КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.4.5461
УДК 621.391.8

Бондарчук Андрій Петрович
Доктор технічних наук, професор кафедри Інженерії програмного забезпечення
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0001-5124-5102
dekan.it@ukr.net

Бржевська Зореслава Михайлівна
Аспірант, асистент кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0002-7029-9525
zoreska.puzniak@gmail.com

Довженко Надія Михайлівна
Кандидат технічних наук, доцент кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0003-4164-0066
nadezhdadovzhenko@gmail.com

Макаренко Анатолій Олександрович
Доктор технічних наук, професор кафедри Мобільних та відеоінформаційних технологій
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0002-4081-328X
makarenkoa@ukr.net

Собчук Валентин Володимирович
Кандидат фізико-математичних наук, доцент кафедри Диференціальних рівнянь і математичної фізики
Східноєвропейський національний університет ім. Лесі Українки, Луцьк, Україна
OrcID 0000-0002-4002-8206
v.v.sobchuk@gmail.com

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ ФУНКЦІОНУВАННЯ АЛГОРИТМУ ПЕРЕДАЧІ ІНФОРМАЦІЇ ПРИ НАЯВНОСТІ ПРИХОВАНИХ ВУЗЛІВ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Анотація. Сенсорні мережі являються однією із найбільш актуальних та перспективних технологій для широкого впровадження в різні сфери життєдіяльності людини. Порівняно недорогі компоненти, а саме – сенсорні вузли, в значних кількостях об'єднані між собою в одну мережу. Шляхом використання значної кількості вузлів, окрім загального впливу на функціональність, це призводить також до зниження надійності мережі в цілому. Отримуючи можливість прямого підключення до мережі зв'язку загального користування чи до мереж наступного покоління зі оптичними складовими, безпроводові сенсорні мережі мають ряд обмежень. Наприклад, відносно мала відстань для передачі інформації між складовими компонентами. Із цього випливає, що з великою ймовірністю, рано чи пізно виникатимуть відмови вузлів, що призведе до ізоляції інших сенсорів. Щоб уникнути цього, або, принаймні, забезпечити зв'язність мережі під час впливу на неї потоку відмов, необхідно використання більшої кількості вузлів на окремій ділянці. Також через наявність зв'язності між сенсорними вузлами виникає цілий ряд ключових особливостей, які повинні бути враховані при проектуванні такої мережі та розгортання її в реальних обставинах. Одним із таких завдань – є забезпечення достовірності та точності передачі пакетів інформації між сенсорними вузлами, адже порушення її цілісності, якості, надійності та безпеки можуть призвести до серйозних наслідків.
Через незначні об'єми пам'яті, сенсорні вузли не здатні фіксувати дані про всі вузли, їх фізичні адреси, метрики для найбільш швидкого передавання пакетів інформації. З

ISSN 2663 - 4023

урахування цього, кількість запитів на один і той же вузол може перевищити критичний показник в певний проміжок часу. Однак, може виникнути і ситуація коли до мережі може бути підключений вузол, який не був перевіреним, протестованим раніше. В цьому випадку, гостро піднімається питання достовірності тих даних, які будуть циркулювати в мережі від подібного, прихованого вузла до інших. Тому, на сучасному етапі розвитку необхідним є дослідження існуючих та впровадження нових алгоритмів передачі інформації при наявності прихованих вузлів в безпроводових сенсорних мережах.
Ключові слова: сенсорна мережа; захист; прихований вузол; алгоритм; інформаційні технології; сенсорні вузли; достовірність; відмови.

1. ВСТУП

Безпроводові сенсорні мережі, як правило, складаються з великої кількості малопотужних багатофункціональних безпроводових пристроїв, які розгорнуті в певній географічній зоні. Маючи обмежені фізичні ресурси здатні лише до обмеженої обробки інформації та комунікації. Проте, об’єднані разом мають можливість до виконання цілого ряду функціональних завдань в сфері науки, техніки, захисту критичної інфраструктури, захисту та моніторингу навколишнього середовища, і т.п.

