УДК 621.39

Максимов В.В., Литвин О.О.
Національний технічний університет України «Київський політехнічний інститут ім. Ігора Сікорського»

МЕТОДИ ВИРІШЕННЯ ПРОБЛЕМИ ПРИХОВАНИХ ТА НЕЗАХИЩЕНИХ ВУЗЛІВ В БЕЗПРОВОДОВИХ AD-HOC МЕРЕЖАХ

Maksymov V.V., Lytvyn O.O. Methods for solving the hidden and exposed problem in wireless Ad-Hoc networks. The problems of hidden and exposed terminals were described in the paper. The classification, which deals with protocols that have the ability to solve hidden and exposed terminal problems, and are separated on the basis of media access into five groups, was proposed. The concept of effective MAC layer protocol of wireless Ad Hoc networks was also proposed, namely the protocol must use multi-channel separation for separating the service information from the data; The protocol should have the least amount of control messages to avoid delays growth; the protocol must be ensured control the direction and power of the antenna; QoS support should be provided; presence in the protocol grouping mechanism or routing control. Afterall, we describe the ways of effective implementation of the MAC layer protocol, which were studied.

Keywords: Ad Hoc network, MAC, DCF, PCF, RTS / CTS, QoS, hidden nodes, unprotected sites

Максимов В.В., Литвин О.О. Методи вирішення проблеми прихованих та незахищених вузлів в безпроводових Ad Hoc мережах. Запропоновано концепт ефективного протоколу MAC рівня безпроводових Ad Hoc мереж, а саме: протокол повинен використовувати багатоканальне розділення, для відокремлення службової інформації від даних; протокол повинен мати найменшу кількість службових повідомлень для уникнення зростання затримок; в протоколі повинно забезпечуватись управління спрямованістю та потужністю антени; повинна забезпечуватися підтримка QoS; наявність у протоколі механізму групування чи управління маршрутизацією.

***Ключові слова*:** Ad Hoc мережі, MAC, DCF, PCF, RTS/CTS, QoS, приховані вузли

Максимов В.В., Литвин О.О. Методы решения проблемы скрытых и незащищенных узлов в беспроводных Ad-Hoc сетях. Предложен концепт эффективного протокола MAC уровня беспроводных Ad Hoc сетей, а именно: протокол должен использовать многоканальное разделение, для отделения служебной информации от данных; протокол должен иметь наименьшее количество служебных сообщений во избежание роста задержек; в протоколе должно обеспечиваться управление направленностью и мощностью антенны; должна обеспечиваться поддержка QoS; наличие в протоколе механизма группировки или управления маршрутизацией.

Ключевые слова: Ad Hoc сети, MAC, DCF, PCF, RTS / CTS, QoS, скрытые узлы,

1. Вступ. Ad Hoc мережі – це тимчасові безпроводові мережі, які створюються спонтанно, при цьому не маючи потреби у наявності спеціального обладнання, точок доступу, не потребують наявності чіткої інфраструктури та централізованого управління. Здійснення всіх цих умов відбувається розподілено, на рівні кожного вузла. Такі мережі є незамінними у певних ситуаціях, як, наприклад, місця проведення бойових дій чи стихійних лих, будь-які інші місця спонтанного скупчення людей, де незалежно від рухомості станції користувач може підключитися до мережі чи відімкнутися за власним бажанням.

В таких мережах кожен вузол виступає у ролі ретранслятора для свого сусіда. При здійсненні такого зв'язку існує дві основні проблеми: прихованих та незахищених вузлів. У зв'язку із тим, що дані проблеми в деяких випадках [1] можуть призводити до повної відсутності зв'язку, їх вирішенню присвячено багато зусиль. Ці проблеми вирішуються на MAC (Medium Access Control) рівні, який призначений для ефективного розподілу ресурсів зв'язку і в значній мірі впливає на показники продуктивності мережі, такі як пропускна здатність, затримки, рівноймовірність доступу до середовища.

