УДК 004.725.7
DOI: 10.31673/2409-7292.2018.033337

Крючкова Л.П., Пшоннік В.О.

ОРГАНІЗАЦІЯ САМООРГАНІЗОВНОЇ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ В ОСШР

Розглянуто способи маршрутизації в мережах передачі даних, виконано порівняльний аналіз найбільш поширених протоколів маршрутизації. Обгрунтовано доцільність застосування протоколу маршрутизації CJDNS для організації самоорганізовної мережі передачі даних в охоронних системах швидкого розгортання.

Ключові слова: охоронні системи швидкого розгортання, самоорганізовні мережі, протокол маршрутизації.

Вступ

Сьогодні, в умовах швидкого розвитку інформаційних технологій, на об'єктах різного профілю широко впроваджуються автоматизовані системи охорони, що являють собою особливий клас автоматизованих систем збору інформації та управління. Згідно з виконаним дослідженням [1], актуальним завданням є захист мобільних об'єктів або пунктів тимчасової дислокації. Саме для захисту подібних об'єктів створюються охоронні системи швидкого розгортання (ОСШР), до яких ставиться низка вимог [1] :

1. Високий рівень захисту контрольованої зони.
2. Висока швидкість розгортання системи.
3. Висока гнучкість системи захисту (розмір та форма контрольованої зони).
4. Надійна робота системи у випадку складного рельєфу або щільної забудови.
5. Висока адаптивність до несподіваних випадків як під час розгортання так і під час штатного режиму роботи.
6. Скритність системи у радіодіапазоні.
7. Захист системи від глушіння та саботажу.
8. Висока автономність системи.
9. Можливість компонування різними типами датчиків, з визначеними інформаційними характеристиками

Вирішальне значення при забезпеченні зазначених вище вимог є протокол маршрутизації мережі передачі даних – засіб комунікації між маршрутизаторами, який дозволяє пристроям сумісно використовувати інформацію про мережу та визначати відстань до різних вузлів.

Основна частина

Протоколи маршрутизації забезпечують автоматичну побудову таблиць маршрутизації, на основі яких виконується переміщення пакетів в мережі. Таблиці маршрутизації містять дані, достатні для прийняття рішення про пересилання будь-якого пакета, що надійшов до маршрутизатора. Вміст таблиці визначається технологією складеної мережі. Як правило обирається "найкоротший" маршрут (під довжиною маршруту розуміють кількість вузлів, які пакет пройде перед тим, як дійде до отримувача)

Усі способи маршрутизації можна поділити на 2 великі групи: без таблиць та з таблицями маршрутизації.

Маршрутизація без таблиць поділяється на лавинну, керовану та від джерела.

Лавинна маршрутизація – найпростіший спосіб передавання даних, який передбачає, що кожен маршрутизатор відправляє пакет усім своїм сусідам окрім того, від кого він отримав свій пакет. Ефективність використання пропускної здатності мережі при такому способі маршрутизації дуже низька.

Керована маршрутизація передбачає, що пакет до певного користувача надсилається за маршрутом, який вже приводив до успіху. В такому випадку необхідно, щоб маршрутизатор-відправник міг фіксувати факт успіху доставки пакета.

Маршрутизація від джерела передбачає, що відправник розміщує у пакет інформацію про те, які проміжні маршрутизатори повинні брати участь у передаванні пакетів. Таку інформацію або надає адміністратор вручну, або вузол-відправник формує автоматично.

Маршрутизація на основі таблиць в свою чергу поділяється на статичну і динамічну (адаптивну). Статична маршрутизація передбачає ручне прописування маршрутів адміністратором. Така маршрутизація при зміні структури мережі потребує ручної зміни маршрутів.

У випадку динамічної маршрутизації мережі можуть оновлювати таблиці маршрутизації та швидко адаптуватися до змін топології і стану з'єднань. Успішне функціонування цього типу маршрутизації залежить від виконання маршрутизатором двох його основних функцій: підтримки таблиці маршрутизації в актуальному стані та своєчасного розподілення інформації у вигляді анонсів та оновлень маршрутів серед інших маршрутизаторів.

