УДК 004.051

Бурячок Володимир Леонідович, професор, д.т.н.
Київський університет імені Бориса Грінченка
v.buriachok@kubg.edu.ua

Соколов Володимир Юрійович, аспірант
Київський університет імені Бориса Грінченка
v.sokolov@kubg.edu.ua

Кіпчук Феодосій Валентинович, магістр
Київський університет імені Бориса Грінченка
aimedforce@gmail.com

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ БЕЗПРОВОДОВИХ ВБУДОВАНИХ СИСТЕМ

Повертаючись до ключових аспектів комп'ютерних систем, потрібно визначити: як працюють вбудовані системи, які завдання вирішають ваші пристрої, архітектура та принцип роботи, чи є необхідність у додаткових модулях, забезпечення безперебійної роботи, налаштування необхідного рівню захисту та запобігання вразливостям, який потенціал розвитку проекту та його масштабованість.

Мета — вирішити проблему «останньої милі». Враховуючи специфіку мережевих пристроїв на основі безпроводових пристроїв, наголошуємо на важливості забезпечення стабільного з'єднання пристроїв, захисту їх роботи від несанкціонованого доступу та запобігання та мінімізація перешкод для нормального функціонування. Використання міні-комп'ютерів дозволяє заощадити багато ресурсів. Такі системи потребують мінімальної потужності, мережевих ресурсів та мають гнучкі налаштування. Вони також мають дуже широке функціональне розширення, завдяки додатковим модулям. Однак вбудовані системи мають також певні обмеження, такі сильно завантажені системи, як серверні частини та сервіси, будуть працювати в невеликому масштабі. Однак при логічній побудові функціональної мережі з таких пристроїв, як клієнти, агенти чи датчики, міні-комп'ютери можуть бути об'єднані у середні та масштабовані мережі [1].

В даний час велика кількість пристроїв здатні взаємодіяти один з одним, що робить їх багатофункціональними. Такі пристрої здатні працювати незалежно, у групах, виступаючи як елемент певної мережі, також відомий як Інтернет речей (IoT).

Безпроводові пристрої можуть бути вразливими до поганого покриття мережі. Цей недолік дозволяє побудувати як мінімум три вектори атаки: з фальшивою точкою доступу, підміною користувача, підробка кінцевого пристрою або точки доступу, засмічення мережі та ін. Ця робота є гарним прикладом заходів безпеки та запобігання подібним атакам [2].

Ця тема також охоплює інші вразливості безпроводових мереж, які мають той самий намір — відмова в обслуговуванні DoS або DDoS [3]. Ця архітектура наразі не нова. В даний час для запобігання DoS-атак потрібне нове рішення та більш міцна архітектура. Незважаючи на поточні випуски оновлених стандартів безпеки безпроводового зв'язку 802.11, на пристроях все ще існує багато вразливостей, тому наразі необхідно проводити аналізи та експерименти з багатьма відомими типами DoS-атак. Для цього створений алгоритм під назвою Альтернативний механізм нумерації (ANM), який запобігає атакам DoS.

Для більш точно налаштованих мереж також потрібно контролювати маршрутизацію потоку даних та керувати на мережевому рівні VLAN [4]. Рішення позиціонується як нова стратегія заходів безпеки. Це забезпечується іншим алгоритмом шифрування для непоширюваного ключа та віртуальної локальної мережі.

Одним із гарних прикладів є використання платформи як точки доступу до мережі з використанням міні-екрану, який може відображати необхідні функції моніторингу [5]. Точка доступу на базі ОС Raspbian вимагає мало ресурсів, представлена у роботі. Використання екранного модуля та програмування дозволяє відображати практично будь-яку інформацію, наприклад: підключені пристрої, стан підключення до шлюзу, спливаючі адреси пристроїв, IP-адреси пристроїв тощо [6].

У функції зовнішньої мережевої карти працювала TP-Link TL-WN722N зі специфікацією мікросхеми AR9271 та зовнішньою антеною [7]. На практиці ця мережева карта була достатньо обмежена для досягнення цілей експерименту. Як результат,

платформа не змогла працювати одночасно з більш ніж 8 пристроями, 1 сервером та 7 клієнтами. Але вбудований контролер CYW43455 підтримує вдвічі більше: 14 клієнтів та 1 сервер.

Алгоритм роботи програмного забезпечення в Business Process Model and Notation (весія 2). Було використане наступне ПЗ у експерименті:

– RPi 3B+ (2.4/5 GHz) з Raspbian Lite OS або OpenWRT;
– MicroSD 16 Gb UHS-I як сховище даних;
– TP-Link TL-WN722N версії 1;
– акумулятора батарея.

Для реалізації точки доступу були визначені наступні програмні засоби:

– hostapd є сервісом для Wi-Fi точки доступу;
– dnsmasq як DHCP-server та DNS;
– ath9k-htc драйвер для TL-WR722N;
– vsftpd як FTP-server.

