https://doi.org/10.5281/zenodo.15384370
УДК 004.738

Яценко Олександр,
асистент кафедри комп’ютерних наук та інформаційних технологій
Яценко Оксана,
асистент кафедри комп’ютерних наук та інформаційних технологій
Житомирський державний університет імені Івана Франка

МЕРЕЖІ З ДИНАМІЧНОЮ ТОПОЛОГІЄЮ: ПРОТОКОЛИ МАРШРУТИЗАЦІЇ ТА АНАЛІЗ ЇХ ВРАЗЛИВОСТЕЙ

Дротові комп'ютерні мережі, завдяки своєму більш ранньому розвитку, мають дуже високу швидкість і узгодженість з'єднань. Вони набагато надійніші та швидші за бездротові мережі. Але все більше пристроїв оснащуються бездротовими модулями передачі даних, так як вони забезпечують користувачам мобільність в межах певної території. Вже існує безліч бездротових технологій. Найпоширеніші стандарти: Bluetooth 11, Wi-Fi; WiMAX. В рамках кожного стандарту ведуться постійні дослідження з метою розробки нових стандартів і технологій, що підвищують швидкість передачі даних, нових принципів організації зв'язку, захисту інформації та можливостей управління трафіком.

Однією з перспективних розробок є бездротові мережі, що самоорганізовуються. Під самоорганізацією розуміють процес упорядкування елементів одного рівня в системі за рахунок внутрішніх факторів, без зовнішнього специфічного впливу. Такі мережі не мають єдиного центру управління, після підключення вузла він автоматично налаштовується, після чого всі вузли беруть

на себе функції управління мережею. Використання таких мереж має ряд переваг: можливість передачі даних на великі відстані без збільшення потужності передавача; стійкість до змін в мережевій інфраструктурі; можливість швидкої перебудови в несприятливих середовищах; простота і висока швидкість розгортання.

У зв'язку з широким спектром застосування даної архітектури в мережах різного призначення, для них розроблено значна кількість протоколів маршрутизації, які, за принципом роботи, можна поділити на три групи: проактивні (табличні), реактивні, гібридні. Проактивні проколи мають риси традиційної табличної маршрутизації: їх використання потребує побудови таблиці маршрутизації та постійного обміну сервісними пакетами для її оновлення. Цей принцип ефективний у відносно невеликих мережах, але може виявитися занадто витратним, якщо кількість пристроїв, підключених до мережі, значно збільшиться. Для того, щоб проактивні протоколи ефективно працювали у великих мережах, не повинно бути значної пропускної здатності та обчислювальних обмежень для обробки таблиць маршрутизації. Поширені сценарії, такі як додавання нового вузла, його переміщення або видалення, можуть спричинити затримки в мережах із проактивною маршрутизацією. Прикладами проактивних протоколів є: DSDV (Destination Sequenced Distance Vector), OLSR (Optimized Link State Routing), TBRPF (Topology Dissemination Base on Reverse-path Forwarding), FSR (Fisheye State Routing).

Протокол DSDV [1] заснований на ідеї класичного алгоритму маршрутизації Белмана-Форда з деякими покращеннями. Кожен вузол підтримує таблицю маршрутизації, яка містить всі доступні напрямки, кількість маршрутів (стрибків) до кінцевого пункту призначення та номер версії. Вузли періодично передають свої таблиці маршрутизації найближчим сусідам. Вузол також передає свою таблицю маршрутизації коли в ній відбулись зміни після останнього обміну. Основним недоліком протоколів на основі DSDV є необхідність регулярної передачі інформації між вузлами для оновлення їх таблиць маршрутизації, що в бездротовій мережі споживає більше заряду батареї мобільного пристрою і займає

частину пропускної здатності радіоканалу, навіть коли мережа не використовується. Крім того, при зміні топології мережі створюється новий порядковий номер для версії інформації про маршрутизацію. У дуже динамічних мережах цей параметр може переповнюватися, тобто DSDV не підходить для мереж з топологією, що швидко змінюється.