На MAC рівні протоколу 802.11 визначено 2 типи спільного доступу до середовища передавання даних: DCF (Distributed Coordination Function) – функція розподіленої координації і PCF (Point Coordination Function) – функція централізованої координації. В Ad Hoc мережах використовується функція DCF, тобто для забезпечення спільного доступу достатньо щоб вузли здійснювали передавання в моменти, коли середовище вільне. Окрім цього, вузлам потрібно гарантувати рівноймовірний доступ до середовища та механізм уникнення колізій, оскільки вони дуже часто виникатимуть, якщо вузли одночасно

прийматимуть рішення про доступність середовища. Також не потрібно забувати про те, що мобільні вузли, як правило, мають обмежений енергетичний ресурс і тому потрібно враховувати здатність протоколу до ефективного використання ресурсу батареї. Для повністю розподілених мереж із випадковим доступом забезпечення цих умов є досить проблемним, що й призводить до великої різноманітності протоколів MAC рівня.

Таким чином ***актуальною*** є задача розробки такого протоколу MAC рівня, який не лише вирішує проблеми прихованих та незахищених вузлів, але й при цьому не має механізмів, які призводять до погіршення показників продуктивності мережі. Одним із шляхів вирішення цієї задачі є створення класифікації протоколів, ознакою яких виступає спосіб доступу до середовища і здатність вирішувати проблеми прихованих та незахищених вузлів.

Метою даної роботи є пошук шляхів по вдосконаленню існуючих протоколів і, на основі розробленої класифікації, з урахуванням ключових особливостей, переваг та недоліків груп та протоколів, які до них входять, надання пропозицій по створенню нових, які можуть вирішити задачу ефективного управління доступом до середовища. Слід відзначити, що в даній роботі протоколи, які не мають необхідних механізмів для вирішення проблем прихованих та незахищених вузлів, не розглядаються.

2. Проблеми прихованих та незахищених вузлів. В безпроводових Ad-Hoc мережах, в умовах недетермінованого по часу початку передавання, виникає проблема, яка називається проблемою прихованих вузлів [2]. Вона добре вивчена для безпроводових мереж, в яких використовуються точки доступу. Для даних мереж існують механізми, на зразок RTS/CTS, які дозволяють ефективно боротися з нею.

У розподілених мережах ситуація інакша. Пояснити виникнення проблеми прихованих вузлів можна на такому прикладі: нехай є два передавачі, які знаходяться в межах доступу отримувача, але недоступні один відносно іншого. При одночасній відправці даних, коли обидва передавачі приймуть рішення, що середовище вільне, у результаті зіткнення отримувач не зможе прийняти інформацію ні від першого, ні від другого відправника.

Дана проблема має негативний вплив на ефективність, енергоспоживання, затримки передавання та QoS. Як показано у [3], більше 40% пакетів втрачається внаслідок виникнення проблеми прихованих вузлів, а із збільшенням кількості вузлів у мережі відбувається зростання кількості втрачених пакетів, варто відмітити, що таке зростання являється лавиноподібним.

Алгоритм RTS/CTS призначений для уникнення ситуації виникнення колізії у зв’язку із наявністю прихованих вузлів в мережі [4]. У відповідності до даного алгоритму, кожен вузол, перед початком передавання даних повинен здійснити передавання спеціального контрольного повідомлення RTS (запит на передавання). Дане повідомлення містить інформацію про тривалість передачі та отримувача. Інші вузли повинні утримуватися від передавання протягом заданого періоду часу. Якщо дане повідомлення доходить до отримувача, він повинен відповісти контрольним повідомленням CTS (готовність до передавання). Після цього передавач відправляє дані, а отримувач здійснює відправлення пакета підтвердження успішного передавання ACK.