Однак, використання потенційних переваг безпроводових сенсорних мереж вимагає високого рівня самоорганізації і координація між сенсорними датчиками для виконання завдань, необхідних для підтримки основного призначення, а саме необхідність створення безпроводових сенсорних вузлів для самоорганізації в багатофункціональну мережу. Створення інфраструктури сенсорної мережі для передачі даних з мульти-хопом вимагає встановлення зв'язків між сусідніми вузлами сенсорів. Однак, на відміну від спілкування через кероване середовище в проводових мережах, спілкування в сенсорних мережах має певні відмінності. Досягається шляхом розповсюдження електромагнітного сигналу через повітря. Таким чином, загальне середовище передачі повинно бути чітко та лаконічно розподілено між всіма мережевими вузлами для уникнення зіткнень, колізій, втрат та зловмисного підслуховування. Для досягнення цієї мети необхідно використовувати протокол контролю доступу до середовища. Тому дослідження побудови та покращення функціонування структури протоколів для сенсорних мереж стає ключовим завданням на сьогодення.

Проблеми побудови та розгортання сенсорних мереж, а також кодування даних вирішувались науковцями, серед яких: С.Г. Бунін, В.О. Романов, В.А. Романюк, І. Акиілдіз (I. Akyildiz), К. Фрагоулі (C. Fragouli), Р. Ахлсведе (R. Ahlswede) та ін. Проблеми забезпечення достовірності діагностування складних інтелектуальних систем досліджувалися в роботах Д.М. Обідіна, О.В. Барабаша, В.А. Савченко, О.Ю. Ільїна, І.Ю. Субача та інших вчених.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

В процесі вибору протоколу управління доступом до носія основним визначальним фактором є продуктивність сенсорної мережі. При проектуванні безпроводових сенсорних мереж було запропоновано кілька протоколів управління доступом. Зв'язок між сенсорними вузлами зазвичай здійснюється за допомогою унікального каналу. Характерним для цього каналу є те, що лише один вузол може передавати повідомлення в будь-який момент часу. Тому необхідним є встановлення протоколу MAC серед вузлів. Метою протоколу MAC є управління доступом до спільного безпроводового середовища.

ISSN 2663 - 4023

Однак, серед суттєвих недоліків, слід відзначити просторовий розподіл зв'язних вузлів [1]. Для того, щоб досягти згоди щодо того, який вузол може отримати доступ до каналу зв'язку в будь-який даний момент часу, вузли повинні постійно обмінюватися координаційною інформацією. Як правило, обмін цією інформацією вимагає використання самого каналу зв'язку. Цей аспект проблеми мультиекспозиційного середовища створює передумови для безпеки вузлів сенсорної мережі, а також - підвищує складність протоколу управління доступом.

Як наслідок, виникають нові витрати пов’язанні із необхідністю регулювання доступу між вузлами, що конкурують. Крім того, просторовий розподіл не дозволяє будь-якому вузлу мережі, при зміні статусу, легко проінформувати інші, сусідні вузли. Тому, будь-яка інформація, явно чи неявно зібрана будь-яким вузлом втрачає свою актуальність.

Виникла необхідність впровадження протоколу розподіленого багатоадресного доступу. Визначення характеру та обсягу інформації, що використовується протоколом розподіленого багатоадресного доступу, є важким завданням, але потенційно доцільним та важливим.

Для розв’язання проблеми доступу до середовища запропоновано кілька стратегій. За допомогою різних механізмів ці стратегії намагаються досягти балансу між рішенням про розподіл ресурсів та накладними витратами, необхідними для досягнення цього рішення. Ці стратегії можна класифікувати за трьома основними категоріями: фіксоване присвоєння, присвоєння за попитом та випадкове присвоєння.

