

8. *Edelson G. S., Tufts D. W. On the ability to estimate narrow-band signal parameters using towed arrays // IEEE Journal of Oceanic Engineering. 1992. V. 17, № 1. P. 48–61.*

9. *Cramer-Rao lower bound for localization of a source with partial temporal coherence using passive synthetic aperture / A. S. Ivanenkov, P. I. Korotin, D. A. Orlov [et al.] // Proc. of the 12th European Conference on Underwater Acoustics. 2012. Edinburgh, United Kingdom. P. 564–571.*

**Рецензент:** доктор техн. наук, доцент **О. М. Ткаченко**, Державний університет телекомунікацій, Київ.

*М. Н. Степанов, В. И. Корсун, К. А. Соколов*

### **МЕТОДИКА ОПРЕДЕЛЕНИЯ КООРДИНАТ СТАЦИОНАРНЫХ ИСТОЧНИКОВ РАДИОИЗЛУЧЕНИЯ В УСЛОВИЯХ МНОГОПОЗИЦИОННОГО ПРИЕМА ЛОКАЦИОННОЙ ИНФОРМАЦИИ**

Проанализировано влияние движения приемных элементов системы мониторинга на ее функциональные возможности пространственно-временной обработки сигналов от априорно неизвестных стационарных источников радиоизлучения и сформулирована методика определения координат их расположения в пассивном режиме мониторинга с ненаправленным приемом.

Предложен метод преследования «ведущий-ведомый» на интервале времени мониторинга для однозначного определения пеленгов на источники радиоизлучения в пассивном режиме при движении радиоприемников с априорно определенной пространственной конфигурацией.

**Ключевые слова:** радиомониторинг; дистанционно пилотируемый летательный аппарат; БПЛА; источник радиоизлучения.

*М. М. Stepanov, V. I. Korsun, K. A. Sokolov*

### **METHOD OF DETERMINATION OF COORDINATES OF STATIONARY SOURCES OF RADIO EMISSION IN CONDITIONS OF MULTIPPOINT RECEPTION OF LOCATION INFORMATION**

The paper analyzes the influence of the motion of the receiving elements of the monitoring system on its functionality in terms of space-time signal processing from a priori unknown stationary sources of radio emission and proposes a method for determining the coordinates of their location in the passive monitoring mode with direct reception.

The proposed method of pursuit of «leading-slave» at the interval of monitoring time for unambiguous determination of bearings for radio sources in the passive mode when moving radios with a priori defined spatial configuration.

**Keywords:** radio monitoring; remote piloted aircraft; UAV; DRV.

УДК 004.7

**А. В. КРИВКІН**, бакалавр,

Державний університет телекомунікацій, Київ

## **ЕВОЛЮЦІЯ ЗАХИСТУ БЕЗПРОВОДОВОЇ ТЕХНОЛОГІЇ Wi-Fi**

**Еволюція технології безпроводових мереж щодо надійності та швидкості її сприйняття пішла на користь як споживачам, так і бізнесу. Таке стрімке зростання розвитку безпроводових мереж зумовило необхідність бути постійно доступними. Обговорено перспективи впровадження інформаційних та телекомунікаційних технологій в Україні та світі, де мережі потребують технічних знань та допомоги стосовно правильного налаштування повністю надмірних Wi-Fi вирішень із використанням переваг найсучасніших функцій безпроводових технологій. Запропоновано порівняння двох технологій.**

**Ключові слова:** безпека; шифрування; стандарт; доступ; протокол.

### **Вступ**

Усе частіше останнім часом у світових ІТ-новинах з'являються повідомлення щодо компаній, які використовують технологію Wi-Fi у повсякденній роботі або надають Wi-Fi послуги клієнтам з анонсуванням різних пристроїв із вбудованою підтримкою Wi-Fi, зокрема мобільні телефони, КПК чи ноутбуки. Очевидно, що впровадження цієї технології здійснюється надзвичайно швидкими темпами, і багато аналітиків давно пророкують їй успішне майбутнє, яке може кардинально змінити сьогоднішній підхід до ви-

користання комп'ютерів і мобільних пристроїв. Стандарт Wi-Fi з'явився ще в середині 90-х і почав активно просуватися з 2000 року. Проте нині лише деякі користувачі уявляють собі, що саме приховано за загадковою аббревіатурою Wi-Fi. Ця технологія наразі розвивається з винятковою швидкістю. Упровадження Wi-Fi відбувається повсюдно в усьому розвиненому світі. Це зумовлено великою кількістю переваг даної технології, хоча вона має і низку недоліків. У статті розглянуто як позитивні, так і негативні боки даної технології, оскільки ця технологія є не тільки засобом

© А. В. Кривкін, 2019

зв'язку, що полегшує роботу, а й приносить значний матеріальний зиск. Отже, розглянемо далі, що саме врешті-решт являє собою Wi-Fi.

