

PROTOCOLES MAC DÉDIÉS AUX WSN

5A ISS

Samia Boukouiss

2024/2025

SOMMAIRE

- I. Introduction
- II. Les couches MAC pour les WSN
 - 1. Optimisation énergétique dans les WSN : enjeux et défis au niveau de la couche MAC
 - 2. Les différentes approches pour l'accès aux canaux
- III. Développement de protocoles MAC adaptés aux WSN
 - 1. Protocole de type CAN-LIKE
 - a. Présentation du protocole
 - b. Gestion des problèmes liés à la transmission
 - c. Sécurité, mobilité, scalabilité, consommation d'énergie
 - 2. Protocole Sensor-MAC
 - a. Présentation du protocole
 - b. Gestion des problèmes liés à la transmission
 - c. Sécurité, mobilité, scalabilité, consommation d'énergie
 - 3. Protocole Wise-MAC
 - a. Présentation du protocole
 - b. Gestion des problèmes liés à la transmission
 - c. Sécurité, mobilité, scalabilité, consommation d'énergie
 - 4. Protocole Energy & Rate-MAC
 - a. Présentation du protocole
 - b. Gestion des problèmes liés à la transmission
 - c. Sécurité, mobilité, scalabilité, consommation d'énergie
- IV. Comparaison des WSN protocoles
- V. Références

I. Introduction

La couche **MAC (couche de contrôle d'accès au support physique)** se situe au niveau inférieur de la couche liaison dans le modèle OSI. Elle est chargée de gérer les interactions entre les utilisateurs et le support physique en remplissant plusieurs fonctions clés : synchroniser les débuts et fins de trames, détecter les erreurs de transmission, sélectionner et filtrer les trames pertinentes, réguler l'accès au canal partagé, et garantir un accès équitable et optimal aux utilisateurs du réseau. Ces responsabilités sont définies dans le standard 802.

En tant qu'élément central du modèle OSI, la couche MAC joue un rôle déterminant dans l'amélioration des performances et la préservation de l'intégrité des communications réseau. Elle contribue à l'efficacité opérationnelle et à la qualité des échanges au sein du réseau grâce à une synchronisation rigoureuse des trames, une surveillance active des anomalies de transmission, et des mécanismes de filtrage et de régulation.

II. Les couches MAC pour les WSN

1. Optimisation énergétique dans les WSN : enjeux et défis au niveau de la couche MAC

La conception de protocoles MAC adaptés aux WSN est primordiale, car elle doit prendre en compte des critères tels que la latence, le débit, la bande passante, l'équité, et surtout, l'efficacité énergétique. Ces réseaux, constitués de nombreux nœuds dispersés dans une zone donnée, ont pour rôle de collecter et transmettre des informations. Un réseau multi-sauts se forme lorsque les nœuds communiquent entre eux via des canaux sans fil, permettant ainsi à un ou plusieurs nœuds de transférer des données.

La conception des protocoles MAC doit également intégrer la gestion de l'évolutivité face aux variations de la taille du réseau, telles que l'apparition, la disparition ou le déplacement des nœuds. Cependant, les communications entre nœuds sont énergivores, et certaines caractéristiques de la couche MAC peuvent entraîner un gaspillage important.

Les capteurs sans fil, souvent alimentés par des piles ou batteries difficiles à recharger ou remplacer, nécessitent une gestion minutieuse de l'énergie. Parmi les principales causes de gaspillage figurent la collision des paquets, qui impose des retransmissions coûteuses, l'écoute non désirée de paquets destinés à d'autres nœuds, et l'overhearing, lorsque les nœuds surveillent inutilement un trafic qui ne les concerne pas. Par ailleurs, l'échange de paquets de contrôle excessifs ou la transmission de données peu pertinentes contribuent également à augmenter la consommation énergétique.

2. Les différentes approches pour l'accès aux canaux

FDMA (Frequency Division Multiple Access) est l'une des méthodes d'accès multiples les plus courantes dans les systèmes analogiques. Elle consiste à diviser la bande de fréquence en plusieurs canaux de largeur égale, chaque conversation étant associée à une fréquence distincte. Parmi ses atouts figurent une réduction du débit d'informations grâce à des codes numériques performants, augmentant ainsi la capacité du système. Toutefois, FDMA présente des limites : la capacité par canal est fixe, les bandes de garde entre canaux entraînent une perte de capacité, et l'utilisation de filtres à bande étroite alourdit les coûts matériels.