На початку експерименту OpenWRT було випущено версію 18.0, але вона не спрацювала правильно: при налаштуванні точки доступу конфігурація шлюзу не зберігалася, тому була взята остання стабільна версія 17.0. Але через місяць були виправлені помилки і версія 18.01 була успішно встановлена та працювала правильно (рис. 1).

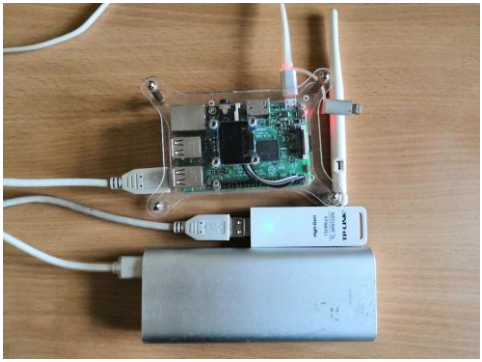

Рис. 1. Експериментальне обладнання

Для імітації стабільного навантаження, близького до умов праці в офісі компанії, було обрано метод генерації трафіку типу з'єднання клієнт-сервер за допомогою FTP: клієнти завантажу-

ють одночасно один великий файл (адже використання файлів різного розміру могло призвести до збоїв у швидкості передачі та помилок).

При виборі FTP-сервера було перевірено кілька програм, і перевага надана vsftpd, який легко налаштувати і який не має обов'язкової бази даних клієнтів та додаткових налаштувань. Крім того, vsftpd використовує мінімальну кількість операційних ресурсів і є досить безпечним, ефективним та не потребує додаткових сервісів на відміну від ProFTPD.

Для повного відстеження завантаження для всіх клієнтів, вибрано файл розміром 30 Мб. Також теоретично цей розмір дозволяє використовувати канал одночасно всіма користувачами, принаймні 90 секунд із 7 підключеними пристроями.

Тестовим середовищем було закрите приміщення, в якому було розміщено 15 персональних комп'ютерів (ПК). Посеред кімнати була розташована точка доступу та один із ПК, який служив сервером. Максимальна відстань від точки доступу до віддаленого ПК досягла 6 м, що є приблизним значенням для роботи в офісних приміщеннях.

На час тестування всі сторонні програми були відключені на усіх станціях, а активність мережі була зведена до мінімуму.

Усіма робочими станціями були Dell OptiPlex 3050 Micro з OS Windows 10 Education, мережевими картами Intel® Dual Band Wireless AC 3165 (802.11ac) 1×1 з зовнішніми антенами, направленими однаково вниз.

Побудувавши поліноміальну лінію тренда (див. рис. 2), легко побачити, що відносне зниження швидкості передачі для обох діапазонів майже однакове і відрізняється приблизно втричі (абсолютний спад швидкості для смуги частот 2,4 ГГц становив 0,04 Мб/с, а для 5 ГГц — 0,18 Мб/с).

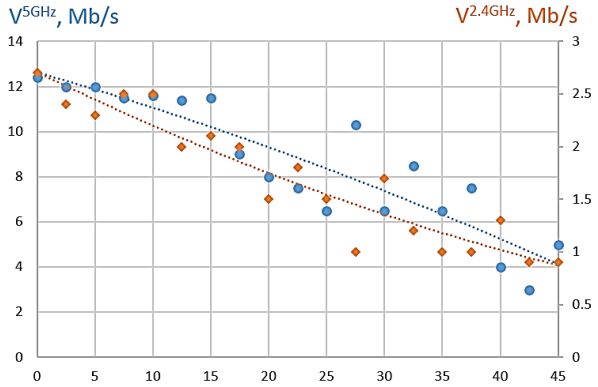

Рис. 2. Передача даних на різних діапазонах

Графік порівняння роботи контролера на різних частотах проводився у закритому приміщенні загальною довжиною до 50 м, непряма видимість без перешкод. У частково зарядженому діапазоні 2,4 ГГц та вільному діапазоні 5 ГГц. Канал 11 обраний для 2,4 ГГц і 5 ГГц для каналу 36 (рис. 3).

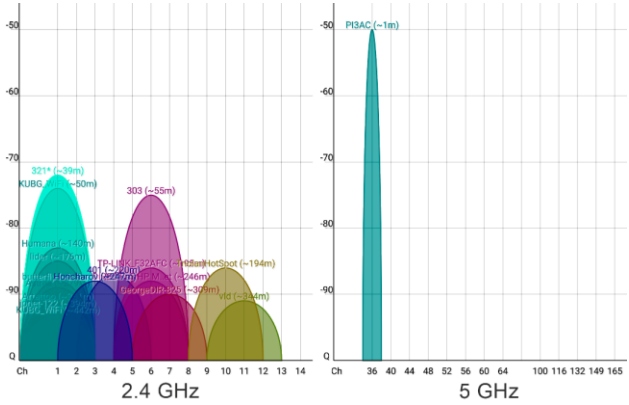

Рис. 3. Сканування частотного діапазону

При вимірюванні та перерахуванні результатів експерименту необхідно обґрунтувати його наукове значення. Для цього отримані результати були оброблені та виведені за допомогою прямої оцінки похибки вимірювання, швидкості завантаження та коефіцієнта Пірсона. Отримано максимальне значення швид-