Протоколи фіксованого присвоєння. В стратегіях фіксованого присвоєння для кожного вузла виділено заздалегідь задану фіксовану кількість ресурсів каналу. Кожен вузол використовує тільки виділені ресурси, не конкурують з іншими вузлами. Типові протоколи, що належать до цієї категорії, мають в собі множинний доступ з поділом каналів за частотою (FDMA), багаторазовий доступ часового поділу (TDMA) та множинний доступ з кодовим розподіленням каналів(CDMA) [2].

Протоколи розподілу за попитом. Основною метою протоколів розподілу за попитом є покращення використання каналів шляхом оптимального розподілу потенціалу каналу між вузлами. На відміну від схем фіксованого призначення, де потужність каналу призначається виключно вузлам мережі в заздалегідь відомому режимі, незалежно від поточних потреб зв'язку, протокол розподілу за попитом ігнорує вузли, які не завершили передачу пакетів, і розглядає лише вузли, які готові до передачі.

Протоколи розподілу попиту зазвичай вимагають механізм управління мережею для розмежування доступу до каналу між конкуруючими вузлами. Крім того, логічний канал керування, крім каналу даних, може знадобитися для того, щоб конкуруючі станції динамічно запитували доступ до середовища зв'язку. Залежно від характеристик протоколу, необхідність запиту доступу до каналу може затримати передачу даних.

Протоколи випадкових призначень. В схемах з фіксованим призначенням кожному комунікаційному вузлу призначається смуга частот в системах FDMA або тимчасовий інтервал в системах TDMA. Однак це призначення є статичним., тому може бути неефективними, адже трафік нефіксований. За відсутності даних, що підлягають передачі, вузол переходить в режим очікування, що призводить до того, що розподілена пропускна здатність буде витрачена даремно. Протоколи випадкового доступу були вперше розроблені для довгих радіоліній та для супутникової зв'язку. Протокол ALOHA був одним з перших протоколів доступу до мультимедіа, та дозволяє вузлам передавати пакети всякий раз, коли у них є дані для передачі. Зусилля по

ISSN 2663 - 4023

підвищенню продуктивності ALOHA приводять до розробки декількох схем для CSMA/CD та CSMA/CA.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Для підвищення пропускної здатності при впровадженні протоколу управління доступом до носія необхідно застосування чутливості несучої до передачі. Не зважаючи на те, що дане рішення може бути застосоване в безпроводових середовищах, виникають дві суттєві проблеми - прихованого і відкритого вузлів [3].

Проблеми прихованих і відкритих вузлів частково пов'язані зі змінними в часі властивостями безпроводового каналу, викликаними такими фізичними явищами, як шум, загасання і втрата шляху. Ці перешкоди в поєднанні зі швидким зменшенням потужності, яка виникає в наслідок віддаленості між передавачем та приймачем, обмежують максимально можливий діапазон передачі пакетів. Це обмеження і той факт, що CSMA сконструйований таким чином, щоб уникнути колізій та зіткнень, викликають проблеми прихованих та відкритих вузлів.

Прихований вузол визначається як вузол, що знаходиться в межах цільового діапазону приймального вузла, але виходить за межі діапазону передавального вузла. Щоб проілюструвати цей приклад, розглянемо рис.1.

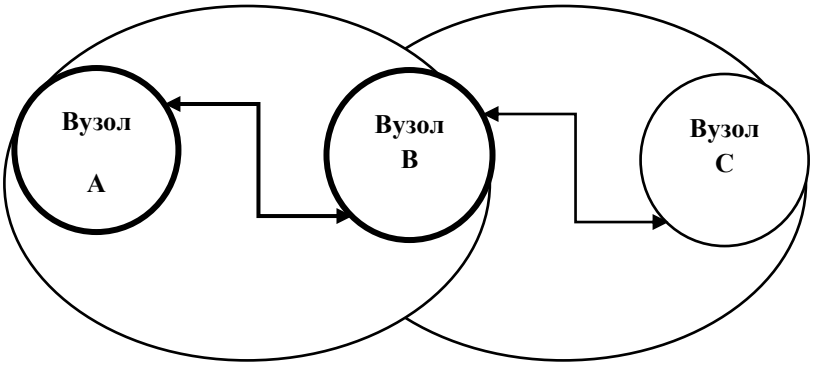

Рис.1. Сценарій функціонування прихованих вузлів в безпроводовій сенсорній мережі