Найбільш поширеним і перспективним протоколом проактивної маршрутизації є протокол OLSR [2] Кожен вузол у цьому протоколі регулярно виявляє сусідні вузли, які доступні в одному та двох переходах на основі трансляції hello-повідомлень, що містять власну адресу вузла, перелік сусідніх доступних вузлів, їх адреси та тип з'єднання. Серед усіх вузлів, доступних за один стрибок, оптимально вибирається підмножина шлюзів MPR (Multipoint Relay) для зв'язку з усіма вузлами, доступними у двох переходах. Кожен вузол, обраний як шлюз MPR, розсилає широкомовні повідомлення TC (Topology Control), які обов'язково містять рекламу маршруту вузлам-селекторам, які вибрали цей вузол як шлюз MPR. Ці повідомлення приймаються і обробляються всіма сусідніми вузлами, але ретранслюються далі по мережі тільки вузлами, обраними в якості шлюзів MPR. На основі отриманих повідомлень TC кожен вузол будує топологію мережі та визначає оптимальні маршрути до всіх приймачів за кількістю переходів для OLSRv1 або за встановленою метрикою для OLSRv2. В результаті, тільки вузли, обрані в якості шлюзу MPR можуть брати участь в пересиланні пакетів даних.

Особливістю реактивних протоколів є те, що вони будують маршрут між конкретними вузлами тільки за вимогою (запитом) ініціатора передачі, тобто лише тоді, коли по них ведеться передача даних. Щоразу, коли вузлу-відправнику потрібно прокласти маршрут, він виконує операцію пошуку маршруту, транслюючи службове повідомлення «запит на встановлення маршруту» сусіднім вузлам. Далі кожен із сусідів надсилає це повідомлення своїм сусідам. Цей процес завершується, коли одержувач повідомлення знайдено. Вузол-одержувач відповідає сервісним повідомленням «відповідь на запит маршруту» ініціатору. При передачі пакета маршрут запам'ятовується у вигляді метрики шляху (список задіяних вузлів) і згодом, при передачі наступних

пакетів, ця інформація використовується для вибору напрямку. У великих мережах цей алгоритм дозволяє зменшити як розмір таблиць маршрутизації, так і обсяг інформації, що відправляється. До основних проблем реактивних протоколів відносять затримку в маршрутизації та відсутність підтримки застарілих маршрутів. Використання реактивних протоколів є доцільним для динамічних мереж з низьким рівнем трафіку, так як частий пошук маршрутів призводить до постійного флуду пакетів в мережі. Прикладами реактивних протоколів є: DSR (Hybrid Wireless Mesh Protocol), AODV (Ad hoc On-Demand Distance Vector), TORA (Temporally Ordered Routing Algorithm), LMR (Lightweight Mobile Routing).

Одним з перших протоколів реактивної маршрутизації був протокол DSR [3]. Особливістю DSR є те, що він накопичує інформацію про маршрут не в таблицях маршрутизації, а безпосередньо в пакеті запитів. При первинному визначенні маршруту пакети відправляються у всіх можливих напрямках і в заголовок додається інформація про пройдений вузол. В результаті, при досягненні мети, заголовок пакета містить повністю сформований маршрут між заданими вузлами. Одним з головних недоліків цього протоколу є те, що він невиправдано збільшує розмір пакета для довгих маршрутів або великих адрес, таких як IPv6. На основі DSR побудовано безліч протоколів, що поліпшують ті чи інші характеристики базової версії.

Ще одним поширеним представником реактивних протоколів є протокол AODV [3]. Цей протокол будує таблиці маршрутизації на кожному вузлі мережі, щоб мінімізувати час, необхідний для передачі інформації між ними, і знаходить шляхи маршрутизації незалежно від використання маршрутів. Першим кроком діє протоколу є побудова таблиці маршрутизації, що містить найкоротший шлях до кожного з вузлів мережі через його сусідів, на кожному вузлі. На кожному наступному кроці кожен вузол обмінюється інформацією зі своїми сусідами про найкоротший шлях, що він знає, до кожного вузла мережі. Після певної кількості кроків таблиці маршрутизації на вузлах перестають змінюватися, та починає передаватися найкоротший знайдений шлях. Протокол AODV, як і протокол