В розподілених мережах такий механізм призводить до виникнення ситуації, у якій вузол не може здійснювати передавання, оскільки приймає хибне рішення про зайнятість середовища у зв’язку із передаванням в цей момент його сусідом до іншого вузла [3]. Пояснити це можна на такому прикладі. Нехай є два передавачі S1, S2 та два отримувачі R1, R2 і вони розташовані так, що отримувачі доступні один відносно іншого, а кожному з передавачів доступен лише свій отримувач. Якщо обидва з передавачів відішлють RTS своїм отримувачам, то перший з них, хто у відповідь згенерує і відправить CTS, заблокує роботу іншого отримувача, так як той, почувши CTS перейде в стан очікування. Тобто прийме помилкове рішення про те, що буде перешкоджати передавати дані іншому. По суті, механізм RTS/CTS, який призначений вирішувати проблему прихованого вузла, породжує іншу проблему – незахищеного вузла.

3. Класифікація протоколів MAC рівня. Стрімкий розвиток протоколів, разом із вирішенням поставлених задач породжує велику кількість запитань та створює ще більшу кількість нових завдань. Спроби систематизувати величезну кількість механізмів, протоколів неперервно продовжуються до сьогоднішнього дня. Відповідно на даний час існує багато варіантів класифікацій. Так у класифікації, запропонованій в [5] (2004 р.), протоколи описуються за 6-ма ключовими ознаками: розподілення каналів і доступу, топологія, потужність, ініціація передавання, дальність дії, завантаження мережі та масштабування. Розподілення каналів і доступу виділяється як одна категорія, оскільки степінь мультиплексування в кожному протоколі тісно пов'язана із алгоритмом уникнення колізій. Інша ознака, завантаження мережі та масштабування описують, по суті, показники продуктивності MAC протоколів. На думку авторів, також необхідно враховувати топологію, оскільки розглянуті ними протоколи мають дуже широкий спектр топологій. В Ad-Hoc мережах, на відміну від централізованих, ініціатором передавання може виступати і отримувач, тому вводиться ще одна ознака: ініціація передавання.

В [6] (2011 р.) ключовою ознакою виступає діаграма спрямованості антен та спосіб доступу до середовища – випадковий чи синхронізований. Варто відмітити, що в даній класифікації протоколи із випадковим доступом в свою чергу поділяються за ознакою уникнення колізій із використанням контрольних RTS/CTS пакетів та тонів зайнятості.

У варіанті, що запропонований в [3] (2012 р.), протоколи поділяються за трьома ключовими ознаками доступу до середовища: із використанням механізму рукостискання, використанням тонів зайнятості та механізмів управління маршрутизацією. Генеалогічне представлення даних протоколів демонструє, що більшість із них були розроблені на основі механізму MACA і використовують рукостискання як підтвердження зв'язку.

Найбільш актуальний та повний варіант класифікації відображено в [7-10] (2011-2014 р.р.). Протоколи поділяються за ознакою доступу до каналу на основі конкуренції, із механізмом планування, резервування та інші, які не використовують конкурентний доступ. Така класифікація вважалася універсальною, але із розробленням нових протоколів та алгоритмів, її недостатньо для того, щоб побачити всю картину.

Пропонується варіант класифікації (рис. 1), який характеризує протоколи MAC рівня як за способом доступу до середовища, так і за можливістю вирішення проблеми прихованих чи незахищених вузлів (на рисунку позначення ПВ означає вирішення протоколами проблеми прихованих вузлів, ПНВ – вирішення протоколами проблеми прихованих і незахищених вузлів). За її основу взято варіант класифікації, відображений у [7-10].