TDMA (Time Division Multiple Access) repose sur une logique différente. Chaque station mobile bénéficie d'un accès exclusif à une fréquence pendant un créneau horaire spécifique, ce qui nécessite une synchronisation précise entre émetteur et récepteur. Cette méthode se distingue par sa flexibilité, car plusieurs créneaux horaires peuvent être attribués à un même utilisateur, permettant de prendre en charge des trafics à débit variable. Cependant, elle requiert des égaliseurs complexes pour gérer des débits élevés, des temps de garde pour éviter les interférences, et engendre une consommation d'énergie accrue.

CDMA (Code Division Multiple Access) adopte une approche radicalement différente. Au lieu de partager la bande en fréquences ou en temps, il alloue à chaque utilisateur l'accès complet à la bande passante grâce à des codes uniques. Ce système offre une grande souplesse de capacité, une utilisation optimisée des ressources radio, et permet des transmissions en rafales. Néanmoins, il exige une sélection minutieuse des codes, une synchronisation temporelle rigoureuse et un contrôle de puissance précis, au prix d'une consommation d'énergie accrue.

Le protocole **CSMA (Carrier Sense Multiple Access)** est couramment utilisé pour réguler l'accès aux canaux de communication. Son fonctionnement repose sur l'écoute préalable du canal par un nœud avant toute transmission. Si le canal est libre, le nœud peut envoyer ses données ; sinon, il attend ou modifie ses paramètres de transmission pour éviter les collisions. Ce mécanisme optimise l'utilisation du support en réduisant les conflits liés à des émissions simultanées. Le **CSMA/CA (Collision Avoidance)**, largement utilisé dans les réseaux sans fil, ajoute des mesures préventives pour minimiser encore davantage les collisions, rendant ce protocole efficace dans des environnements complexes.

Chacune de ces méthodes (FDMA, TDMA, CDMA, CSMA) présente des forces et des faiblesses. Le choix de la méthode dépendra des contraintes spécifiques et des objectifs visés par le système.

III. Développement de protocoles MAC adaptés aux WSN

1. Protocole de type CAN-LIKE

a. Présentation du protocole

Le protocole **CAN-LIKE** est une évolution du protocole MAC issu du Controller Area Network (CAN), repensée pour s'adapter aux besoins des réseaux locaux sans fil. En reprenant les principes fondamentaux du CAN, comme l'arbitrage par compétition et la gestion hiérarchique des priorités, ce protocole est modifié pour relever les défis spécifiques liés aux communications sans fil.

Son fonctionnement repose sur une séquence organisée en plusieurs étapes : l'écoute du canal, la phase de synchronisation, l'arbitrage et la transmission des données. Ce processus inclut un système d'arbitrage bit par bit qui optimise la gestion des priorités entre nœuds concurrents, garantissant ainsi une transmission fiable et bien coordonnée.

b. Gestion des problèmes liés à la transmission

Le protocole CAN-LIKE adopte le TDMA comme méthode d'accès multiple. Afin de surmonter les défis spécifiques liés aux transmissions dans les réseaux sans fil, il intègre plusieurs mécanismes ingénieux. L'un de ses points forts réside dans son arbitrage compétitif : les nœuds en concurrence transmettent des signaux de synchronisation ainsi que des bits de priorité, permettant ainsi une détection rapide des conflits éventuels et réduisant le risque de collisions.

Pour gérer les décalages temporels causés par la propagation des signaux, le protocole introduit également une fenêtre d'ambiguïté, conçue pour compenser ces variations. Grâce à la combinaison de ces mécanismes, le protocole CAN-LIKE garantit une gestion efficace des transmissions, même dans des environnements sans fil soumis à des délais imprévisibles et à des interférences.

c. Sécurité, mobilité, scalabilité, consommation d'énergie

Concernant la sécurité, le protocole CAN-LIKE hérite des caractéristiques du CAN, notamment sa structure de diffusion, qui le rend vulnérable à certaines attaques comme l'injection de messages ou le spoofing. Ces vulnérabilités résultent de l'absence de mécanismes de sécurité natifs dans le CAN original, ce qui signifie que des messages malveillants peuvent potentiellement être acceptés s'ils semblent conformes. Cependant, dans des implémentations spécifiques adaptées aux réseaux sans fil, des mécanismes supplémentaires sont souvent introduits, comme le chiffrement des données ou l'authentification des nœuds, pour protéger les communications contre les écoutes et les intrusions malveillantes.