#### Основна частина

Технологія Wi-Fi — безпроводовий аналог стандарту Ethernet, на основі якого сьогодні побудовано чималу кількість офісних комп'ютерних мереж. Його було зареєстровано в 1999 році, і він став справжнім відкриттям для менеджерів, торгових агентів, співробітників складів, основним робочим інструментом яких є ноутбук або інший мобільний комп'ютер.

#### Wi-Fi Protected Access

На щастя, підмножина захищеного доступу Wi-Fi (WPA) 802.11i відкрита для вирішення вразливості щодо доступу до ключів WEP, до повного вирішення 802.11i — керованої промисловості. WPA було спеціально розроблено з метою підвищення рівня безпеки для нових безпроводових локальних мереж та керування наявними рішеннями за допомогою оновлень програмного або мікропрограмного забезпечення. Це рішення орієнтовано на всі відомі вразливості і є надійним рішенням щодо безпеки з такими функціями [1; 2]:

- реалізації автентифікації на основі 802.1X EAP (*Extended Protocol Authentication*), що застосовує взаємну автентифікацію;
- застосування протоколу тимчасової ключової цілісності (TKIP) до наявних RC4 WEP для накладення надійних даних шифрування та управління ключами;
- покращеної цілісності повідомлення (за допомогою перевірки цілісності повідомлення Майкла).

#### Virtual Private Network vs. Reverse Proxy

Більшість людей для підімкнення до своєї корпоративної мережі використовують віртуальну приватну мережу із загальновідомою назвою «Тунелі». Навіть безпроводові та проводові маршрутизатори споживання мають VPN та деякий брандмауер із можливістю DMZ. Альтернативою VPN, яка швидко набуває загального визнання, є використання зворотного проксі для отримання широкого доступу. Зворотний проксі передає http-трафік назад і впоперек брандмауера від пристрою до бек-серверів та веб-служб, наприклад, Microsoft, обмін серверів, бази даних, файлові сервери та будь-які веб-програми.

Усе це здійснюється через http, https або http за допомогою AES, 3DES чи іншого шифрування для захисту переданих даних. Це ідеальне рішення для ноутбуків, що мають доступ до безпроводових та мобільних мереж. Майже всі програми і

багато програмних вирішень використовують цей метод, зокрема: пристрій керування, вирішення безпеки, синхронізація PIM, обмін файлами (наприклад, Microsoft SharePoint) і синхронізація бази даних. Сюди можна додати мультимедійні та голосові програми, а також миттєві повідомлення. Microsoft SQL 2005 та Microsoft VisualStudio 2005 будуть тісно зінтегровані та підтримуватимуть наступні покоління необхідного проксі-коду, щоб увімкнути синхронізацію бази даних http, де розробники можуть додати необхідну безпеку — наприклад, *Advanced Encryption Standard (AES)*, шар захищеного сокета (*SSL*) або стандарт шифрування даних (*DES*). AES є найвищим оптимальним шифруванням для мобільних пристроїв, завдяки низьким потребам щодо пам'яті та потужності оброблення процесора. Це має величезний вплив на мобільність стосовно ресурсу акумулятора, часу, ціни та споживача. Високе розуміння проблем, пов'язаних із безпекою безпроводового зв'язку, є ключовим фактором захисту ваших даних та мережі. Це стосується будь-якого типу зв'язку — проводового або безпроводового. За останні вісім років безпека безпроводових мереж зазнала великих змін щодо усунення вразливості конфіденційності. Безпроводова мережа може бути безпечнішою за умови застосування нових доступних рішень. IEEE 802.11 Group, Wi-Fi Alliance та основні постачальники мережного обладнання, такі як Hewlett-Packard, CISCO та Microsoft працюють разом над розробленням нових стандартів рівнів безпеки. WPA, як тимчасове рішення щодо вразливості WEP, доступне майже на всіх мобільних пристроях HP. WPA, що є підмножиною стандарту 802.11i, вирішує всі проблеми вразливості WEP. Окрім того, розроблено WPA попередньо розділений ключ для використання в домашніх умовах або в домашніх офісах, де немає потреби в сервері автентифікації.