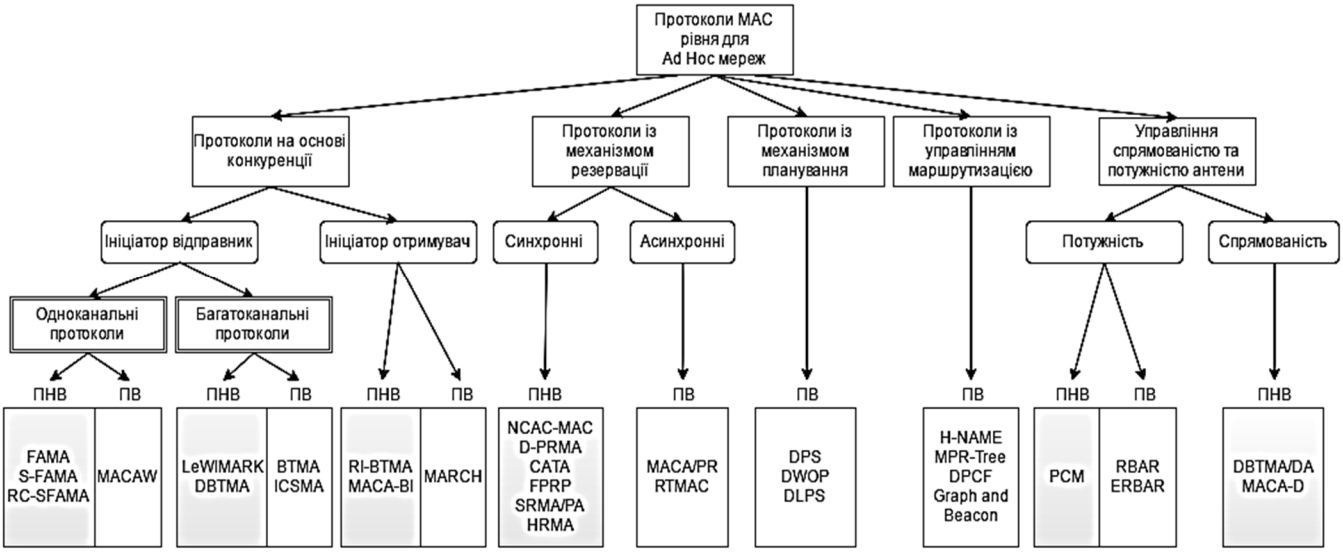

Рис. 1 Класифікація протоколів MAC рівня безпроводових Ad Hoc мереж

Класифікація включає 5 груп: протоколи на основі конкуренції, із механізмом резервування, із механізмом планування, із управлінням маршрутизацією та управлінням параметрами антени.

Протоколи на основі конкурентного доступу, в залежності від того який вузол виступає ініціатором передавання, поділяються на дві категорії: ініціатор відправник і отримувач. По кількості каналів, протоколи поділяються на багатоканальні та одноканальні. У багатоканальних протоколах відбувається розподілення службових пакетів та корисної інформації, що призводить до зменшення ймовірності виникнення колізій, та разом із тим до підвищення продуктивності мережі. Незалежно від того, багатоканальні це протоколи чи одноканальні, із ініціатором відправником чи отримувачем, доступ у них до середовища базується на основі конкурування і наперед не відомо, який із вузлів отримає доступ, тому недоліком таких протоколів є те, що вони не мають можливості забезпечувати QoS.

В окремі групи виділені протоколи із використанням механізмів планування та резервування на використання ресурсів мережі. Це може бути або частотний ресурс, або часові слоти. Наявність наперед відомого графіку передавання створює сприятливі умови для забезпечення такими протоколами QoS. Протоколи із механізмом резервування в свою чергу поділяються на синхронні, в яких для забезпечення встановлення зв'язку та успішного резервування відбувається синхронізація між усіма вузлами, та асинхронні, в яких така синхронізація не відбувається і відповідно економиться час на інші потреби.

Як було сказано раніше, особливістю Ad Hoc мереж є рівноправність всіх вузлів в мережі при відсутності будь якого централізованого управління. Але все більшого значення набувають протоколи із управлінням маршрутизацією (четверта група), які використовують різні механізми групування, графів, дерев багатоточкової ретрансляції. Вони активно застосовуються у сенсорних мережах, але також знаходять своє застосування і у Ad Hoc мережах, хоча в таких протоколах значна частина часу витрачається на службові операції.