DSR, створює маршрути в міру необхідності. Однак він використовує один запис на вузол призначення, на відміну від DSR, який підтримує кілька записів маршруту для кожного вузла призначення. AODV надає інформацію про збій або зміну в мережі та пропонує альтернативні маршрути, але не вимагає глобальної періодичної маршрутизації. Крім зменшення кількості трансляцій в результаті виходу з ладу лінії зв'язку, AODV має й інші суттєві особливості. Щоразу, коли доступний маршрут від джерела до пункту призначення, до пакетів не додаються додаткові поля заголовка. Процес виявлення маршруту починається, коли маршрути не використовуються або термін їх дії закінчився. Ще однією відмінною рисою AODV є його здатність забезпечувати односпрямовану, багатоадресну та широкомовну передачу даних.

Особливість протоколу TORA [3] є те, що кожен вузол будує зважений орієнтований ациклічний граф з коренем у вузлі-відправнику та тупиком у вузлі призначення. Функціонування методу передбачає три кроки: створення маршруту, його підтримку та знищення. Перевага: надання декількох маршрутів доставки інформації адресату. Недолік: необхідність тимчасової синхронізації вузлів, можливі тимчасові «маршрутні коливання» тощо.

Гібридні протоколи поєднують в собі проактивні та реактивні механізми протоколів. Вони, як правило, поділяють мережу на підмережі, в яких використовується проактивний протокол, а зв'язок між цими підмережами здійснюється методами реактивних протоколів. Така організація маршрутизації дає можливість зменшити розмір таблиці маршрутизації та об’єм службової інформації, якою обміняться вузли мережі. До гібридних протоколів відносять: HWMP (Hybrid Wireless Mesh Protocol), HDVG (Hierarchical Distance-Vector Georouting), ZRP (Zone Routing Protocol). Недоліком гібридних протоколів є відносна складність реалізації та знижена ефективність маршрутизації через необхідність поділу мережевої структури на кластери.

Протокол ZRP [4], передбачає зонування мережі. При цьому в межах зон діє проактивна маршрутизація IARP (Intra-zone Routing Protocol), а взаємодія між зонами організовується на основі реактивної маршрутизації IERP (Inter-

zone Routing Protocol).

Протокол гібридної маршрутизації HWMP [5] базується на протоколі AODV та є обов'язковим для всіх пристроїв IEEE 802.11s як протокол за замовчуванням. У великих мережах це дозволяє зменшити розмір таблиць маршрутизації, які підтримуються вузлами, оскільки їм потрібно знати лише точні маршрути для вузлів підмережі, до якої вони належать.

Аналіз існуючих вразливостей в протоколах маршрутизації. Забезпечення безпеки процесу маршрутизації передбачає виявлення потенційних атак противника, оцінку їх загроз і вразливості використовуваних протоколів маршрутизації. Атаки, націлені на протоколи маршрутизації, можна розділити на: зовнішні та внутрішні, пасивні та активні.

Під зовнішніми атаками маються на увазі атаки зловмисника, який не має доступу до мережі. Захист від зовнішніх атак включає в себе шифрування передаваної маршрутної інформації і надання різних охоронних послуг.

Внутрішні атаки – це атаки вузла, який пройшов автентифікацію в мережі. До можливих способів захисту від внутрішніх атак (при наявності в мережі скомпрометованих вузлів) відносяться: поділ інформації на частини і передача їх по незалежних маршрутах, виявлення скомпрометованих вузлів і виключення їх з процесу маршрутизації за рахунок використання вузлами систем виявлення вторгнень [6].

Активні атаки спрямовані на часткове або повне порушення роботи мережі шляхом введення в мережу повторюваної (застарілої) або помилкової (модифікованої) маршрутної інформації.

Пасивні атаки здійснюються шляхом прослуховування радіопередач і збору інформації про маршрут з метою розкриття топології мережі і способів її вирішення. Вони не заважають нормальній роботі протоколів маршрутизації, але їх практично неможливо виявити.

