УДК 504.7.

<https://doi.org/10.17721/1812-5409.2419/4.10>

Керімов В. О., аспірант¹

Kerimov V. O., PhD stud.¹

**Впровадження безпеки до автономного
протоколу ієрархічної організації
бездротових сенсорних мереж**

**Introducing Security to Efficient Tree-based
Self-organizing Protocol**

¹Міжнародний науково-навчальний центр
інформаційних технологій та систем, 02000, м.
Київ, проспект Академіка Глушкова, 40,
e-mail: ¹mostlybrainless@gmail.com

¹International Research and Training Center for
Information Technologies and Systems under NAS
and MES of Ukraine, 02000, Kyiv, Glushkova av.,
40,
e-mail: ¹mostlybrainless@gmail.com

Нині бездротові сенсорні мережі широко застосовуються для виконання різноманітних задач. Задля побудови такої мережі значного масштабу, кожен з сенсорів, що її складають, має був дешевим. А значить, в умовах обмежених ресурсів сенсорів, бажаною була б побудова надійного та ефективного протоколу їх взаємодії, що забезпечував би рівномірне використання ресурсів окремими сенсорами та максимізував тривалість життя мережі. Для досягнення цієї мети протоколи із вбудованими схемами реорганізації мережі в залежності від залишку енергії в конкретних вузлах, були запропоновані. Не врахованими в таких протоколах залишаються міркування безпеки, що також є важливими при експлуатації мережі. Ця стаття пропонує модифікацію до протокола, що допоможуть виявляти та брати до уваги підозрілу поведінку певних сенсорів.

Ключові слова: бездротова сенсора мережа, безпека, протокол, дерево.

Wireless sensor networks are widely used in many modern settings. In order to build substantial networks each sensor must be cheap. So it follows that, since resources of individual sensor are limited, there is a need to create protocols that would use them sparingly and evenly in order to maximize lifetime of the network. To reach this goal some useful self-organizing tree-based protocols were created that use different properties of the network nodes, such as number of children, number of hops from the ultimate sink, distance and remaining energy, to optimally select and reselect parent node in a network. However, there is also a challenge of providing security of the network. In this paper we propose a way of integrating a simple security method akin to iterative filtering into the protocol and discuss corresponding trade-off between attack prevention and increase of energy consumption.

Key Words: wireless sensor network, security, protocol, tree.

Статтю представив д.ф.-м.н. Анісімова А.В.

Вступ

Сьогодні бездротові сенсорні мережі використовуються в найрізноманітніших контекстах і сферах, в тому числі таких як масове виробництво та спостереження за довкіллям. Для успішного виконання кожного з цих завдань необхідне улагодження збору та пересилання

даних. Необхідність у великій кількості сенсорів зумовлює використання недорогих моделей з обмеженими обчислювальними можливостями. За таких важливо налагодити взаємодію між сенсорами у такий спосіб, щоб забезпечити найдовше життя мережі.

Проблема з застосуванням ієрархічних структур задля організації агрегації даних з вузлів мережі в тому, що витрата енергії в різних вузлах буде нерівномірною. Наприклад, вузли, що агрегують інформацію з більшої кількості дочірніх вузлів витратитимуть енергію швидше за інші, через що тривалість життя мережі може не знизитись. Щоб уникнути цієї проблеми, протоколи, що реагують на такі події як падіння рівня енергії у вузлі нижче заданого рівня або «смерть» вузла, та реорганізують частини дерева, було створено.

Окрім подовження життя мережі, важливою задачею є протидія різноманітним атакам недоброзичливців, у тому числі й тим, що мають на меті спотворити справжні заміри сенсорів [2].

Метою цієї статті є включення до самоорганізуючогося ієрархічного мережевого протоколу складової, що забезпечуватиме безпеку від подібних атак, а саме – яка помічатиме та від'єднуватиме з мережі сенсори, підозрювані у підробці даних.

Протоколи з самоорганізацією

Багато з запропонованих в останні роки протоколів для бездротових мереж роблять кроки в напрямку децентралізації рішення задачі, на якому фокусується і ця робота. Децентралізований підхід до задачі подається в [3], що описує протокол LPEDAP, що базує свій підхід до побудови топології на децентралізованому алгоритмі зі знаходження мінімального кістякового (каркасного) дерева під назвою «локальне мінімальне кістякове дерево» (LSTM) [4]. Протокол передбачає як початкову побудову дерева, так і подальше підтримання його зв'язності.

Конструювання топології починається з трансляції вузлами мережі пакетів HELLO, що також містять їх координати та залишки заряду батареї, завдяки чому сенсори знаходять своїх найближчих сусідів у топології. Після цього починається наступний етап власне побудови маршрутів передачі даних, одночасно з яким відбувається побудова дерева згідно з LSTM. Розбудова дерева ведеться від базової станції. Вона транслює дані про себе у пакеті ROUTE-DISCOVERY на радіус достатній, для того, щоб сигнал зловили всі з кола найближчих сусідів, що роблять його своїм батьківським вузлом або чекають на подальші трансляції протягом зазначеного часу, виходячи з того, чи

входить ребро між відправником та приймачем сигналу до мінімального кістякового дерева. Далі всі вузли, що знайшли собі батьківський вузол, транслюють найближчим сусідам у своїй околиці аналогічний пакет, доки мережа не постане деревом з коренем у базовій станції.