В п'ятій групі відображено протоколи, в яких доступ до середовища відбувається за допомогою управління параметрами антени – потужністю та спрямованістю. Окрім цих переваг використання спрямованих антен – мінімумальна інтерференція, відсутність завади передаванню сусідів, збільшення кількості одночасних передавань в каналі, їх недоліком є складність у коректному визначенні спрямованості антен одна відносно іншої.

4. Аналіз протоколів. Маючи класифікацію протоколів, наступним кроком необхідно виділити серед них ті, які мають найбільшу користь із точки зору поставленої задачі. Окрім вирішення проблем прихованих та незахищених вузлів, вони повинні мати мінімальні затримки (тобто час, який був проведений, поки пакет був в черзі на MAC рівні), пропускна здатність повинна виділятися здебільшого на передавання даних, а не службової інформації, забезпечення рівноймовірного доступу до середовища і також повинно забезпечуватися оптимальне використання енергії.

Видно, що протоколи, які вирішують проблему незахищених вузлів, вирішують і проблему прихованих вузлів, але не навпаки і, відповідно, більший інтерес представляють протоколи, які дозволяють вирішувати обидві проблеми. Функціонал протоколів першої категорії гармонічно доповнює один одного, при цьому забезпечуючи виправлення їхніх недоліків. Основна ідея протоколу FAMA [12] – це підбір тривалості контрольних пакетів, але таке рішення призводить до надлишкового збільшення часу передавання та використання енергії. Частковим вирішенням цієї проблеми є протокол S-FAMA [12], в якому час поділяється на слоти, щоб кожен вузол мав "маячок" початку передавання і здійснював конкурування за певні слоти. В свою чергу це конкурування призводить до того, що мережа перевантажується контрольними повідомленнями, виникає багато колізій. Рішенням є протокол RC-SFAMA [12], який дозволяє обмежити кількість RTS повідомлень.

Використання кількох каналів дозволяє забезпечити значно кращу пропускну здатність: так протокол BTMA [13] має кращі показники продуктивності ніж одноканальні протоколи. Але у даних протоколів можуть виникати колізії службових сигналів на виділеному каналі у

випадку зростання завантаження мережі. В такому випадку значно кращі показники продуктивності і можливості вирішення проблем прихованих та незахищених вузлів демонструє протокол DBTMA [3]. Його недоліком є необхідність у доволі складному обладнанні, а також слабка завадостійкість. В розгляді поставленої задачі, найбільш ефективним є протокол Le-WIMARK [14], який має кращі показники пропускної здатності та затримки, більшу завадостійкість, як при високому так і при низькому завантаженні мережі.

Основною перевагою протоколів із ініціатором отримувачем є той факт, що у звичайних протоколах, вузол повинен перемикатися між режимами передавання/приймання (відправки RTS, отримання CTS), що вносить певні затримки. У протоколі MACA-BI [15] на відміну від його попередника MACA використовується двосторонній обмін інформацією. Але ці протоколи ефективні лише у деяких варіантах застосувань Ad-Hoc мереж, в інших випадках обмеження, такі як наявність алгоритму прогнозування трафіку, довжина черги очікування та швидкість отримання пакетів на стороні відправника, призводять до неефективності даного протоколу.

Серед протоколів із механізмом резервації найбільший інтерес складає протокол CATA [16], який забезпечує резервування часових слотів, гарантуючи вирішення проблеми прихованих та незахищених вузлів. Висока продуктивність забезпечується завдяки підбору тривалості часових слотів на основі теорем, запропонованих винахідниками протоколу. Його недоліком є механізми відстрочки передавання, які потребують вдосконалення.

Процес забезпечення повноцінного планування у розподілених децентралізованих Ad Hoc мережах складний, тому протоколи 3-ї категорії не мають необхідних механізмів для вирішення проблеми незахищених вузлів, а їх особливості використовуються як додатковий функціонал в інших категоріях, як наприклад у протоколах із механізмом резервування чи управління маршрутизацією де потрібно встановлювати пріоритети серед потоків.