Виділяють такі атаки на транспорті протоколи самоорганізовуваних динамічних мереж:

– переповнення – зловмисник може безперервно транслювати кадри PREQ, що призведе до переповнення мережі [6]. Це призведе до видалення інформації про маршрут цільового вузла в таблиці маршрутизації і він буде змушений запитувати нові шляхи через підроблені кадри PERR;

– саботаж – зловмисник може збільшити порядковий номер запиту в PREQ-кадрі, тим самим обманюючи підмережі мережі [6]. У цьому випадку таблиця маршрутизації для кожного вузла буде оновлюватися на основі припущення, що кадр PREQ містить нову інформацію. Зловмисник також може знизити показник, щоб зробити шлях кращим, хоча насправді існують більш оптимальні шляхи;

– атаки типу «wormhole» та «blackhole». Суть атаки «wormhole» полягає в тому, що зловмисник прослуховує весь мережевий трафік, записує його і передає по віртуальному каналу вузлу-спільнику, який безпосередньо передає інформацію в мережу. Під час атаки «blackhole» передавані пакети даних будуть видалені зловмисником під час пересилання [7]. У цих атаках маршрут повинен проходити через вузол зловмисника;

– replay attack – зловмисник може перехопити передані пакети за кілька сеансів зв'язку [6]. Надсилаючи перехоплені кадри і підробляючи MAC-адресу, зловмисник переконає вузол призначення, що хост жертви намагається знову зв'язатися з ним. В результаті зловмисник починає здійснювати зв'язок з вузлом призначення, а вузол-адресат вважає, зо зловмисник є першоджерелом.

– подслушивание – HWMP-кадры содержат информацию о маршрутизации. Информация о маршрутизации может быть получена путем прослушивания обмена кадрами в HWMP. Эта информация может быть полезной или бесполезной. В некоторых случаях число узлов сети в WMN должно храниться в секрете.

Крім перерахованих вище атак, окремо можна відзначити проблему егоїстичності вузлів (Selfish Attack), яка приховує маршрути з метою економії ресурсів, і атаку змови на репутаційний механізм, що використовується в ряді

протоколів маршрутизації для забезпечення їх захисту (різновид Sybil Attack). Реалізація цієї атаки дозволяє занизити або завищити репутацію вузла, що також може призвести до зміни маршруту доставки пакетів.

Список використаних джерел та літератури

1. Perkins C. E., Bhagwat P. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. ACM SIGCOMM Computer Communication Review. 1994. Vol. 24, no. 4. P. 234–244. URL: https://doi.org/10.1145/190809.190336 (date of access: 01.05.2024).

2. Optimized link state routing protocol for ad hoc networks / P. Jacquet et al. IEEE International Multi Topic Conference 2001. IEEE INMIC 2001, Lahore, Pakistan. URL: https://doi.org/10.1109/inmic.2001.995315 (date of access: 01.05.2024).

3. Gupta A. K., Sadawarti H., Verma A. K. Performance analysis of AODV, DSR & TORA Routing Protocols. IACSIT International Journal of Engineering and Technology. 2010. Vol. 2, no. 2. P. 226–231.

4. Haas Z. J. A new routing protocol for the reconfigurable wireless networks. ICUPC 97 - 6th International Conference on Universal Personal Communications, San Diego, CA, USA. URL: https://doi.org/10.1109/icupc.1997.627227 (date of access: 01.05.2024).

5. RFC 7181. The Optimized Link State Routing Protocol Version 2. Effective from 2014-04-01. Official edition. 2014. URL: https://doi.org/10.17487/RFC7181 (date of access: 01.05.2024).

6. A Survey on Security in Wireless Mesh Networks / P. Yi et al. IETE Technical Review. 2010. Vol. 27, no. 1. P. 6–14. URL: https://doi.org/10.4103/0256-4602.58969 (date of access: 07.05.2024).

7. Al-Shurman M., Yoo S.-M., Park S. Black hole attack in mobile Ad Hoc networks. ACM-SE 42: Proceedings of the 42nd annual Southeast regional conference, Huntsville, Alabama, 2–3 April 2004. New York, New York, USA, 2004. URL: https://doi.org/10.1145/986537.986560 (date of access: 01.05.2024).

8. Міночкін А. І., Романюк В. А., Шаціло П. В. Виявлення атак в

мобільних радіомереж. Збірник наукових праць. Київ, 2005. С. 102–111. URL: https://www.viti.edu.ua/files/rom/2005/3_2005.pdf (дата звернення: 01.05.2024).