De plus, les mécanismes de priorisation et de retransmission propres au protocole incluent parfois des contrôles pour détecter les anomalies, comme les erreurs dans les transmissions ou les comportements atypiques. L'utilisation de contrôles d'intégrité des données, comme les codes de redondance cyclique (CRC), renforce également la détection des altérations. Ces ajouts, bien que non natifs, permettent d'améliorer considérablement la sécurité du protocole dans des contextes où la fiabilité des communications est cruciale.

Concernant la mobilité, le protocole CAN-LIKE rencontre des défis liés à la mobilité des nœuds. La gestion de la mobilité est cruciale, car le mouvement des nœuds peut entraîner des interruptions ou des problèmes de synchronisation des canaux. Le CAN-LIKE, qui repose sur l'accès au canal via le TDMA, peut être affecté par ces variations de position, rendant la synchronisation entre les nœuds plus complexe. Pour atténuer ces effets, des mécanismes supplémentaires sont souvent introduits, comme l'ajustement dynamique des créneaux d'accès et l'utilisation de fenêtres de synchronisation flexibles. Ces ajustements permettent au protocole de mieux s'adapter aux changements dans la topologie du réseau tout en maintenant la communication entre les nœuds mobiles.

La scalabilité du protocole CAN-LIKE fait face à plusieurs défis. D'une part, l'architecture de diffusion de CAN, combinée à la croissance du nombre de nœuds dans un réseau, complique la gestion de l'accès au canal. Avec l'augmentation du nombre de nœuds, des collisions peuvent se produire et la gestion des créneaux d'accès devient plus complexe. Pour surmonter cela, des solutions adaptatives sont nécessaires, comme l'optimisation des créneaux de transmission et l'adaptation dynamique des fenêtres de synchronisation pour mieux gérer la topologie changeante des WSN.

D'autre part, les topologies dynamiques et la mobilité des nœuds augmentent également les défis de scalabilité. Les nœuds mobiles peuvent entraîner des interférences et des pertes de communication, d'où la nécessité de réajustements dynamiques pour maintenir une communication stable. L'usage de protocoles adaptatifs qui ajustent les ressources du réseau et des techniques comme l'agrégation de données et le partitionnement du réseau peuvent également améliorer la scalabilité tout en optimisant l'utilisation des ressources limitées, comme la bande passante et l'énergie des capteurs.

Sur le plan énergétique, le protocole CAN-LIKE cherche à concilier performances réseau et optimisation de la consommation. Grâce à des phases de compétition minutieusement synchronisées et à l'intégration de périodes d'observation, il limite les activités inutiles, réduisant ainsi la consommation d'énergie.

En outre, la structure rigoureuse des différentes phases et la gestion précise des priorités permettent de maximiser l'utilisation des ressources tout en respectant les contraintes temporelles imposées par les applications temps réel. Ce protocole se distingue ainsi par son efficacité, offrant une communication fiable et performante tout en maintenant une consommation énergétique maîtrisée, même dans des environnements sans fil exigeants.

2. Protocole Sensor-MAC

a. Présentation du protocole

Le protocole **Sensor-MAC (S-MAC)** est spécifiquement conçu pour répondre aux besoins des réseaux de capteurs sans fil, où l'optimisation de l'énergie est cruciale. Fonctionnant sur des batteries limitées, ces réseaux nécessitent une gestion efficace des ressources. S-MAC met en œuvre une stratégie périodique d'écoute et de sommeil : les nœuds restent actifs lorsqu'ils reçoivent des données, mais passent en mode sommeil, désactivant leur radio, en l'absence d'activité. Cette périodicité est synchronisée entre les nœuds pour harmoniser leurs cycles de veille et de repos.

b. Gestion des problèmes liés à la transmission

S-MAC traite les défis liés aux transmissions dans les WSN grâce à plusieurs mécanismes. Pour minimiser les collisions, il utilise une détection de porteuse virtuelle basée sur l'échange de paquets RTS/CTS (Request-to-Send/Clear-to-Send). Ce processus permet aux nœuds de vérifier si le canal est occupé avant d'émettre, réduisant ainsi les risques de conflits. En outre, pour limiter l'écoute inutile, S-MAC intègre une signalisation en canal qui incite les nœuds non impliqués à se mettre en mode sommeil, économisant ainsi l'énergie du réseau. Ces solutions combinées garantissent une transmission plus fluide et efficace tout en réduisant les interférences.

c. Sécurité, mobilité, scalabilité, consommation d'énergie

Le protocole S-MAC, étant principalement conçu pour des réseaux de capteurs sans fil à faible consommation d'énergie, ne prend pas en compte les mécanismes de sécurité de manière native. Cela peut le rendre vulnérable à plusieurs types d'attaques, comme l'écoute clandestine, l'injection de messages ou les attaques de déni de service (DoS). Cependant, plusieurs études proposent l'ajout de mécanismes de sécurité au-dessus de ce protocole, comme le chiffrement des données et l'authentification des nœuds pour sécuriser la communication dans les réseaux de capteurs sans fil. Cela permet de protéger les informations échangées et d'assurer l'intégrité des messages malgré l'absence de sécurité native dans S-MAC.