У відповідності із [3] основною проблемою протоколів з управлінням маршрутизацією є те, що в основі в них закладений механізм MACAW, а це призводить до того, що вони не здатні вирішувати проблеми незахищених вузлів. Серед протоколів даної категорії найбільш привабливим виступає протокол на основі графів, але при збільшенні кількості вузлів у мережі його використання стає неможливим. На цьому фоні виділяється протокол DPCF, який має високі показники продуктивності навіть при великій кількості сусідів, при цьому не вносячи затримок.

За рахунок спрямованості антен в протоколах MAC рівня збільшується відношення сигнал/шум для тієї ж потужності сигналу, що передається. Це дозволяє і забезпечити більшу дальність дії протоколу, що приводить до зменшення кількості скачків при передаванні і зменшенні затримок. Основним недоліком є алгоритми визначення напряму антени одна відносно іншої.

Протокол PCM [17], який періодично збільшує потужність під час передавання, забезпечує економію енергії, не зменшуючи при цьому пропускної здатності. Проблемою цього протоколу є складний механізм реалізації змінної потужності передавання. Для рішення цього питання використовується заміна високого рівня потужності для даних тоном зайнятості на максимальній потужності у виділеному каналі. Також значного погіршення при роботі даного протоколу задають завмирання в каналі. Тобто доводиться іти на компроміс між продуктивністю протоколу і енергозберіганням.

Протоколи із використанням спрямованих антен є перспективним рішенням для багатьох застосувань Ad Hoc мереж. Для прикладу протокол DBTMA/DA [18], який є розширенням DBTMA, має вдвічі вищі показники пропускної здатності і вдвічі менший час затримок. Така ж ситуація спостерігається і для протоколу MACA-D. Не дивлячись на це, у цієї технології є свої проблеми, які пов’язані як в цілому із роботою спрямованих антен (наприклад, асиметричність коефіцієнту підсилення, виникнення зон глухоти, блокування “керівника лінії” [19]), так і особливостями протоколів (наприклад, для протоколу MACA-D основна проблема, це визначення напряму вузлів один відносно іншого).

5. Варіанти вдосконалення протоколів. ***Перший варіант*** передбачає вдосконалення існуючих протоколів. Можна виділити два протоколи, CATA і Le-WIMARK. які вирішують проблеми прихованих та незахищених вузлів, але при цьому є шляхи вдосконалення алгоритмів їх роботи для покращення продуктивності. Наприклад, для протоколу Le-WIMARK одним із варіантів є зміна тривалості інтервалу очікування, або зміна структури службового повідомлення "StatusMessage", або ж спроба переконфігурації протоколу для роботи із спрямованими антенами. Для протоколу CATA основним напрямом є вдосконалення механізмів відстрочки та підбір найбільш оптимальної тривалості кадрів, на основі модернізації або заміни основних теорем, на яких базується робота протоколу.

Другий варіант полягає в об'єднанні алгоритмів роботи кількох механізмів в один. Наприклад, серед протоколів із управлінням маршрутизацією основною проблемою є їх синтез із механізмом MACA, який не може вирішувати ні проблему прихованих вузлів, ні незахищених, і, відповідно, такі синтезовані протоколи не є досконалими. Тому одним із варіантів є модифікація існуючого протоколу MPR-Tree чи DPCF і заміна MACA на інший протокол, для прикладу MACA-BI, який належить до групи протоколів із ініціатором отримувачем або ж MACA-D, який використовує спрямовані антени. При виборі протоколу для поєднання не слід забувати і про спробу зменшити кількість службових повідомлень, тому деякі поєднання взагалі неможливі з цієї точки зору.