кості на платформі WRT з максимальною швидкістю 600 кб/с і найнижчою на зовнішній платформі RPi 200 кб/с. Інші вимірювання були неуспішними через нестабільну передачу даних. Також були помилки у вигляді не запущеного завантаження після запуску команди, завантаження закінчувалось не більше ніж на декількох клієнтах і робило неможливим загальний результатів усіх станцій. Ліміт максимальної кількість клієнтів відбувався на адаптері TP-Link. Він був визначений на OpenWRT з внутрішнім адаптером для 7 та 14 клієнтів.

Ця робота окреслює та обґрунтовує поточні проблеми підключення кінцевих пристроїв у безпроводових мережах. Наявні можливості вбудованих систем можуть підтримувати з'єднання від декількох до кількох десятків пристроїв але необхідно ретельно вибирати безпроводові адаптери, які запропоновані виробниками на вбудованих платформах або розробляти рішення з використанням додаткових адаптерів, антен, підтримуваних технологій шифрування та протоколів передачі даних. У цій роботі вбудований мережевий контролер показав себе набагато краще, ніж зовнішній. Відповідно до експерименту, можемо зазначити:

– статистика вказує на можливі помилки в роботі сервісів. Навіть якщо була врахована досить універсальна мова програмування Python, яка імітувала навантаження та нормальне FTP-з'єднання клієнт-сервер;

– обмежена сумісність мережевих контролерів (мікросхем) та роботи мережевих служб ОС, хоча вона досить широка, проте вона не може гарантувати її повну продуктивність. Тож коли потрібно вибрати конкретне обладнання, архітектуру системи та сервіси — потрібно виконати тестування та налаштування прототипу для завершення. Крім того, кожен сервіс та проміжний вузол в системі повинні забезпечуватися достатньою безпекою на всіх рівнях передачі даних через модель OSI.

У наступній роботі планується перевірити службу обміну даними, базу даних або веб-сервер із певним рівнем захисту. А також проведення тесту на проникнення, перевірку стабільності описаних вище заходів безпеки та загальну оцінку вразливості розумних систем.

Анотація. У тезах представлені результати тестування навантаження вбудованих апаратних платформ для рішень Internet of Things. Проаналізовано можливості обладнання. Операційні системи різних виробників були об'єднані в єдину класифікацію і для двох найпопулярніших операційних систем проведено тестування навантаження, яке проводилось на зовнішньому та внутрішньому адаптерах безпроводової мережі. Було розроблено власне програмне рішення на основі мови програмування Python. Кількість пристроїв безпроводового зв'язку становила від 7 до 14. Експериментальні результати будуть корисні при розгортанні безпроводової інфраструктури для невеликих комерційних та наукових безпроводових мереж.

Література:

1. Sokolov V. Yu. Scheme for Dynamic Channel Allocation with Interference Reduction in Wireless Sensor Network / V. Yu. Sokolov, A. Carlsson, I. Kuzminykh // Proceedings of the IV International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2017), October 10–13, 2017: abstracts. — Kharkiv : IEEE, 2017. — P. 564–568. — DOI: 10.1109/INFOCOMMST.2017.8246463.

2. Sobh T. S. Wi-Fi Networks Security and Accessing Control / T. S. Sobh // International Journal of Computer Network and Information Security. — 2013. — Vol. 5, no. 7. — P. 9–20, — DOI: 10.5815/ijcnis.2013.07.02.

3. Liu H. A New Secure Strategy for Small-Scale IEEE 802.11 Wireless Local Area Network / H. Liu, H. Zhang, W. Xu, Y. Yang // International Journal of Wireless and Microwave Technologies. — Vol. 2, no. 4. — P. 21–27. — DOI: 10.5815/ijwmt.2012.04.04.

4. Durairaj M. ANM to Perceive and Thwart Denial of Service Attack in WLAN / M. Durairaj, A. Persia // International Journal of Computer Network and Information Security. — Vol. 7, no. 6. — P. 59–66. — DOI: 10.5815/ijcnis.2015.06.07.

5. Buryachok V. L. Using 2.4 GHz Wireless Botnets to Implement Denial-of-Service Attacks / V. L. Buryachok, V. Yu. Sokolov // Web of Scholar. — 2018. — No. 6(24), vol. 1. — P. 14–21. — DOI: 10.31435/rsglobal_wos/12062018/5734.

6. IoT Collection [Електронний ресурс]. — Режим доступу : https://github.com/oestoidea/iot.

7. Raspberry Pi Documentation. Release 0.0 [Електронний ресурс]. — Режим доступу: https://media.readthedocs.org/pdf/raspberry-piintro/latest/raspberry-pi-intro.pdf.