En ce qui concerne la mobilité, la synchronisation temporelle des périodes d'activité et de sommeil des nœuds peut être perturbée par le déplacement des nœuds. Ce mouvement des nœuds complique le maintien de la connectivité et l'efficacité de la communication. Pour améliorer la gestion de la mobilité, des ajustements dynamiques des périodes de sommeil et des fenêtres de synchronisation flexibles ont été introduits pour mieux s'adapter aux changements dans la topologie du réseau.

S-MAC est particulièrement adapté aux réseaux de capteurs sans fil de petite et moyenne taille. Cependant, dans des réseaux plus vastes, la scalabilité peut poser problème, car l'augmentation du nombre de nœuds entraîne davantage de collisions et une gestion plus complexe des créneaux d'accès. Pour pallier ce problème, des solutions telles que l'adaptation

dynamique de la taille des fenêtres de synchronisation et l'optimisation des cycles d'activité ont été proposées, afin d'améliorer l'efficacité du réseau sans nuire à sa performance.

La réduction de la consommation énergétique est au cœur des priorités de S-MAC. Le protocole permet aux nœuds de rester en mode sommeil pendant des périodes définies, réduisant ainsi la consommation lors des phases d'inactivité. Pendant les phases actives, l'énergie est également optimisée grâce à la synchronisation des cycles de réveil et à l'ajustement dynamique des périodes de sommeil en fonction de la charge de trafic. Ces optimisations prolongent la durée de vie des nœuds et renforcent la résilience du réseau. Selon une étude [4], un nœud utilisant S-MAC consomme environ 450 mJ en mode émission, illustrant son efficacité énergétique dans un contexte réel.

3. Protocole Wise-MAC

a. Présentation du protocole

Le protocole **Wise-MAC** a été développé pour fonctionner avec la puce système WiseNET, conçue par le CSEM. Cette puce intègre un émetteur-récepteur radio FSK à faible consommation (double bande 434 et 868 MHz), un microcontrôleur CoolRISC 8 bits optimisé pour une basse consommation, une mémoire vive, ainsi que des interfaces numériques et analogiques. Fonctionnant avec une tension comprise entre 0,9 V et 1,5 V, WiseNET peut utiliser une pile alcaline simple et économique comme source d'alimentation. Ce transceiver se distingue par sa très faible consommation énergétique de 2 mA en mode réception et sa latence de mise sous tension réduite à 800 μ s.

b. Gestion des problèmes liés à la transmission

Wise-MAC propose plusieurs mécanismes pour gérer les transmissions dans des environnements à risques de collisions. Une détection de porteuse non persistante est mise en œuvre, avec un temps d'attente calculé comme un entier aléatoire multiplié par le temps de basculement du transceiver. Afin de prévenir les collisions impliquant plusieurs nœuds tentant de transmettre simultanément au même relais, Wise-MAC intègre un préambule de réservation basé sur le protocole CSMA avec un support de durée aléatoire avant l'envoi du préambule de réveil.

Pour traiter les problèmes liés au nœud caché, la portée de détection de porteuse est étendue au-delà de la portée d'interférence. Cependant, cette extension se fait au prix d'une diminution de la capacité du réseau.

c. Sécurité, mobilité, scalabilité, consommation d'énergie

Le protocole Wise-MAC, tout comme son prédécesseur S-MAC, ne dispose pas de mécanismes de sécurité natifs, ce qui le rend vulnérable à des attaques telles que l'écoute clandestine ou l'injection de messages. Pour sécuriser les communications, des solutions additionnelles comme le chiffrement des données et l'authentification des nœuds peuvent être appliquées, mais ces ajouts peuvent impacter l'efficacité énergétique et la latence du réseau.