Коригування створеного алгоритмом дерева відбувається за умов

- а) додача до мережі нового сенсора або
- б) вичерпання заряду сенсора, або, формальніше, зменшення заряду сенсора нижче певної межі.

Ми базуємо наше рішення на протоколі, що описано в [5]. Цей протокол (названий Efficient Tree-based Self-organizing Protocol, або ETSP) уможливорює автоматичну організацію вузлів мережі у ієрархічну структуру дерева, для визначення маршруту даних до базової станції та пізнішого оновлення цієї структури для подовження життя мережі у схожий з [3] спосіб.

Цей протокол теж складається з двох процедур: одна створює дерево після вибору кореня, а інша оновлює його, коли з'являється необхідність збалансувати витрати енергії всіх сенсорів для подовження життя мережі. Відмінність алгоритмів у тому, що в [6] у виборі з-поміж потенційних батьківських вузлів сенсори обирають за формулою, що, на відміну від алгоритму LSTM, що залежить тільки від відстаней між сенсорами та їх залишкової енергії, враховує також кількість поточних дітей у вершин дерева та довжина до базової станції у ребрах. В статті розглядається декілька формул, що по різному комбінують ці параметри.

Так само змінною, на нашу думку, може бути і список подій, що спричинятимуть оновлення дерева в протоколі. Ми можемо скористатися цим для від'єднання від мережі сенсорів, що, після деякого моніторингу, будуть визначені підозрілими.

Безпека сенсорних вузлів

[6] змальовує метод, що можна використовувати для оцінки надійності сенсорних вузлів, – ітеративне фільтрування, що діє схоже з принципом відсіювання крайніх. За методом, береться блок з послідовних замірів сенсорів і за допомогою ітеративного алгоритму отримує з нього два вектора: перший – вектор ваг сенсорів, які можна співвіднести з їхньою надійністю, а другий, його називають репутаційним, – сума зважених замірів. В статті

[7] вказано на недолік цього метода: він в своєму базовому варіанті ініціалізує ваги усіх векторів

вузла мають від'єднуються від нього та початнуть пошук нового батьківського сенсора,

Таблиця 1

Змінені параметри протоколу

Параметр	Значення
Комунікаційний радіус	10 м
Початкова енергія вузлів	27 Дж

однаково, чим нападник може скористатися, якщо йому вдасться отримати контроль над двома сенсорами, для атаки змови, за якої один з ворожих сенсоров зміщує середнє значення замірів усіх векторів, а інший відправляє значення, що точно дорівнює зміщеному середньому значенню і таким чином залишається непоміченною алгоритмом. Стаття пропонує вирішити цю проблему оцінюючи середнє значення та дисперсію кожного сенсора і врахувати їх для ініціалізації більш змістовних початкових ваг.

Запропоноване рішення

В цій статті ми пропонуємо додати алгоритм ітеративного фільтрування до протоколу самоорганізації бездротової сенсорної мережі, щоб захистити її від прихованих атак. Хоча алгоритм, приведений в [7], призначався для вузлів, розділених на кластери, його легко адаптувати і для мережі, структурованої за принципом дерева. У дереві ж-бо вузли мережі агрегують інші, що віддалені від кореня на одне ребро, подібно до кластера.

Імплементувати детектування та захист від атак пропонується наступним чином додавши до протокола ще один алгоритм. Кожен з вузлів мережі, що збирає дані (тобто усі, крім листів дерева) має проганяти алгоритм ітеративного фільтрування на своїх «дітях».

Вибрано алгоритм ітеративного фільтрування, а не його покращений варіант з [6], тому що він потребує менше обчислень.

Новий алгоритм протоколу буде застосовуватися, коли вага, встановлена для одного з дітей вузла виявиться меншою за альфа α відсотків від суми всіх вагів. В цьому випадку сенсор, що моніторить своїх дітей, транслюватиме повідомлення, що складатиметься з префікса "PT_UNTRUSTWORTHY_SINK" та IP-адреси підозрілого вузла. Інші вузли ретранслюють повідомлення після отримання його першого разу, щоб збільшити шанси на отримання повідомлення дітьми задетектованого вузла. Коли це відбувається, "діти" враженого

процес чого вже описано раніше в протоколі.

Експеримент

Для проведення експерименту сенсорну мережу було симульовано за допомогою мережевого симулятора ns-3. Топологію та базові заміри було взято з даних, наданих лабораторією Intel[3]. Надана мережа складається з 54 сенсорів, розташованих на відстані 40 на 30 метрів. В експерименті було задіяно протокол ETSP з параметрами, тотожними тим, що вказані в оригінальній статті [6], за винятком тих, що вказані в таблиці 1.