#### Wi-Fi Protected Access 2 (WPA2)

Як наступник WPA, стандарт WPA2 було ратифіковано IEEE 2004 року як 802.11i. Як і його попередник, WPA2 також пропонує корпоративний та особистий режими. Хоча WPA2 все ще має вразливості, він вважається найбезпечнішим наявним стандартом безпроводової безпеки. WPA2 замінює шифр RC4 і TKIP двома більш потужними механізмами шифрування та автентифікації: розширеним стандартом шифрування AES та режимом лічильника з протоколом коду автентифікації коду ланцюга шифрувального блока CCMP. Також WPA2 підтримує сумісність із зворотним процесом як резервний, якщо пристрій не може підтримувати CCMP. Розроблений урядом США для захисту секретних даних AES складається з трьох симетричних блок-шифрів. Кожний зашиф-

ровує та розшифровує дані у блоках із 128 бітів за допомогою 128, 192 і 256-бітних ключів. Хоча використання AES потребує більшої обчислювальної потужності з боку AP і клієнтів, постійні вдосконалення комп'ютерного та мережного обладнання пом'якшили проблеми з ефективністю. CCMP захищає конфіденційність даних, дозволяючи отримувати дані лише авторизованим користувачам мережі, а також застосовує код шифрування ланцюга коду автентифікації повідомлення для забезпечення цілісності повідомлення [4]. WPA2 також запровадив більш безпроблемний роумінг, що дає можливість клієнтам переходити з однієї AP в іншу в одній мережі без потреби повторної автентифікації, використовуючи кешування Pairwise Master Key або попередню автентифікацію.

### IEEE 802.11ax

IEEE 802.11ax — це еволюційне покращення стандарту 802.11ac. Одна з цілей 802.11ax, також відома як безпроводовий зв'язок HE, — забезпечити більш високий рівень ефективності в наявних мережах Wi-Fi:

- послідовне уможливлення високої швидкості передавання даних за типових умов Wi-Fi [3];
- зосередження на ключових показниках ефективності KPI, які підвищують якість QoS.

У традиційному підприємницькому просторі включають у себе:

- середовища з високою щільністю UHD із кількома користувачами, кожний з яких має трьох-чотирьох клієнтів 802.11, а також усіх споживачів мережних ресурсів одночасно;
- посилене прийняття додатків у режимі реального часу, зокрема 4K відео, та розширену або віртуальну реальність AR/VR.

Забезпечення швидкостей передавання даних у гігабітах в одному просторовому потоці з використанням 1024 QAM пропонує пік теоретичної пропускної здатності, який досягається регулярно за низької щільності підприємства. Однак, коли щільність клієнта (і, як наслідок цього, щільність точки доступу) збільшується, імовірність досягнення цієї пропускної здатності зменшується у міру того, як утримання каналів чи ефірного часу використання збільшується від використання клієнтом або в тому самому наборі базових послуг BSS (точка доступу), або у клієнтів і в сусідній точці доступу, і перекривається BSS (OBSS). Це часто називають останньою деградацією каналу. Втручання ICH, особливо проблематично в місцях відкритого простору, зокрема конференц-залах та нагромадженнях точок, де поширення ВЧ близьке до ідеального або лінійного зору LOS. Для усунення цих відомих явищ 802.11ax репрезентує OFDMA, який є новим механізмом доступу до каналу, але не відрізняється від стільникових LTE

радіомереж, оскільки він підтримує надійність Wi-Fi у неліцензованих спектрах. OFDMA забезпечує безперешкодне передавання кільком клієнтам як у висхідній, так і у низхідній лінії зв'язку UL у межах відповідних можливостей передавання TXOP. Доступ від каналу EDCA до UL-OFDMA дає змогу точці доступу впливати на відносні пріоритети доступу до каналу клієнтів, навіть від 11ax до 802.11ac клієнтів. Вони більш ефективні та менш схильні до втрат пакетів і дрижання через суперечливість, а тому, дозволяючи точці доступу точно контролювати як висхідну лінію, так і передавання низхідної лінії зв'язку, також уможливають отримання більшого детермінізму.

### Коли оновлення до 802.11ax?

Клієнти підприємств та постачальників послуг сьогодні можуть робити вибір між двома чудовими технологіями:

- IEEE 802.11ac з MU-MIMO, формуванням променя та швидкістю передавання від 290 до 1300 Мбіт/с у діапазоні 80 МГц;
- IEEE 802.11ax до 8 SS та 600–1800 Мбіт/с для клієнтів із 1024 QAM плюс додатково передбачуваність для розширення програми.

Стандарт IEEE 802.11ac доступний сьогодні і є надійним для більшості випадків використання. Тоді як IEEE 802.11ax — це майбутнє безпроводових локальних мереж, проте точки доступу до 802.11ax, сертифіковані Wi-Fi, будуть відкриті лише через кілька місяців. Клієнтські смартфони, планшети, ноутбуки тощо, які підтримують 802.11ax, також будуть доступні, починаючи з 2019 року.