La mobilité dans Wise-MAC reste un défi, car le déplacement des nœuds perturbe la synchronisation temporelle nécessaire à son fonctionnement. Pour y remédier, des mécanismes tels que l'ajustement dynamique des périodes de sommeil et l'utilisation de fenêtres de synchronisation flexibles permettent de maintenir la connectivité et de réduire l'impact des mouvements, bien que ces solutions soient limitées dans des environnements très mobiles.

Wise-MAC éprouve des difficultés à s'adapter à de grands réseaux en raison de l'augmentation des collisions et de la complexité de synchronisation. Pour contrer cela, il intègre des mécanismes adaptatifs comme la réduction des transmissions inutiles et l'agrégation de données. Ces approches limitent la surcharge de communication tout en optimisant la gestion énergétique et les ressources réseau.

Wise-MAC optimise l'énergie grâce à une technique d'échantillonnage périodique du préambule,

où les nœuds détectent l'activité sur le support à intervalles réguliers et ajustent leur état actif uniquement lorsque nécessaire. Un préambule de réveil est envoyé avant chaque message pour synchroniser les récepteurs avec précision, évitant une écoute passive prolongée.

En parallèle, une table dynamique contenant les horaires d'échantillonnage des voisins permet d'adapter la durée des préambules selon le trafic. Ce double mécanisme réduit les réveils inutiles, offrant une consommation énergétique efficace, même avec des charges de trafic fluctuantes.

4. Protocole Energy & Rate-MAC

a. Présentation du protocole

Le protocole ER-MAC a été développé pour répondre aux exigences des WSN en optimisant la consommation d'énergie. Contrairement à d'autres protocoles MAC qui priorisent le débit ou l'équité, ER-MAC se concentre sur la prolongation de la durée de vie des nœuds dans des environnements à ressources limitées.

b. Gestion des problèmes liés à la transmission

ER-MAC utilise une approche TDMA qui élimine les collisions et réduit les écoutes inutiles, tout en limitant les surcharges dues aux paquets de contrôle. Les nœuds ajustent leurs créneaux de transmission en fonction de leur niveau d'énergie résiduelle et du taux de trafic des voisins.

Lorsqu'un nœud atteint un niveau critique d'énergie, une phase de vote est initiée, permettant aux nœuds les plus sollicités de prolonger leurs périodes de sommeil. Cette stratégie équilibre la consommation énergétique et assure une utilisation optimale des ressources, prolongeant ainsi la durée de vie du réseau.

c. Sécurité, mobilité, scalabilité, consommation d'énergie

ER-MAC n'intègre pas de mécanismes de sécurité natifs. Il est lui aussi exposé à des attaques telles que l'écoute clandestine, l'injection de données ou les attaques par déni de service (DoS). Pour renforcer la sécurité, des solutions complémentaires comme le chiffrement des données ou l'authentification des nœuds peuvent être ajoutées, bien qu'elles augmentent la complexité et la consommation énergétique.

Il est conçu pour des réseaux statiques et offre une gestion limitée de la mobilité. Le déplacement des nœuds peut entraîner une dégradation des performances, notamment en termes de perte de connectivité et de synchronisation. Des adaptations comme l'ajustement dynamique des paramètres de communication ou la reconfiguration automatique du réseau peuvent améliorer sa robustesse face à la mobilité, mais elles ne sont pas natives au protocole.

Il gère efficacement les petits et moyens réseaux, mais sa scalabilité dans des réseaux très denses est limitée. L'augmentation du nombre de nœuds entraîne des défis liés à la gestion des cycles d'accès et à la coordination, augmentant les risques de collisions et de latence. Des mécanismes adaptatifs, tels que l'agrégation de données et la gestion dynamique des cycles d'accès, peuvent améliorer la scalabilité dans des réseaux plus larges.

ER-MAC a démontré une amélioration significative en matière d'efficacité énergétique grâce à des simulations effectuées avec le logiciel ns-2. Le protocole ajuste dynamiquement les créneaux de transmission en fonction de la criticité énergétique des nœuds, ce qui permet d'optimiser l'utilisation des ressources tout en s'adaptant aux conditions changeantes du réseau.

Les résultats des simulations montrent que le protocole conserve une excellente efficacité énergétique, même avec une augmentation modérée de la charge de trafic. Cette adaptabilité fait d'ER-MAC une solution robuste pour les WSN, répondant aux défis de la gestion de l'énergie dans des environnements contraints.

IV. Comparaison des WSN protocoles

Quatre protocoles de communication dédiés aux WSN ont été explorés et comparés dans ce document : Wise-MAC, Energy & Rate-MAC, CAN-LIKE MAC et Sensor-MAC. Ces protocoles, chacun avec ses particularités, visent à répondre aux multiples besoins du marché des capteurs sans fil.