Вузол B знаходиться в межах діапазону передачі вузлів A і C. Крім того, можна припустити, що вузли A і C знаходяться за межами їх взаємних діапазонів передачі. Отже, будь-яка передача з будь-якого з двох вузлів не буде фіксуватися останнім. З огляду на цю мережеву конфігурацію, припустимо, що вузол A повинен передати пакет даних вузлу B. Згідно з протоколом CSMA вузол A визначає канал і фіксує, що він вільний. Далі, вузол A відправляє свій пакет. Припустимо, що до того, як вузол A завершить свою передачу до вузла B, вузол C робить спробу передати власний пакет з даними вузлу B.

Використовуючи протокол CSMA, вузол C визначає канал, а також визначає чи канал вільний. В будь-якому випадку, вузол C діє поза діапазону передачі вузла A, і не може чути сигнал, який передається вузлом A.

В результаті таких дій, обидві передачі зіштовхуються у вузлі B, тим самим викликаючи втрату обох пакетів даних. Ні вузол A, ні вузол C не знають про зіткнення, через те, що це відбувається в приймачі.

Важливо підкреслити, що наявна проблема з відкритим вузлом також є результатом внутрішніх особливостей безпроводових каналів. Відкритий вузол - це

ISSN 2663 - 4023

вузол, що знаходиться в межах діапазону передавача, але виходить за діапазон приймача.

Для того, щоб зменшити вплив проблеми прихованого і відкритого вузла на пропускну здатність сенсорної мережі необхідно започаткувати використання сигналу «зайнято». Основна ідея даної концепції пов'язана з тим, що на приймаючому вузлі відбуваються колізії, тоді як CSMA виконується на вузлі передачі. Щоб усунути дану невідповідність, підхід «зайнятий тон» потребує використання двох окремих каналів: каналу даних і каналу управління. Канал даних використовується для передачі даних виключно. Канал управління використовується приймачем для подачі сигналів іншим вузлам в мережі, які знаходяться в процесі прийому даних.

Відразу після того, як вузол починає приймати пакет даних, який несе свою адресу в поле адреси призначення, вузол ініціює випромінювання немодульованій хвилі на каналі управління, вказуючи, що його приймач зайнятий. Вузол продовжує передавати сигнал «зайнято» одночасно з тим, що він приймає пакет даних, поки пакет не буде повністю прийнятий. Перед передачею пакета даних вузол повинен спочатку визначити канал управління для присутності «тону зайнятості». Вузол переходить до передачі пакета даних тільки в тому випадку, якщо канал управління вільний. В іншому випадку вузол відкладає свою передачу до тих пір, поки канал управління більше не буде зайнятий.

Підхід з зайнятим тоном вирішує як проблеми з прихованим, так і відкритим вузлом, припускаючи, що сигнал «зайнятого тону» випромінюється на такому рівні, що він не слабкий, щоб не бути почутим вузлом в межах діапазону приймача, і не занадто сильний, щоб завадити (створити перешкоди) для прийому-передачі більшій кількості вузлів мережі

Недолік даної концепції - необхідність роботи вузла в дуплексному режимі для одночасної передачі і прийому. Ця вимога значно збільшує складність конструкції вузла, тим самим збільшуючи його вартість і енергоспоживання.

Другий підхід до розв’язання проблеми прихованих вузлів заснований на запобіганні зіткнень [4]. Досягається за допомогою алгоритму рукостискання «ready-to-send» (RTS), «Clear-to-send» (CTS).

