. J. Wireless & ; Mobile Netw., vol. 5, no 4, p. 75–89, août 2013. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://doi.org/10.5121/ijwmn.2013.5406

[9] J. Polastre, J. Hill et D. Culler, « Versatile low power media access for wireless sensor networks », s. d. [En ligne]. Disponible : https://people.eecs.berkeley.edu/~culler/papers/ucb-tr-bmac.pdf

[10] M. Buettner, G. Yee et R. Han, « X-MAC : A short preamble MAC protocol for duty-cycled wireless sensor networks », s. d. [En ligne]. Disponible : https://www.cse.wustl.edu/~lu/cse521s/Papers/x-mac.pdf

[11] W. Ye, J. Heidemann et D. Estrin, « An energy-efficient MAC protocol for wireless sensor networks », s. d.

[12] S. K. Punia et F. Ziya, « Study on MAC protocols and attacks : A review », s. d.

[13] H. Pham et S. Jha, « An adaptive mobility-aware MAC protocol for sensor networks (MS-MAC) », s. d. [En ligne]. Disponible : https://www.cs.uc.edu/~cdmc/mass/mass2004/35169.pdf

[14] Contributors to Wikimedia projects. « Time-division multiple access - Wikipedia ». Wikipedia, the free encyclopedia. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://en.wikipedia.org/wiki/Time-division_multiple_access#/media/File:Tdma-frame-structure.png

[15] Injong Rhee, A. Warrier, M. Aia, Jeongki Min et M. L. Sichitiu, « Z-MAC : A hybrid MAC for wireless sensor networks », IEEE/ACM Trans. Netw., vol. 16, no 3, p. 511–524, juin 2008. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://doi.org/10.1109/tnet.2007.900704

[16] V. Rajendran, K. Obraczka et J. J. Garcia-Luna-Aceves, « Energy-Efficient, collision-free medium access control for wireless sensor networks », Wireless Netw., vol. 12, no 1, p. 63–78, févr. 2006. Consulté le 24 nov. 2025. [En ligne]. Disponible : https://doi.org/10.1007/s11276-006-6151-z

[17] J. Elson et D. Estrin, « Time synchronization for wireless sensor networks », s. d. [En ligne]. Disponible : https://www.circlemud.org/jelson/writings/timesync.pdf

[18] Y. Wu, J. Stankovic, T. He et S. Lin, « Realistic and efficient multi-channel communications in wireless sensor networks », s. d.