Les protocoles S-MAC et Wise-MAC se concentrent principalement sur la réduction de la consommation d'énergie via des cycles de sommeil et des mécanismes d'écoute passive, mais leurs performances se dégradent dans des réseaux denses ou mobiles. S-MAC est limité par la scalabilité et la gestion de la mobilité, tandis que Wise-MAC améliore l'efficacité énergétique, mais peine à gérer les réseaux dynamiques.

En revanche, ER-MAC et Energy & Rate-MAC sont plus adaptés aux réseaux plus grands et denses. Ils ajustent dynamiquement les créneaux de transmission en fonction de l'énergie restante des nœuds, ce qui améliore leur efficacité et leur scalabilité, bien qu'ils nécessitent des mécanismes adaptatifs pour gérer les collisions et la latence dans des réseaux très denses.

Tous les protocoles manquent de sécurité native, ce qui nécessite des ajouts externes pouvant affecter l'efficacité énergétique. ER-MAC et Energy & Rate-MAC sont les plus flexibles et performants dans des environnements changeants, tandis que S-MAC et Wise-MAC conviennent mieux aux réseaux statiques et à faible densité.

Le choix d'un protocole doit donc s'appuyer sur une analyse approfondie des besoins spécifiques de l'environnement, en tenant compte des forces et des limites de chaque approche pour atteindre un équilibre optimal.

V. Références

- [1] IEEE 802, https://fr.wikipedia.org/wiki/IEEE_802
- [2] TDMA and CDMA in Mobile Communications Arun A Bhatji, A Thesis submitted to the Department of Electrical and Computer Engineering in partial fulfillment of the requirements for the degree of Master of Science.
<https://diginole.lib.fsu.edu/islandora/object/fsu%3A175931/datastream/PDF/view>
- [3] Approche inter-couches pour l'économie d'énergie et la fiabilité dans les Réseaux de Capteurs Sans Fil dédiés aux Applications Critiques de Surveillance, Ali Benzerbadj
https://www.researchgate.net/publication/328212038_Approche_inter-couches_pour_l%27economie_d%27energie_et_la_fiabilite_dans_les_Reseaux_de_Capteurs_Sans_Fil_dedies_aux_Applications_Critiques_de_Surveillance
- [4] Ye, Wei, J. Heidemann, et D. Estrin. « An energy-efficient MAC protocol for wireless sensor networks ». In Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, 3:1567-76 vol.3, 2002.
<https://doi.org/10.1109/INFCOM.2002.1019408>
- [5] Xuan Hung Nguyen, Gérard Mouney. Spécification du protocole > pour la couche MAC des réseaux locaux sans fil. Ecole d'Été Temps Réel 2011 (ETR'11), Aug 2011, Brest, France. pp.195-198. fhal00656663f <https://hal.science/hal-00656663/document>
- [6] WiseMAC, an ultra low power MAC protocol for the wiseNET wireless sensor network, A. El-Hoiydi, J.-D. Decotignie, C. Enz and E. Le Roux Swiss Center for Electronics and Microtechnology (CSEM SA)
https://www.researchgate.net/publication/221091751_WiseMAC_an_ultra_low_power_MAC_protocol_for_the_wiseNET_wireless_sensor_network
- [7] Energy Consumption Reduction in S-MAC Protocol for Wireless Sensor Network Author links open overlay panel. Jagriti a, D.K Lobiyal b, India Available online 19 November 2018
<https://www.sciencedirect.com/science/article/pii/S1877050918321264>
- [8] Energy and Rate based MAC Protocol for Wireless Sensor Networks Rajgopal Kannan Ram Kalidindi S. S. Iyengar Department of Computer Science Louisiana State University
https://www.researchgate.net/publication/220415861_Energy_and_rate_based_MAC_protocol_for_wireless_sensor_networks
- [9] S2-CAN: Sufficiently Secure Controller Area Network, Mert D. Pesé, Jay W. Schauer, Junhui Li, and Kang G. Shin
<https://rtcl.eecs.umich.edu/rtclweb/assets/publications/2021/acsac21-pese.pdf>
- [10] Scalability Analysis for Wireless Sensor Networks Routing Protocols, Lubna K. Alazzawi; Ali M. Elkateeb; Aiyappa Ramesh; Waleed Aljuhar
<https://ieeexplore.ieee.org/document/4482903>