Використовуючи даний алгоритм, схема CSMA/CA вимагає, щоб вузли застосовували стандартний механізм, щоб уникнути зіткнення безпроводових повідомлень. Оскільки вузол не може визначити, чи відбулося зіткнення. Він намагається уникнути колізій, чекаючи, що безпроводовий носій буде звільнено протягом певного часу, який потрібен для поширення пакета через всі його носії.

Коли вузол має намір передати пакет даних, він спочатку визначає несучу, щоб визначити, чи вже передає інший вузол. Якщо ніякі інші передачі не виявлені, вузол відправляє короткий пакет (RTS) одержувачу.

Якщо одержувач знаходиться в режимі очікування, а канал вільний, надсилає коротке повідомлення (CTS) у відповідь. Після прийому пакета CTS передавач відправляє фактичний пакет даних приймачу. Якщо після закінчення визначеного періоду часу передавальна станція не приймає пакет CTS у відповідь на свій пакет RTS, він очікує певний період часу, перш ніж повторити алгоритм встановлення зв'язку RTS/CTS ще раз.

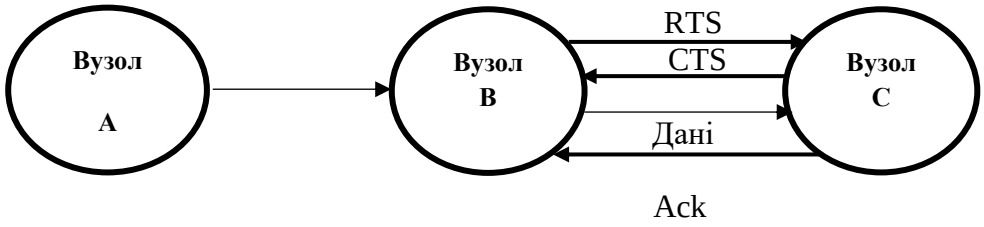

Рис.2. Ухилення від зіткнень з використанням алгоритму рукостискання RTS/CTS.

Використовуючи алгоритм RTS/CTS, вузол B, маючи намір передати пакет даних вузлу C, визначає несучу. Після фіксування незавантаженості каналу, передає пакет RTS. На додаток до адреси призначення, пакет також містить поле тривалості, яке вказує час, необхідний для завершення передачі пакету і отримання відповідного підтвердження.

У відповідь приймач (вузол C), передає пакет CTS, який містить час, що залишився до завершення передачі. Після прийому пакета RTS станція A встановлює внутрішній таймер на час, що залишився до завершення передачі пакету даних і уникає передачі будь-якого пакета вузлу B, до закінчення таймера. Коли вузол B приймає пакет CTS, він переходить до передачі свого пакета даних. У багатьох середовищах процедура встановлення зв'язку RTS/CTS достатня для значного зниження колізій і збільшення використання смуги пропускання.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Забезпечення достовірності та точності передачі інформації між сенсорними вузлами є адже порушення її цілісності, якості, надійності та безпеки можуть призвести до серйозних наслідків. Тому, на сучасному етапі розвитку необхідним є впровадження в технології побудови та функціонування мережі нових принципів обробки та захисту інформації. Процедура встановлення зв'язку RTS/CTS не повністю розв’язує проблему з прихованим вузлом, але широко використовується в безпроводових мережах, як надійний засіб зменшення колізій та збільшення пропускної здатності мережі.

Перспективами подальших наукових досліджень є: аналіз зарубіжного досвіду протидії впливу передачі пакетів від прихованих вузлів, а також більш глибоке дослідження технологій передачі достовірної інформації між сенсорними вузлами в безпроводових сенсорних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Гераїмчук М.Д., Івахів О.В., Паламар М.І., Шевчук Б.М. Основи побудови перспективних безпроводових сенсорних мереж. Монографія. – К.: ЕКМО, 2010. – 124 с.
[2] Akyildiz I. F., Melodia T., Chowdury K. R. Wireless multimedia sensor networks: applications and testbeds // Proceedings of the IEEE (invited paper), 2008. – Vol. 96. – № 10 – Pp. 1588-1605.
[3] Campobello G., Leonardi A., Palazzo S. Energy Saving and Reliability in Wireless Sensor Networks Using a CRT-based Packet Splitting Algorithm //University of Messina, Italy. – 2010.
[4] Ilyas M., Mahgoub I. „Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems”, CRC Press, New York, 2005.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