При розподіленні інформації про мережу, механізм динамічної маршрутизації використовує один із протоколів маршрутизації. Такий протокол визначає набір правил, що використовуються маршрутизатором при здійсненні зв'язку із сусідніми маршрутизаторами. Протокол маршрутизації визначає: яким чином розсилаються оновлення маршрутів; яка інформація міститься в оновленнях; як часто розсилаються оновлення; яким чином виконується пошук отримувачів оновлень.

Кожен із алгоритмів маршрутизації використовує свій власний спосіб вибору найкращого шляху. Для цього він генерує метрику для кожного маршруту у мережі. Зазвичай чим менша величина метрики, тим кращим вважається маршрут.

Метрики обчислюються на основі одного або більше параметрів:

- смуга пропускання – описує пропускну здатність каналу;
- затримка – час, який потрібен пакету для проходження по каналу від відправника до одержувача;
- навантаження – ступінь використання мережевих ресурсів, маршрутизатора чи каналу;
- надійність – характеризує рівень помилок у мережевому каналі;
- кількість переходів – число маршрутизаторів, через які повинен пройти пакет перед надходженням до пункту призначення;
- вартість – довільне значення, розраховується на основі ширини смуги пропускання, фінансових витрат або інших характеристик, які обирає мережевий адміністратор.

На даний час для самоорганізовних мереж передачі даних є офіційно рекомендований стандартний протокол маршрутизації IEEE 802.11s. В існуючих мережах стандарту 802.11 термінальні (абонентські,кінцеві) станції (STA) пов'язані з точками доступу (Mesh Access Point - MAP) і можуть взаємодіяти тільки з ними. MAP мають вихід в інші мережі (наприклад, Ethernet), але не можуть обмінюватися інформацією один з одним (рис. 1). У mesh-мережі, крім термінальних станцій і точок доступу, присутні спеціальні пристрої - вузли mesh-мережі (Mesh Point - MP), здатні взаємодіяти один з одним і підтримують mesh-служби. Портали mesh-мережі (Mesh Point Portal, MPP), будучи MP, з'єднують mesh-мережу з зовнішніми мережами.

Таким чином, mesh-мережа з точки зору інших пристроїв і протоколів більш високого рівня функціонально еквівалентна розгалуженій Ethernet-мережі, всі вузли якої безпосередньо з'єднані на канальному рівні.

Протокол займається оновленням таблиць маршрутизації в межах всієї мережі, працює на L2 рівні по моделі OSI [2], IP адреси необхідно налаштувати на кожній точці доступу, або користуватися послугами DHCP [3]. Також він відповідає за пошук і взаємодія із сусідніми точками та інтеграцію нових точок в Mesh-мережу. Mesh-мережа може працювати як із загальним паролем і бути закритою, так і без, шифрування (як і в звичайній Wi-Fi мережі) є тільки до точки доступу (при використанні мережі з паролем) на жаль тунельне end-to-end шифрування у даному випадку відсутнє.