Щоб перевірити точність виявлення атак, було синтезовано комплекти даних з замірами мережі, де заміри одного з сенсорів були статистично викривлені, по комплекту на кожний сенсор. Тривалість життя мережі вимірювалася з розрахунку, що мережа «помирає», коли вичерпується заряд з понад 40 відсотків її вузлів.

За результатами моделювань, тривалість життя мережі, яка керується оригінальним протоколом, була 209,7 с, в той час як середній час для мережі, що керується змінним протоколом, був 133,2 с.

В дереві, початково побудованому в мережі, з двадцяти двох вузлів, що не є листами дерева, чотирнадцять мають від одного до двох дітей, що унеможливорює виявлення фальшованих замірів за допомогою статистичного методу. Через це швидкість виявлення атаки значно варіювалася від вузла до вузла, а для одинадцяти вузлів так і не відбулася. З іншого боку, не відбулося жодного помилкового спрацювання.

Висновки

Запропонована модифікація до алгоритму ієрархічної самоорганізації бездротової мережі сенсорів, суттєво скорочує тривалість життя мережі (в середньому на 36,5%). В експерименті вдалося досягнути доволі високого значення F1 – 0,887. Проте децентралізованість та автономність протоколу початкова структура дерева, що формується для агрегації даних у мережі, сильно

залежить від геометрії початкового розташування сенсорів, що накладає обмеження на застосовуваність ітеративного фільтрування для детекції сенсорів, підозрілих на поширення недостовірних даних.

Подальша робота може бути спрямована на знаходження початкового дерева, за яких новий

протокол буде оптимально сприятливим для виявлення атак, або на модифікації алгоритму, що призведуть до зниження його енергетичних витрат.

Список використаних джерел

1. *Malik A. S.* Energy consumption balancing (ECB) issues and mechanisms in wireless sensor networks (WSNs): A comprehensive overview / F. Ishmanov, A. S. Malik, S. W. Kim – Eur. Trans. Telecommun. – 2011. – pp. 151–167.
2. *Przydatek B.* SIA: secure information aggregation in sensor networks / B. Przydatek, D. Song, A. Perrig – Proceedings of ACM SenSys, Los Angeles, California, USA. – 2003. – pp. 255–265.
3. *Ramya K. M.* LPEDAP: Localized power-efficient data aggregation tree protocol for wireless sensor networks / K. M. Ramya, P. Shanthi – IJARCST, 2, no.1. – 2014. – pp. 229–234.
4. *Li N.* Design and analysis of an MST-based topology control algorithm / N. Li, J. C. Hou, L. Sha – IEEE Transactions on Wireless Communications. – 4, no.3. – 2005. – pp. 1195–1206.
5. *Qui T.* An efficient tree-based self-organizing protocol for internet of things / T. Qui, X. Liu, L. Feng та ін. – IEEE Access. – no.4. – 2016. – pp. 3535 – 3546.
6. *Kerchove C. De* Iterative filtering in reputation systems / C. De Kerchove, P. Van Dooren – SIAM J. Matrix Anal. Appl. – 31, no.4. – 2010. – pp. 1812–1834.
7. *Rezvani M.* Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks / M. Rezvani, A. Ignjatovic, E. Bertino та ін. – IEEE. – 12, no.1. – 2015. – pp. 98–110.
- (WSNs): A comprehensive overview. Eur. Trans. Telecommun. pp. 151–167.
2. PRZYDATEK B. (2003) SIA: secure information aggregation in sensor networks. Proceedings of ACM SenSys, Los Angeles, California, USA. pp. 255–265.
3. RAMYA K. M., SHANTHI P. (2014) LPEDAP: Localized power-efficient data aggregation tree protocol for wireless sensor networks. International Journal of Advanced Research in Computer Science and Technology, 2, no.1, pp. 229–234.
4. LI N., HOU J. C., SHA L. (2005) Design and analysis of an MST-based topology control algorithm / N. Li, J. C. Hou, L. Sha – IEEE Transactions on Wireless Communications, 4, no.3, pp. 1195–1206.
5. QUI T., LIU X., FENG L. (2016) An efficient tree-based self-organizing protocol for internet of things. IEEE Access. no.4, pp. 3535–3546.
6. KERCHOVE C. DE, DOOREN P. VAN (2010) Iterative filtering in reputation systems. SIAM J. Matrix Anal. Appl., 31, no.4, pp. 1812–1834.
7. REZVANI M., IGNATOVIC A., BERTINO E. ET AL. (2015) Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks. IEEE Transactions on Dependable and Secure Computing, 12, no.1, pp. 98–110.

Надійшла до редколегії 21.03.19

Reference

1. MALIK A. S. (2011) Energy consumption balancing (ECB) issues and mechanisms in wireless sensor networks