Andrii P. Bondarchuk
Doctor of Technical Sciences, Professor of The Department of Software Engineering
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0001-5124-5102
dekan.it@ukr.net

Zoreslava M. Brzhevska
Postgraduate student, Assistant of The Department of Information and Cybersecurity
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0002-7029-9525
zoreska.puzniak@gmail.com

Nadiia M. Dovzhenko
Candidate of Sciences, Assistant Professor of The Department of Information and Cybersecurity
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0003-4164-0066
nadezhdadovzhenko@gmail.com

Anatoliy O. Makarenko
Doctor of Technical Sciences, Professor of The Department of Mobile and Video information technologies
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0002-4081-328X
makarenkoa@ukr.net

Valentin V. Sobchuk
Candidate of Physical And Mathematical Sciences, Assistant Professor of The Department of Differential Equations And Mathematical Physics
Lesya Ukrainka Eastern European National University, Lutsk, Ukraine
OrcID 0000-0002-4002-8206
v.v.sobchuk@gmail.com

THE RESEARCH OF PROBLEMS OF THE INFORMATION ALGORITHM FUNCTIONING IN THE PRESENCE OF PRESERVED NODES IN WIRELESS SENSOR NETWORKS

Abstract. Sensor networks are one of the most relevant and promising technologies for wide application in various spheres of human life. Relatively inexpensive components, namely, sensor nodes are combined into one network. Due to the use of a significant number of nodes, in addition to the overall impact on functionality, this also leads to a decrease in the reliability of the network. Wireless connectivity has a number of limitations when it comes to the direct connection to the public communications network or the next-generation networks with optical components. For example, the relatively small distance to send information between constituent components. It follows next idea -sooner or later there will be the denial of nodes, which will lead to the isolation of other sensors. To avoid this, or at least to ensure the network connectivity during a failover, more nodes on a separate site need to be used. Also, due to the presence of connectivity between touch nodes, there are a number of general features that should be taken into account when designing such a network and deploying it in real-world conditions. One of these tasks is to ensure the accuracy of packets of information's transfer between the sensor nodes, as violations of its integrity, quality, reliability and safety can lead to serious consequences. Due to insignificant volumes of memory, sensor nodes are not able to capture data about all nodes, their physical addresses, metrics for the fastest transmission of information packets. In view of this, the number of requests for the same node may exceed the critical rate at a certain time. However, there may also be a situation where a node that has not been earlier tested can be connected to the network. In this case, the question of the authenticity of the data that will circulate in the network from a similar, hidden node to others is sharply raised. Therefore, it is necessary to study the existing and

the introduction of new algorithms for the transmission of information in the presence of hidden nodes in wireless sensory networks at the present stage of development.

Keywords: sensor network; protection; concealed node; algorithm; Information Technology; sensor nodes; certainty; refusals

REFERENCES

[1] Gerayimchuk M.D., Ivaxiv O.V., Palamar M.I., Shevchuk B.M. Osnovy pobudovy perspektyvnyx bezprovodovyx sensornyx merezh. Monografiya. – K.: EKMO, 2010. – 124 s.
[2] Akyildiz I. F., Melodia T., Chowdury K. R. Wireless multimedia sensor networks: applications and testbeds // Proceedings of the IEEE (invited paper), 2008. – Vol. 96. – № 10 – Pp. 1588-1605.
[3] Campobello G., Leonardi A., Palazzo S. Energy Saving and Reliability in Wireless Sensor Networks Using a CRT-based Packet Splitting Algorithm //University of Messina, Italy. – 2010.
[4] Ilyas M., Mahgoub I. „Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems", CRC Press, New York, 2005.