6. Висновки. В роботі розглянуто проблеми прихованих та незахищених вузлів і протоколи, які дозволяють їх вирішувати. У зв'язку із необхідністю систематизувати інформацію про велику кількість протоколів, запропоновано класифікацію, в якій розглядаються протоколи, що мають можливість вирішувати проблеми прихованих та незахищених вузлів та поділені за ознакою доступу до середовища на 5 груп: на основі конкуренції, із механізмами резервування, планування, управлінням маршрутизацією та управлінням параметрами антени.

Запропоновано концепт ефективного протоколу MAC рівня безпроводових Ad Hoc мереж: протокол повинен використовувати багатоканальне розділення, для відокремлення службової інформації від даних, цим самим зменшуючи ймовірність виникнення колізії; наявність в протоколі якомога меншої кількості службових повідомлень для уникнення зростання затримок; в протоколі повинно забезпечуватись управління спрямованістю та потужністю антени; повинна забезпечуватися підтримка QoS; наявність у протоколі механізму групування чи управління маршрутизацією.

Література

1. Thierry Plesse. OLSR Performance Measurement in a Military Mobile Ad-hoc Network [Електронний ресурс] / Thierry Plesse, Jerome Lecomte, Cedric Adjih, Marc Badel, Philippe Jacquet, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Adokoe Plakoo // – Режим доступу: https://ai2-s2-pdfs.s3.amazonaws.com/7281/4b08c628ddcb52074b3d004dba9db5fcbf93.pdf.

2. Jayasuriya Aruna. Hiddenvs. Exposed Terminal Problem in Ad hoc Networks [Електронний ресурс] / Aruna Jayasuriya, Sylvie Perreau, Arek Dadej // University of South Australia. – 2004. – Режим доступу: http://www.sandilands.info/sgordon/doc/jayasuriya2004-hidden.pdf

3. Boroumand L. A Review of Techniques to Resolve the Hidden Node Problem in Wireless Networks / L. Boroumand, R.H. Khokhar, L.A. Bakhtiar // Smart Computing Review. – April 2012. – Vol. 2, No. 2. –PP. 95-109.

4. Протоколы беспроводных сетей семейства 802.11 // [Електронний ресурс] – Режим доступу: http://compress.ru/article.aspx?id=10805

5. Jurdak R. A survey, classification and comparative analysis of medium access control protocols for ad hoc networks / R.Jurdak, C.V. Lopes // IEEE Communications. – 2004. – Vol. 6, No. 1. – PP. 2-16.

6. Bazan O. A Survey On MAC Protocols for Wireless Adhoc Networks with Beamforming Antennas [Електронний ресурс] / O. Bazan, M. Jaseemuddin // IEEE Communications Surveys, 10 January 2011. – Режим доступу: https://www.researchgate.net/publication/224231689_

7. MAC Protocols for Ad Hoc and Sensor Networks [Електронний ресурс] // Computer and Communication Systems, [WSN] Winter 2011/2012. – Режим доступу: http://www.ccs-labs.org/teaching/wsn/2011w/04-mac.pdf.

8. Moltchanov D.A. MAC protocols [Електронний ресурс] / D.A. Moltchanov // TUT, 2011. – Режим доступу: http://www.cs.tut.fi/kurssit/TLT-2616/lect04.pdf.

9. Prakash C. Ad Hoc Wireless Media Access Protocols [Електронний ресурс] / C. Prakash // Lovely Professional University, Punjab 2013. – Режим доступу: http://www.slideshare.net/cprakash2011/lecture-7-8-ad-hoc-wireless-media-access-protocols.

10. J. P. Sheu J.P. MAC Protocols for Ad Hoc Wireless Networks [Електронний ресурс] / J. P. Sheu. – Режим доступу: http://hscc.cs.nthu.edu.tw/~sheujp/lecture_note/wn_Chapter_6_MAC.pdf // 2014.

11. Garcia-Luna-Aceves J.J. Floor Acquisition Multiple Access (FAMA) in Single-Channel Wireless Network [Електронний ресурс] / J.J. Garcia-Luna-Aceves, Chane L. Fullmer // Computer Engineering Department, University of California, 1998. – Режим доступу: https://ccrg.soe.ucsc.edu/publications/ chane.monet97.pdf.