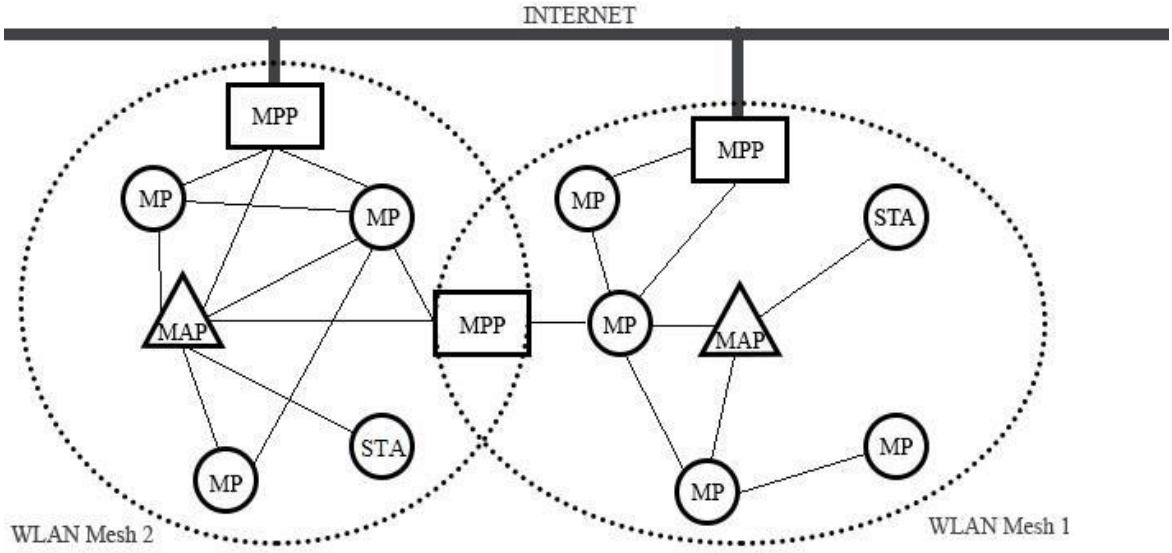

Рис. 1. Приклад побудови mesh-мережі

Згідно встановлених вимог до мереж, які використовуються у ОСШР, стандартний протокол IEEE 802.11s не задовольняє всім вимогам. Натомість йде розробка більш гнучких протоколів маршрутизації на базі open source стандартів [4].

Для організації подібних мереж з використанням *WiFi* технології розроблено відповідні протоколи маршрутизації, тому було проаналізовано найбільш поширені з них [5,6]. А саме: CJDNS, B.A.T.M.A.N., DTN, Netsukuku, OSPF.

Результати порівняльного аналізу протоколів маршрутизації у самоорганізовних мережах наведено в таблиці 1.

Таблиця 1.

Порівняльний аналіз протоколів маршрутизації у самоорганізовних мережах

	CJDNS	B.A.T.M.A.N.	DTN	Netsukuku	OSPF
Автоматичне визначення адреси	Так	Ні	Ні	Так	Ні
Автоматична маршрутизація	Так	Так	Так	Так	Частково
Розподілена маршрутизація	Так	Так	Так	Так	Частково
Об'єднання мереж	Так	Ні	Ні	Ні	Ні
Підтримка iPv4 \ iPv6	- \ +	+ \ +	+ \ +	+ \ -	+ \ -
Підтримка шифрування трафіку	Так	Ні	Ні	Ні	Ні
Автоматичне налаштування	Так	Так	Так	Ні	Так
Статус розробки	У розробці	Розроблено	У розробці	Проект закрито	Розроблено
Підтримка Linux\Unix	Так	Так	Так	Так	Так
Підтримка Windows	Так	Ні	Ні	Ні	Ні
Підтримка Mac OS	Так	Так	Так	Так	Так

Вимоги до ресурсів обладнання	Низькі	Низькі	Низькі	Високі	Низькі
Інтеграція у ядро Linux	Ні	Так	Ні	Ні	Так

За результатами аналізу встановлено, що доцільним для використання в самоорганізовних мережах є протокол CJDNS.

CJDNS - зашифрована IPv6 мережа, в якій використовуються публічні ключі шифрування для отримання публічної адреси і розподіленої таблиці маршрутизації DHT (distributed hash table) [7,8] . Це дозволяє створювати мережі з дуже простим налаштуванням, які будуть захищені від потенційних проблем нині існуючих IPv4 і IPv6 мереж. У CJDNS мережі на кожному пакеті, який спрямовується на локальний маршрутизатор, відзначається найкращий маршрут для нього. Кращий маршрут – це фізично найближчій до вас роутер, який має адресу, близький за значенням до адреси призначення. Наступний роутер в ланцюгу також читає дане поле і відправляє пакет в потрібному напрямку. Крім того, роутери постійно взаємодіють один з одним, обмінюючись інформацією, щодо маршрутів за допомогою DHT.