З огляду на те, що більшість підприємств-клієнтів розгортають нові точки доступу одночасно, облаштовуючи будівлю або модернізуючи приміщення, то саме IEEE 802.11ax стане у пригоді, оскільки забезпечуватиме:

- 4K/8K відео в діапазоні для кількох одночасних користувачів;
- клієнтів із надвисокою щільністю (UHD);
- детермінованість для додатків AR/VR та значну економію електроенергії, особливо для пристроїв IoT.

### Висновки

У нашій країні найбільшу зацікавленість до технологій безпроводового доступу (особливо широкосмугового) виявляють оператори стільникового зв'язку і провайдери інтернету. Використанню безпроводових систем для корпоративних потреб приділяється значно менше уваги, хоча саме цей сегмент замовників є сьогодні одним з основних споживачів подібних вирішень в Україні. На жаль, за останні роки ситуація з виділенням для цього належного частотного ресурсу не стала простішою.

Перевага безпроводових локальних мереж очевидна — їх простіше і дешевше розгортати та модифікувати, оскільки вся громіздка кабельна інфраструктура виявляється зайвою. Ще одна перевага — забезпечення мобільності користувачів. Однак за ці переваги безпроводові мережі розплачуються довгим переліком проблем, які зумовлює нестійке і непередбачуване безпроводове середовище. Завади від різноманітних побутових приладів та інших телекомунікаційних систем, атмосферні завади і відбиття сигналу завдають великих труднощів для надійного приймання інформації.

Зрештою, ключ до подолання перешкод щодо впровадження безпроводових технологій зараз і в майбутньому полягає в правильному розумінні, плануванні та побудові безпроводової мережі підприємства.

Безпроводова мережа — це не вирішення на кшталт «встановив і забув». Потрібно регулярно здійснювати аудит мережі, взаємодіяти з IT-службами на ранніх стадіях побудови мережі, а також під час її функціонування.

Дотримуючись цих нескладних умов, користувачі можуть насолоджуватися гнучкістю і універсальністю, властивими безпроводовим вирішенням, у багатьох випадках знижуючи свої витрати.

Отже, ідея використання безпроводових каналів передавання даних як альтернатива кабельних мереж набуває дедалі більшої популярності. Передусім це пов'язано з нерозвиненістю інфраструктури «останньої милі». Напевно, коли в Україні буде створено широку інфраструктуру високошвидкісного абонентського доступу (наприклад, по каналах ISDN), потреба в безпроводових каналах помітно знизиться. Однак наскільки швидко це станеться — невідомо, а поки безпроводові технології ще можуть бути достатньо корисними.

#### Список використаної літератури

1. **IEEE 802.11** [Електронний ресурс]. URL: [https://uk.wikipedia.org/wiki/IEEE\\_802.11](https://uk.wikipedia.org/wiki/IEEE_802.11) (07.10.2019).
2. **Макаренко В., Доля С.** Особенности стандарта беспроводной связи IEEE 802.11ac (WiFi). Киев: VD MAIS, 2012. № 7.
3. **IEEE 802.11ax: The Sixth Generation of Wi-Fi.** Cisco public, 2019.
4. **A base station switching on-off algorithm using traditional MIMO and spatial modulation** [Електронний ресурс]. URL: <https://ieeexplore.ieee.org/document/%206708091>. Назва з екрану (28.09.2019).

**Рецензент:** канд. техн. наук **В. І. Кравченко**, Державний університет телекомунікацій, Київ.

А. В. Крывкин

#### ЭВОЛЮЦИЯ ЗАЩИТЫ БЕСПРОВОДНОЙ ТЕХНОЛОГИИ Wi-Fi

Эволюция технологии беспроводных сетей относительно надежности и скорости ее восприятия стала выгодной как потребителям, так и бизнесу. Такой стремительный рост развития беспроводных сетей обусловил необходимость быть постоянно доступными. Обсуждены перспективы внедрения информационных и телекоммуникационных технологий в Украине и мире, где сети требуют технических знаний и помощи для правильной настройки полностью чрезмерных Wi-Fi решений с использованием преимуществ современных функций беспроводных технологий. Предложено сравнение двух технологий.

**Ключевые слова:** безопасность; шифрование; стандарт; доступ; протокол.

A. V. Kryvkin

#### THE EVOLUTION OF Wi-Fi WIRELESS TECHNOLOGY PROTECTION

The evolution of wireless technology in reliability and speed went hand in hand with its quick perception by both consumers and business. This explosive growth has necessitated a wireless network that is constantly available. Discussing the prospects for the development of information and telecommunication technologies in Ukraine and the world, where networks need the necessary technical knowledge and help to properly configure completely excessive Wi-Fi solutions, taking advantage of the modern wireless technology features. You can choose between two great technologies.

**Keywords:** security; encryption; standard; access; protocol.