12. Liang-fang Qian. A slotted floor acquisition multiple access based MAC protocol for underwater acoustic networks with RTS competition / Liang-fang Qian, Sen-lin Zhang // Frontiers of Information Technology & Electronic Engineering. – March 2015. – Volume 16, issue 3. – PP 217-226.

13. Al-Mahdi H. Collision reduction mechanism for masked node problem in ad hoc networks / H. Al-Mahdi, M.A. Kalil, F. Liers, A. Mitschele-Thiel // AEU – International Journal of Electronics and Communications. – Sep. 2009. – Vol. 63, No. 9. – PP. 754-776.

14. Kalfas G. Le-wimark: An intelligent power-efficient ad hoc mac protocol with busy tone and power control [Електронний ресурс] / G. Kalfas, G.I. Papadimitriou, P. Nicopolidis, A.S. Pomportsis // in Proc. of Wireless Pervasive Computing, 2008. – Режим доступу: http://ieeexplore.ieee.org/document/4556247/.

15. Rafzar Mojtaba. Single Channel Versus Multichannel MAC Protocols for Mobile Ad Hoc Networks // [Електронний ресурс] / Mojtaba Rafzar, Ali Abedi // Proceedings of the World Congress on Engineering and Computer Science, 2011. –.Режим доступу: https://www.researchgate.net/publication/265561943_ Single_Channel_Versus_Multichannel_MAC_Protocols_for_Mobile_Ad_Hoc_Networks.

16. Tang Z. A protocol for topology-dependent transmission scheduling in wireless networks [Електронний ресурс] / Z. Tang, J.J. Garcia-Luna-Aceves // In IEEE Wireless Communications and Networking Conference. – Sep. 2011. – PP. 1333-1337. – Режим доступу: https://ccrg.soe.ucsc.edu/publications/ kevin.wcnc99.pdf.

17. Eun-Sun Jung. A Power Control MAC Protocol for Ad Hoc Networks / Eun-Sun Jung, Nitin H. Vaidya // Wireless Networks. – January 2005. – Volume 11. – Pages 55-66.

18. Zhuochuan Huang. A Busy-Tone Based Directional Mac Protocol for Ad Hoc Networks [Електронний ресурс] / Zhuochuan Huang, Chien-Chung Shen // Department of computer and Information science, University of Delaware, October 2002. – Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.20.5468&rep=rep1&type=pdf.

19. Sudipta Majumder. Directional MAC Protocols in Ad-Hoc Networks / Sudipta Majumder, Syed Emdadul Haque, Fernaz Narin Nur // International Journal of Computer Applications (0975 – 8887). – August 2014. – Volume 100, No.11. – PP. 29-36.

Автори статті

Максимов Володимир Васильович – кандидат технічних наук, доцент кафедри телекомунікаційних систем, Національний технічний університет України «Київський політехнічний інститут ім. Ігора Сікорського», м. Київ. Тел. +380 (68) 810 40 47. E-mail: maksimov46@ukr.net

Литвин Олександр Олександрович – студент, кафедра телекомунікаційних систем, Національний технічний університет України «Київський політехнічний інститут ім. Ігора Сікорського», м. Київ. , Тел.: +380 (98) 094 83 21. E-mail: litvinolek@gmail.com

Authors of the article

Maksymov Volodymyr Vasylyovych – candidate of sciences (technical), assistant professor of telecommunication system department, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Kyiv. Tel. +380 (68) 810 40 47. E-mail: maksimov46@ukr.net.

Lytvyn Oleksandr Oleksandrovych – student, telecommunication system department, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Kyiv. Tel.: +380 (98) 094 83 21. E-mail: litvinolek@gmail.com

Дата надходження
в редакцію: 15.06.2016 р.

Рецензент:
доктор технічних наук, професор В.Г. Сайко
Державний університет телекомунікацій