На даний час вже існують діючі приклади самоорганізовних мереж, на базі CJDNS протоколів [9]. Так, Hyperboria – самоорганізовна децентралізована мережа, яка сама будує маршрути між вузлами. Як проголошують її творці, це те, чим інтернет має стати: вільним, без цензури, швидким і з можливістю автоматичного масштабування [10] .

Висновки

Запропонований для передачі даних в ОСШР протокол маршрутизації CJDNS забезпечує відповідність вимогам до такого класу охоронних систем за часом налаштування, скритністю, захищеністю від глушіння та автономністю вже розгорнутої мережі.

Висока швидкість розгортання системи забезпечується розподіленими таблицями маршрутизації DHT.

Скритність системи у радіодіапазоні обумовлюється тим, що більшість вузлів мережі залишаються пасивними на протязі значного періоду часу. Сформована згідно з цією вимогою таблиця маршрутизації суттєво знижує ймовірність виявлення наявності функціонування ОСШР.

Захист системи від глушіння та саботажу забезпечується за рахунок перехресних зон дії окремих вузлів. При цьому кожний вузол завжди буде мати декілька варіантів побудови маршруту зв'язку з отримувачем.

Список використаних джерел

1. Пшоннік В. О. Охоронні системи швидкого розгортання. Сучасний стан і тенденції розвитку [Електронний ресурс] / Пшоннік В. О. // СУЧАСНИЙ ЗАХИСТ ІНФОРМАЦІЇ. – 2018. – Режим доступу до ресурсу: http://journals.dut.edu.ua/index.php/dataprotect/issue/view/104.

2. ISO Central Secretariat. ISO/IEC 7498-4:1989 -- Information technology -- Open Systems Interconnection -- Basic Reference Model: Naming and addressing" [Електронний ресурс] / ISO Central Secretariat // International Organization for Standardization.. – 2015. – Режим доступу до ресурсу: http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989(E).zip.

3. ИВАНОВ П. DHCP: искусство управления IP-адресами [Електронний ресурс] / Павел ИВАНОВ // СЕТИ #10. – 2000. – Режим доступу до ресурсу: http://citforum.ru/nets/tcp/dhcp.shtml.

4. The Open Source Definition [Електронний ресурс]. – 2007. – Режим доступу до ресурсу: https://opensource.org/docs/osd.

5. Manolidis C. Multi-hop mesh routing on B.A.T.M.A.N. advanced routing protocol [Електронний ресурс] / Charalampos Manolidis // Witestlab. – 2016. – Режим доступу до ресурсу: https://witestlab.poly.edu/blog/batman/.

6. Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with ZebraNet [Електронний ресурс] / Philo Juang, Hidekazu Oki, Yong Wang та ін.] // ACM New York, USA. – 2002. – Режим доступу до ресурсу: https://dl.acm.org/citation.cfm?doid=605397.605408.

7. Traffic Engineering (TE) Extensions to OSPF Version 2 [Електронний ресурс] // IETF. – 2015. – Режим доступу до ресурсу: https://datatracker.ietf.org/doc/rfc3630/?include_text=1.

8. Loewenstern A. DHT Protocol [Електронний ресурс] / A. Loewenstern, A. Norberg // Standards Track. – 2017. – Режим доступу до ресурсу: http://www.bittorrent.org/beps/bep_0005.html.

9. List of Known Meshlocals [Електронний ресурс] – Режим доступу до ресурсу: https://docs.meshwith.me/meshlocals/existing/.

10. Shifttstas. Hyperboria: Интернет 2.0 [Електронний ресурс] / Shifttstas. – 2013. – Режим доступу до ресурсу: https://habr.com/post/181862/.

Надійшла: 5.07.2018 Рецензент: д.т.н. Вишнівський В.В.